Viedoc™

Preparing for the EU GDPR in Clinical and Biomedical Research

Authors
Alan Yeomans, Quality Manager, PCG Solutions
Isabelle Abousahl, CIPP/E (Certified Information Privacy Professional / Europe), Alcoam by Design

Disclaimer

Even though this document includes information of a legal nature, it has been drafted and published for informational purposes only. Thus, this document shall not be regarded as legal advice and neither as an exhaustive source for rules or regulations applicable on the subject for the document. PCG Solutions AB has applied reasonable efforts to assure the accuracy of the content of the document but gives no guarantee regarding the accuracy and completeness of the content. Readers of this document should seek appropriate independent professional legal advice prior to relying on, or entering into any commitment based on this document. Any contractual obligations of PCG Solutions AB are exclusively regulated in its agreements with each customer. Accordingly, nothing contained in this document shall be construed as imposing any additional obligations and/or undertakings for PCG Solutions AB.

Contents

1 Introduction

1.1 Objective

It is important that all companies understand how they will be affected by the new European Union (EU) General Data Protection Regulation[1] (GDPR), even those not currently active within the EU. The objective of this white paper is to share the elements taken into consideration by PCG Solutions and to prepare our customers for GDPR by describing in what ways those elements may affect them.

Many of the responsibilities and obligations defined by GDPR are not new for companies in the Clinical Research sector, therefore the white paper concentrates on those areas that might be considered new requirements to the Clinical Research sector. Many companies will find they are already in compliance with these areas as they are similar to requirements to be found in local data privacy regulations in other parts of the world.

At PCG Solutions, we think it is important that we and our customers:

- prepare proactively for GDPR
- communicate on the approach foreseen for its implementation
- keep abreast of the new guidelines and information that will be made available by the Supervisory Authorities until May 2018, and beyond

1.2 Background

In the European Union, the Data Protection laws from each Member State are implementations of the Directive 95/46/EC on *"the protection of individuals with regard to the processing of personal data and on the free movement of such data[2]"*.

This Directive was implemented in 1995. As for any Directive, each Member State had the possibility to generate their own specific interpretation and adaptation of the text in their national law. This has led to a lack of harmonisation across Europe.

As of the 25th of May, 2018, this Directive will be repealed and replaced by GDPR. A Regulation is a binding legislative act, which must be applied in its entirety across the EU. It will then become directly applicable and enforceable by law by each Member State, at the same date, and thus in a harmonised manner.

[1]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L 119, 4.5.2016, p. 1–88.

[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. Official Journal L 281, 23/11/1995 P. 0031 – 0050.

2 Terminology

Many of the terms used in the GDPR, defined in Article 4, have direct equivalents in the clinical research sector, where applicable these are explained below.

2.1 Data Subject

"An identified or identifiable natural person" whose information is being collected for the clinical trial. In clinical research this corresponds to the subject or patient, as well as to the investigator, the site staff and other study personnel such as monitors, data managers, project managers, etc.

"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."

2.2 Personal Data

"Any information relating to an identified or identifiable natural person ('data subject')."

In some clinical trials, knowing the site and diagnosis may be sufficient to be able to identify the data subject.

2.3 Genetic Data

"Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

In some clinical trials, samples are taken from the subjects or patients in order to characterise their genetic profile and to use this information to correlate sub-populations of patients responding to the treatment to a specific genetic profile, which then may be studied and validated as a biomarker.

2.4 Data Concerning Health

"Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

This category of personal data is widely used in clinical trials (e.g. results from physical evaluations, measurements of vital signs, results from biological tests, etc.).

2.5 Processing

Processing is defined by GDPR as *"...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*

Any operation that affects the data from a clinical trial during its entire life-cycle, from its collection by the sites as source data to its reporting, archival and destruction.

2.6 Pseudonymisation

"The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

In a clinical trial, it is standard practice to pseudonymise the data collected within the sponsor's Case Report Forms. The key-code used to this end is kept separately and securely by the investigator.

2.7 Controller

The controller is defined in GDPR as *"...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".*

In clinical research, the **Sponsor** is always a controller. Other organisations may qualify as joint controllers (e.g. a CRO being delegated a full clinical development plan, or an investigator in an academic trial).

2.8 Processor

The processor is defined in GDPR as *"...a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

In clinical research this corresponds to anyone appointed by the Sponsor to work with the clinical trial, including **CROs** (project management, monitoring, data management, statistics, medical coding, medical writing, etc.) and **Vendors** (eCRF/EDC, ePRO, IVRS/IWRS, central labs, etc.).

2.9 Supervisory Authority

A supervisory authority is *"an independent public authority which is established by a Member State", "to be responsible for monitoring the application of the GDPR".*

3 What is GDPR?

Data Protection and Good Clinical Practice (GCP) are highly ethical matters. They have both been progressively regulated, since the mid-20th century, seeking for a harmonised approach, with an intent to reach a broad geographical scope: this has led to the OECD Guidelines[3] for Data Protection (which principles have been incorporated in the EU Data Protection laws) and ICH E6 Guidelines for GCP[4]. It is therefore not surprising that most of their fundamental principles are analogues (e.g. consent). On the other hand, there are principles specific to clinical trials which have to be considered as they may be different from standard data protection practices (e.g. the very long retention time required for clinical trial data).

The GDPR, in comparison to the EU Directive on Data Protection, will bring key changes, such as, but not limited to:

- an extra-territorial effect of the law
- the accountability principle, applied to controllers AND processors
- new rights for the data subjects (e.g. the right "to be forgotten", the right to data portability)
- introduction of "privacy by default" and "privacy by design" principles
- privacy impact assessment under the responsibility of the controllers
- an increased control and sanction regime enforced by the supervisory authorities

The reader will find in this section the GDPR requirements which are the most relevant in the context of clinical trials. It is not intended to be a didactic, nor an exhaustive view of the GDPR content, but rather to highlight the key points that are considered by PCG Solutions for an implementation in context of the use of Viedoc.

3.1 Lawfulness

This is in relation to the legal basis on which the processing of the subject's personal data can take place. For clinical studies conducted under GCP, the legal ground for the processing of personal data remains with GDPR the explicit consent of the data subject, as we will see in the following sub-sections.

3.1.1 Special categories of personal data

They are:

> *"...data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation...".*

Data from clinical trials, and from the biomedical research in a broader manner, most generally falls into the special categories of personal data.

[3]Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. Organisation for Economic Co-operation and Development. The OECD Privacy Framework. OECD 2013 (the first update of the original 1980 version).

[4]International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use. ICH Harmonised Tripartite Guideline. Guideline for Good Clinical Practice E6 (R1). Finalised Guideline May 1996 + Integrated Addendum (R2).

The collection of special categories of personal data is prohibited by the GDPR, unless one of a list of exceptional conditions are met, among which if the data subject give their explicit consent for the collection of these categories of data.

However, GDPR also allows Member States of EU to place restrictions on the ability of the data subject to consent to the collection of the above data, so in individual Member States it may not be possible to collect some of the above categories of data, unless additional conditions are met (this may apply for instance to genetic data, since it may by itself allow identification of a person). GDPR does also allow for the processing of the above categories of data without explicit data subject consent in some special cases, one of which may apply when performing non interventional clinical research: scientific research purposes. To be lawful, the processing of special categories of personal data for scientific research purposes must be subject, however, to appropriate safeguards (e.g. de-identification techniques), adapted to the level of risks for the data subjects. The *"safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"* described in Article 89 must be addressed by the sponsor.

3.1.2 In a nutshell

The explicit consent of the data subject constitutes the lawful criteria for the processing of subject's data usually collected in clinical trials.

Special attention must be placed on the legislation of Member States where patients are located, to ensure the explicit consent applies to every type of data collected, especially to genetic data if required by the protocol.

The characteristic of the written informed consent in ICH E6 GCP is in line with the written informed consent in GDPR.

For clinical research projects not based on informed consent (for example observational studies), the sponsor must apply the appropriate safeguards according to the level of risks incurred for the data subjects, which may imply data de-identification, according to Article 89 *"Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"*.

3.2 Data protection principles

In comparison to the Data Protection Directive, the GDPR adds a new principle: accountability, and strengthens the principles of transparency, data confidentiality and integrity.

The accountability principle introduces responsibilities that must be endorsed by both the controller AND the processors. This will be detailed in sections 4, 5 and 6 of this document. As part of these responsibilities, the security of processing defined in Article 32 of the GDPR is addressing the requirements that must be met in order to fulfil the data confidentiality and integrity principle.

The transparency principle defines the information that must be provided to the data subjects (for instance, whether *"the controller intends to transfer personal data to a third country"*). This must be considered as part of the informed consent form for clinical trials, or as part of the information provided to the persons participating in studies not based on consent (e.g. observational studies).

3.3 Rights of the data subject

The controller must act on the request of the data subject for exercising his or her rights. A summary of these rights is included here, for more detail see the GDPR itself.

In clinical trials, the primary point of contact for the data subject who wants to exercise his or her rights is defined as the investigator, who plays in this perspective the role of a joint-controller[5]. The investigator interacts with the sponsor (the controller) to ensure that the requests from the data subjects are answered appropriately.

3.3.1 Right of access

The data subject has the right to obtain from the controller:

- confirmation as to whether or not personal data concerning him or her are being processed
- access to the personal data if it is being processed, including metadata as defined in the regulation (such as the purpose of the processing, special categories of personal data involved, etc.)

3.3.2 Right to rectification

The data subject has the right to obtain from the controller rectification of inaccurate data concerning him or her, and that *"without undue delay and in any event within one month of receipt of the request"* (Article 12.3).

3.3.3 Right to erasure

This is a new right added by GDPR, also known as "the right to be forgotten", the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. Without undue delay is defined as being within one month of the receipt of the request.

One important restriction to this right for clinical research is:

- The paragraph does not apply if processing is necessary for scientific research purposes.

This means that clinical trials can retain their data for the full archive period as specified by ICH GCP and local regulations even if the data subject requests erasure of the data.

3.3.4 Right to restriction of processing

The data subject has the right to obtain from the controller restriction of processing (including erasure) when disputes arise concerning the collection and processing of the personal data.

3.3.5 Right to data portability

This is a new right added by GDPR. The data subject has the right to receive the personal data which he or she has provided to a controller in a structured, commonly used and machine-readable format with the aim of transmitting those data to another controller without hindrance.

For data collected in clinical research, this right is more likely to be exercised at the level of the data subject's medical file, rather than the data collected as part of the sponsor CRFs. In the former, the request would be addressed by the hospital (site). In the later, the site transfer eCRF functionality in Viedoc, as well as the use of internationally adopted data standards (CDISC: Clinical Data Interchange Standards Consortium), enables the easy transfer of the subject's data from one site to another site.

[5]Opinion 1/2010 on the concepts of "controller" and "processor" - Article 29 Data Protection Working Party - Adopted on 16 February 2010 / 00264/10/EN WP 169.

3.3.6 Right to object

When personal data are processed for scientific research purposes (e.g. clinical research) the data subject has the right to object at any time to the processing of their personal data.

3.3.7 Automated individual decision making

The data subject has the right not to be subject to a decision based solely on automated processing. However, it is possible to circumvent this right by explicitly including information about the automated processing and a data subject consent in the informed consent. Decisions based solely on automated processing are not common in clinical trials for drugs, but may happen in the case of medical devices.

4 Scenarios

To illuminate the different cases that exist for users of Viedoc, the following scenarios have been defined that cover typical Viedoc studies, sponsors and CROs/vendors.

When changes are made during the course of the trial (for example a site within the EU is added to an ongoing trial that was not in the EU before that) then GDPR becomes applicable as described below, and not just for the data subjects at that site.

4.1 Data Subjects in the EU

If the clinical trial includes data subjects within the EU, then the GDPR applies in its entirety. This applies irrespective of where the sponsor and CROs/vendors are located, where the data processing is performed or where the data submission is planned.

If a sponsor not based in the EU is processing data from data subjects within the EU then they must nominate in writing a representative within the EU who fulfils their responsibilities with regards to GDPR.

Note that this applies even if the data subjects are not EU citizens, if their information is collected while they are within the EU.

4.2 Sponsor in the EU

If the sponsor for the clinical trial is based in the EU then the GDPR applies to the data processing activities, even if the processing itself is not performed within the EU and even if there are no data subjects within the EU.

4.3 Sponsor not in the EU

A sponsor not based in the EU should however carefully assess whether they fulfil the following criteria:

- If they have offices in the EU involved in some aspects of the clinical trial (e.g. a central data management organisation and/or system managed from a EU based establishment), then the sponsor may be considered as established in the EU and the GDPR would apply.

- If the clinical trial data is intended to support a market authorisation filing in the EU, then it has to be considered that there is a data processing activity taking place in Europe for the purpose of the data submission. The GDPR may therefore apply.
- If a full service CRO established in the EU, is being delegated the definition of the purpose of the clinical trial, and, as such, qualifies as a joint-controller, then the GDPR would apply even if the sponsor is not located in the EU.

A sponsor cannot avoid GDPR simply by not being based in the EU. It must perform a legal assessment, based on the specific context of its activities and territorial business and organisation, in order to determine whether the GDPR applies to the data processing activities of a given clinical trial.

4.4 Only PCG Solutions in the EU

If the sponsor, CRO, sites, subjects and data submission are all outside of the EU then the only connection between the clinical trial and the EU is the use of Viedoc, as PCG Solutions is based in the EU.

GDPR does apply to PCG Solutions and Viedoc, but only by the amount represented by the degree of responsibility PCG Solutions has for data processing within the trial. Note that this will normally not be controversial, as PCG Solutions have many customers within the EU and must fulfil the requirements in GDPR for those customers.

In this case GDPR does NOT apply to the sponsor or the CRO for the clinical trial. The sponsor should however inform PCG Solutions concerning the data privacy regulations that they are expected to follow with respect to their location and the location of their partners. Also, if this status should change during the trial, then PCG Solutions should be notified.

5 PCG Solutions Responsibilities and Obligations

PCG Solutions is a *"Processor"* as defined in GDPR. There are general responsibilities and obligations defined as part of a data processor agreement by GDPR that PCG Solutions fulfil, such as the existence of contracts defining the exact nature of the work delegated to PCG Solutions by the sponsor, that are also requirements in ICH E6 GCP. Another example is Article 31, which requires the controller and the processor to cooperate with the supervising authority – something which is already required by ICH E6 GCP. These obligations are considered to be already clear (as they are also required by Clinical Research authorities) and in the interest of brevity they are not discussed here.

There are however other responsibilities and obligations that are not as obviously governed by present clinical trial regulations, even if they could be considered self-apparent. How PCG Solutions complies with these is described below.

PCG Solutions has one of four roles in clinical trials, but the differences in responsibilities and obligations between the roles is small. First the responsibilities and obligations that always apply (the majority) are described, and then the variations are described per role below that.

The following obligations as defined by GDPR are of special interest to the services provided by PCG Solutions:

Article of GDPR	Obligation
Article 28.2	The processor shall not engage another processor without prior specific or general written authorisation of the controller
Article 28.3g	The processor deletes or returns all the personal data to the controller after the end of the provision of services relating to processing
Article 28.4	Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract … shall be imposed on that other processor
Article 29	The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller
Article 30.2	Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller
Article 32.1	The processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk
Article 33.2	The processor shall notify the controller without undue delay after becoming aware of a personal data breach
Article 37	Designation of the data protection officer

5.1.1 Article 28.2 – Engaging another processor

PCG solutions uses suppliers for study setup and for user and site setup services. The names of these suppliers are included in the standard contracts between the controller and PCG Solutions, and are authorised by the controller when they first contract PCG Solutions.

If these suppliers should change then PCG Solutions will gain the authorisation of all affected customers (customers whose trial will use the services provided by the new suppliers).

5.1.2 Article 28.3g – Returning the data at the end of the trial

What to do at the end of the trial is defined in the contract between the controller and PCG Solutions. PCG Solutions offers data archiving services that are built upon extending user access to the data in Viedoc. PCG Solutions performs no other services than storage of the data.

The sites download archive copies of their data from Viedoc. Once all sites have downloaded their data, the controller initiates deletion of the data from Viedoc.

5.1.3 Article 28.4 – Obligations of contracted third parties

Contracts with third parties should be compliant with the requirements of article 28.3 of GDPR. PCG Solutions covers this in their standard suite of contracts, or, if the customer wishes to use their own contracts, then this must be included.

5.1.4 Article 29 – Only process data on the instructions of the controller

This varies depending on the role PCG Solutions has in the trial, and is described in the following sections.

5.1.5 Article 30.2 –Record of processing activities

GDPR requests that specific information be recorded, this information includes:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, the controller's or the processor's representative and the data protection officer (if applicable)
- the categories of processing carried out on behalf of each controller
- transfers of data to third countries and international organisations
- a general description of the technical and organisational security measures

All the information requested by GDPR is included in contracts between PCG Solutions and the controller(s).

5.1.6 Article 32.1 – Level of security

The security measures employed by PCG Solutions are described in the standard Service Level Agreement (SLA) which is appended to the contract between the controller and PCG Solutions.

It includes (but is not limited to): access rights control, data encryption means, redundant storage media and servers meant to ensure availability and continuity of service, a backup strategy meant to ensure a rapid recovery in case of any physical or technical incident, a constant monitoring of production servers, penetration testing and vulnerability scan, etc.

5.1.7 Article 33.2 – Personal data breach

It is the responsibility of all personnel at PCG Solutions to inform the management immediately of any suspected fraud or misconduct (including personal data breach) connected with a clinical trial.

The CEO is then responsible for swiftly informing the controller and coming to an agreement on actions to be taken and to make an action plan. This includes agreement on responsibility for communications with the authorities.

This process is detailed in PCG Solutions SOPs.

5.1.8 Article 37 – Designation of the data protection officer

PCG Solutions has a designated data protection officer.

5.2 PCG Solutions provide Viedoc and no other services

Sponsor (overall responsibility for the trial)													
Medical Writing		**Project Management**		**Monitoring**		**Data Management**		**Biostatistics**		**Medical Affairs**		**Trial Sites**	
Study Protocol	Study Report	Submission	Oversight	IMP	Data Review	Data Capture / PRO	Data Integrity	Safety Endpoints	Efficacy Endpoints	SAE Reports	Patient Safety	Trial Setup	Helpdesk

For many of our customers the sole responsibility that PCG Solutions has within a clinical trial is the provision of Viedoc as an eCRF solution used by the trial.

PCG Solutions is still a “Processor” as defined in GDPR, as Viedoc is used to store clinical trial data. This storage includes even structuring, retrieval and consolidation of the data which are all forms of automated processing.

When storing data in Viedoc the following obligations as defined by GDPR are of relevance to the service provided by PCG Solutions:

5.2.1 Article 29 – Only process data on the instructions of the controller

PCG Solutions personnel has no access to the data or the trial when storage is the only service provided.

5.3 PCG Solutions provide Viedoc and trial setup services

Sponsor (overall responsibility for the trial)													
Medical Writing		**Project Management**		**Monitoring**		**Data Management**		**Biostatistics**		**Medical Affairs**		**Trial Sites**	
Study Protocol	Study Report	Submission	Oversight	IMP	Data Review	Data Capture / PRO	Data Integrity	Safety Endpoints	Efficacy Endpoints	SAE Reports	Patient Safety	Trial Setup	Helpdesk

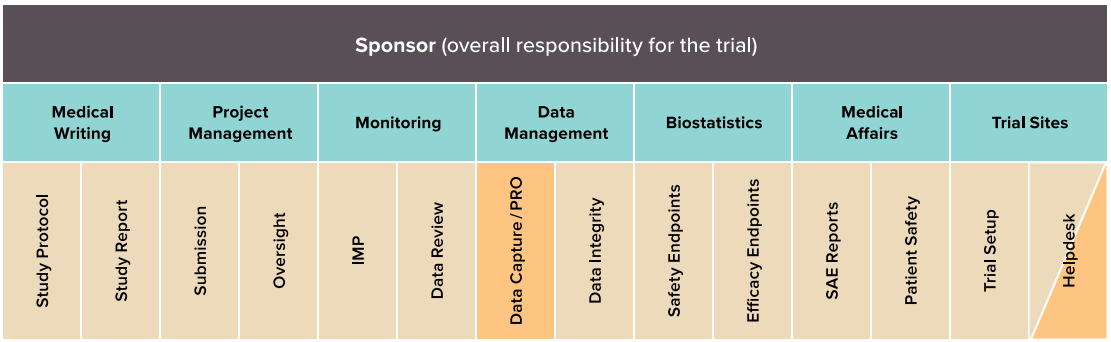
For many customers PCG Solutions also provides trial setup services, either for their first few Viedoc studies before a customer assumes setup responsibilities themselves, or for all their Viedoc studies.

When storing data in Viedoc and performing trial setup services the following obligations as defined by GDPR are of relevance to the service provided by PCG Solutions:

5.3.1 Article 29 – Only process data on the instructions of the controller

PCG Solutions personnel has access to the trial in order to perform the trial setup. The sponsor (controller) can remove the access that PCG Solutions personnel has to the trial at any time of their choosing, and PCG Solutions personnel will not be able to access the trial until the sponsor (controller) grants them access again.

5.4 PCG Solutions provide Viedoc and user management services for Viedoc



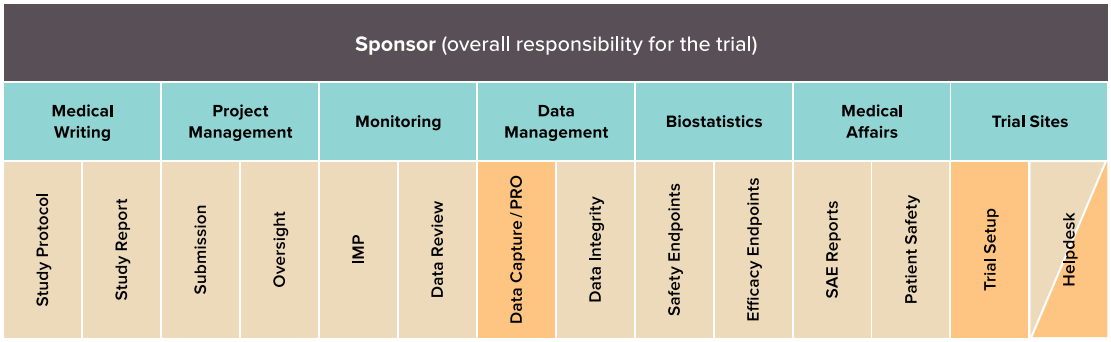
For many customers PCG Solutions also provides user management services for their trial in Viedoc, that is the addition of sites and users to their Viedoc trial.

When storing data in Viedoc and providing user management services the following obligations as defined by GDPR are of relevance to the service provided by PCG Solutions:

5.4.1 Article 29 – Only process data on the instructions of the controller

PCG Solutions personnel (or contracted third party personnel) have access to the trial in order to add sites and users. Sites and users are added only on the instruction of the sponsor (controller). The sponsor (controller) can remove the access that PCG Solutions personnel has to the trial at any time of their choosing, and PCG Solutions personnel will not be able to access the trial until the sponsor (controller) grants them access again.

5.5 PCG Solutions provide Viedoc, trial setup and user management services for Viedoc



For many of our customers PCG Solutions also provides both trial setup services and user management services for their trial in Viedoc. This is a combination of the obligations for the previous two cases, as described below:

When storing data in Viedoc, performing trial setup and providing user management services, the following obligations as defined by GDPR are of relevance to the service provided by PCG Solutions:

5.5.1 Article 29 – Only process data on the instructions of the controller

PCG Solutions personnel (or contracted third party personnel) has access to the trial in order to perform the trial setup and to add sites and users. Sites and users are added only on the instruction of the sponsor (controller). The sponsor (controller) can remove the access that PCG Solutions personnel has to the trial at any time of their choosing, and PCG Solutions personnel will not be able to access the trial until the sponsor (controller) grants them access again.

6 Sponsor Responsibilities and Obligations ("Controller")

6.1 Scenario 4.4, and scenario 4.3 where the GDPR does not apply to the sponsor after legal assessment:

- The sponsor should conform to the data protection legislation that applies according to the country where the sponsor and the data subjects are located. PCG Solutions should be made aware of the legislation that applies as well as of the specific requirements it imposes on data processors.
- The contract set with PCG Solutions, should however remain compliant to the requirements set by Article 28.3 of the GDPR, in order to enable PCG Solutions to fulfil its legal requirements as a European company. It has to be noted that these requirements constitute a guarantee regarding the fulfilment of some aspects of GCP by PCG Solutions (especially concerning the security and integrity of data, which is required by GCP in a similar manner as GDPR). They are therefore not expected to be contradictory or overcomplicated for the sponsor.

6.2 Scenarios 4.1, 4.2, and 4.3 when the GDPR applies to the sponsor as a conclusion of the legal assessment:

In addition to the obligations defined in sections 3.1, 3.2 and 3.3 for the controller, the sponsor has an accountability level which involves additional responsibilities and obligations, as follows:

Article of GDPR	Obligation
Article 24	Responsibility of the controller: (1) implement appropriate technical and organisational measures; (2) implement appropriate data protection policies; (3) adherence to approved codes of conduct or approved certification mechanisms may be used
Article 25	Privacy by design and by default
Article 26	Joint controllers
Article 28.1	The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures
Article 29	Any person acting under the authority of the controller, who has access to personal data, shall not process those data except on instructions from the controller
Article 30.1	Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility
Article 31	Cooperation with the supervisory authority
Article 32	Security of processing: (1) the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk; (4) The controller take steps to ensure that any natural person acting under the authority of the controller who has access to personal data does not process them except on instructions from the controller
Article 33	(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority. (5) The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article
Article 34	Communication of a personal data breach to the data subject
Article 35	Data protection impact assessment
Article 36	Prior consultation of supervisory authority
Article 37	Designation of the data protection officer

The sponsor should ensure appropriate organisational and technical measures are implemented in every stage of the clinical trial, and by every party, in a proportionate manner to the risks represented for the data subjects by the processing of his/her personal data.

6.2.1 Implement appropriate data protection policies

The sponsor shall consider if it is appropriate to implement data protection policies in order to frame the appropriate organisational and technical measures at companywide level.

6.2.2 Data protection by design and by default

In the case of clinical trials, pseudonymisation, consistency of the Case Report Forms and of the statistical analysis to the approved Study Protocol, the Good Clinical Data Management Principles and the Statistical Analysis Plan are standard practices, defined as part of the ICH E6 GCP, and consistent with a "privacy by design" and "privacy by default" approach in clinical trials.

By default, the personal data must be accessible only according to the role of each person allowed to process the study data. This is also consistent with the principles set by GCP for access to the clinical trial records.

The sponsor must ensure that these principles are fulfilled by contract with all the processors.

6.2.3 Joint controllers

In addition to the sponsor, other parties may be joint controllers by being involved in the definition of the purposes and means of processing. These could include a principal investigator and/or a full service CRO (e.g. when it is delegated a full clinical development plan). The sponsor should ensure that the respective responsibilities for compliance with the obligations under the GDPR are defined in a transparent manner. The arrangement may designate a contact point for data subjects, which for a clinical trial will be the investigator.

6.2.4 Conduct a data protection impact assessment

Considering that special categories of personal data are usually largely processed in clinical research studies, the sponsor should consider performing a data protection impact assessment before the beginning of each study. This is required as per Article 35 of the GDPR.

6.2.5 Consult the supervisory authority

When the above-mentioned data protection impact assessment *"indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk"*, the sponsor should consult the supervisory authority prior to processing the data, according to Article 36 of the GDPR.

6.2.6 Notification of a personal data breach

It is the responsibility of the sponsor to notify a personal data breach, without undue delay, to the competent supervisory authority. Where feasible, the delay should not exceed 72 hours after having become aware of it. If the delay happens to be longer, the notification should be accompanied by reasons for the delay.

If the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, it may not be notified, but should be documented, including its effects and the remedial action taken. Such documentation is requested by the supervisory authority to verify compliance with Article 33 of the GDPR.

In addition, according to Article 34, *"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay"*. The communication should be made in clear and plain language and contain the following information:

- the name and contact details of the data protection officer or other contact point where more information can be obtained
- the likely consequences of the personal data breach
- the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

For a clinical trial the communication can be handled by the investigator based on the information gathered and provided by the sponsor, since the sponsor does not have direct access to the data subject names and the investigator has the medical relationship with the study subject.

6.2.7 Designation of a data protection officer

The sponsor should have a designated data protection officer, and the name and contact information from this person should be communicated as part of the contractual information provided to the CROs.

7 CRO and Vendors Responsibilities and Obligations ("Processor")

7.1 In scenario 4.4, and scenario 4.3 where the GDPR does not apply to the sponsor after legal assessment

Any CRO located in the EU will have to comply to GDPR to the degree of their responsibility as a processor.

7.2 In scenarios 4.1, 4.2, and 4.3 when the GDPR applies to the sponsor as a conclusion of the legal assessment:

The sponsor, as controller, should ensure that each processor fulfils its responsibilities and obligations in compliance with GDPR, and according to the specific services engagement contracted.

The table below provides a summary view of the obligations from each party.

Obligation	Sponsor	PCG Solutions	CRO	Vendors
Implement appropriate technical and organisational measures	✓	✓	✓	✓
Implement appropriate data protection policies	✓			
Designate a Data Protection Officer	✓	✓	✓	✓
Implement privacy by design	✓			
Implement privacy by default	✓			
Designate in writing a representative in the Union if established outside EU	✓	NA	✓	✓
Conduct a data protection impact assessment	✓			
Consult the supervisory authority	✓			
Maintain records of processing activities	✓	✓	✓	✓
Cooperate with the supervisory authority	✓	✓	✓	✓
Notify a personal data breach	To the supervisory authority	To the sponsor	To the sponsor	To the sponsor
Communicate a personal data breach to the data subject	To the sponsor			
Impose sufficient guarantees when engaging a processor	✓	✓	✓	✓
Setup a processor contract compliant with GDPR requirements	✓	✓	✓	✓
Delete or return data to sponsor at the end of contract		✓	✓	✓

According to article 32: *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".*

The implementation of appropriate technical and organisational measures is defined by GDPR as a joint accountability for the controller and the processors (the sponsor and the CROs and Vendors in clinical trials). These measures should be appropriate and proportionate to the type of activities that are delegated by the sponsor.

8 CONCLUSION & KEY TAKEWAYS

GDPR requires companies to have control of their information management and its governance. In the Clinical Research sector this has long been vital for the success of clinical drug development, so it is not a pivotal change to how companies work. Instead companies need to ensure that their internal policies are aligned with the regulations defined in GDPR.

PCG Solutions customers should take the following key takeaways with them after having read this white paper:

1. For customers who are not active within the EU, not offering products or services to anyone within the EU and not intending to submit their products for approval by the EU Regulatory Authorities then it is sufficient to know that PCG Solutions will follow GDPR even when working with you, and that this should be seen as PCG Solutions following a best practice for data privacy.
2. Customers who are active within the EU, who are offering products and/or services to citizens of the EU or who are intending to submit their products for approval by the EU Regulatory Authorities will need to prepare for GDPR. This white paper aims at offering some guidance to the necessary preparations to be made. It is however up to each company to draw up their own action plan, making allowances for their specific context when preparing for GDPR.
3. The sanctions imposed are high if GDPR is violated. Preparing for GDPR is a risk management exercise.