WHITE PAPER

Five crucial steps towards a GDPR proof clinical trial

DPO Consultancy
Privacy Experts for Life Sciences

MARCH 2024

Dounia van de Weerd-Skalli

Introduction

Clinical trials are of great importance to the public interest. New tests and treatments are developed through various types of research studies, and their effects on human health are evaluated. Individuals volunteer to take part in clinical trials to test medical interventions. This includes people of all different ages, which may also include children. In many different aspects clinical trials are carefully designed, reviewed and completed. Before the clinical trial can start, the study protocol needs to be approved by the relevant committee. The committee will also take into account the right to respect the physical and mental integrity as a fundamental right[1] for all persons located in the European Union (EU). This also applies to the right to the protection of personal data.[2]

Needless to say, the personal data that is involved in clinical trials are very sensitive since it concerns an individual's health. When this data falls into the wrong hands, this may lead to major and severe negative impacts on an individual's life. Logically, organizations have to take all the appropriate measures to be able to securely handle this data.

Besides the law obligations that aim to protect the individual's rights, there is also a legal basis needed for processing personal data when organizing clinical trials. This legal basis, also referred to as a lawful ground, is provided by the General Data Protection Regulation (GDPR).[3] The GDPR came into force on the 25th of May 2018, and aims to ensure the protection of individuals with regard to the processing of personal data, and to harmonize rules on the free movement of such data. It provides different lawful grounds for the processing of personal data. One of the most familiar ones is consent. Professionals in the life sciences industry often tend to confuse informed consent with GDPR-consent.These are in fact two very different types of consent.

Many life sciences organizations struggle with organizing GDPR proof clinical trials. The GDPR has unfortunately developed a very negative image for hindering organizations from doing their business. This white paper aims to show how to interpret and apply the GDPR in such a proper and efficient way, that it may benefit your organization. When the GDPR is properly applied, and you have all measures in place, you are allowed to easily transfer, process, handle, collect and store data in the most efficient way possible. And also important, without having to worry about negative consequences, like receiving fines from the data protection authority, civil claims of individuals, or reputational damage of your organization. If the steps described in the next chapters are taken into account, you have taken a big step towards a GDPR proof clinical trial.

1 Article 3(1) Charter of Fundamental Rights of the EU (C 326/393).
2 Article 8(1) Charter of Fundamental Rights of the EU (C 326/393).
3 General Data Protection Regulation (EU) 2016/679 (GDPR).

1. Determine your role in the data processing

The first step is to determine your role in data processing activities of a clinical trial. Different roles are distributed over the various parties involved. Distinguishing the roles is of great importance, since each one has its own obligations and responsibilities.

Controller

In clinical trials the sponsor is always a controller. The sponsor determines for what purposes the data is processed, and also how it is processed. In the GDPR this is referred to as: *"determining the purposes and means of the processing of personal data"*.[4]

Joint-controllership

There might be joint-controllership if the sponsor determines the purposes and means of processing the data jointly with another party.[5] This party might be a Clinical Research Organization (CRO) that has been delegated a full clinical development plan.

Processor

Whenever the processing of data is carried out on behalf of a controller, that party is considered to be a processor.[6] In clinical trials this is often the CRO or vendors like hospitals. Both CROs and vendors are acting upon the reasonable instructions of the sponsor.

A processor may also engage with another vendor involved in the same processing activity. This other party is referred to as the *sub-processor*. For instance, this may be laboratories used for sample analysis or cloud storage software providers that deliver tools to process the personal data.

Responsibilities and obligations

It is important to understand that each role has different responsibilities and obligations. Many organizations lose sight on who should perform what task, and tend to get confused. To provide insight in all the GDPR-tasks per role, a complete overview of the responsibilities and obligations is provided on the next page (Table 1). Luckily, fulfilling many of these responsibilities and obligations can become more manageable by the designation of a data protection officer (DPO).

4 Article 4(7) GDPR.
5 Article 26 GDPR.
6 Article 28(1) GDPR.

Table 1: Overview of the roles and obligations per role in a clinical trial [7]

Responsibilities and obligations	Controller: Sponsor	Processor: CRO or Vendor
Implement appropriate technical and organizational measures while processing personal data.	✓	✓
Implement the appropriate data protection policy.	✓	✓
Appoint a data protection officer (DPO)..	✓	✓
Adhere and apply the principles of Privacy by Design and Privacy by Default.	✓	
Designate a representative in the European Union in writing if she is established outside the EU.	✓	✓
Performing a data protection impact assessment (DPIA).	✓	
Consult the supervisory authority when needed.	✓	
Maintain a record of processing activities.	✓	✓
Cooperate with the supervisory authority.	✓	✓
Report a personal data breach.	✓ *To the supervisory authority*	✓ *To the sponsor*
Communicate a data breach to the individuals involved.	✓	✓ *Only CRO's*
Only conduct business with other parties (processors) who offer sufficient guarantees by taking appropriate technical and organizational measures.	✓	✓
Conclude a data processing agreement (DPA) with each processor that meets all the GDPR requirements.	✓	✓
Delete or return data to sponsor at the end of the contract.	✓	✓
Ensure compliance with approved codes of conduct or recognized certification mechanisms.	✓	
Make sure that anyone acting under the authority of the controller and who has access to personal data may not process that data, except on instructions from the controller.	✓	
Determine joint responsibility in joint-controllership with another party if they jointly determine the purposes and means of processing the personal data.	✓	

7 A. Yeomans & I. Abousahl, 'Preparing for the EU GDPR in Clinical and Biomedical Research', *PCG 2017 Solutions AB*, p. 22-23.

"All the parties involved in clinical trials should be aware of their obligations and responsibilities under the GDPR"

As the table shows both controllers and processors need to appoint a DPO, it is an important side note that this is done externally rather than internally. Reasons such as guaranteeing the independent position of a DPO plays a major role in this case. However, this complex topic deserves a white paper of its own and will not be further elaborated on for now.

All the parties involved in clinical trials should be aware of their obligations and responsibilities under the GDPR. Although many responsibilities and obligations align between both roles, there are also some differences to be found.

2. Assess what personal data you process and how to protect it

Once you have determined your role and accompanying responsibilities you are able to focus on what personal data you process. This is necessary because of the fact that there are different types of data that each require different levels of protection and rules regarding the processing activity. But first, it is important to understand what data qualifies as personal data and what appropriate measures you should take.

The definition of personal data

The GDPR states that personal data means: "any information relating to an identified or identifiable natural person".[8] This definition of personal data is broad, and it is widely applicable due to the possibility of the direct and indirect identification of an individual. Obviously, personal data is someone's name, address, telephone number, etc. However, it may also include other information that makes it possible to identify an individual in a certain context. In clinical trials a certain clinical site, diagnosis and results may be known. When you have access to a database that contains such information, and which can be linked to a particular individual, identification is easy. Study data from a clinical trial is thus considered to be personal data.

Types of personal data

The GDPR distinguishes two types of personal data: regular and special personal data. Special categories of personal data is listed, and is including, but not limited, to data revealing:

- Genetic data
- Biometric data for the purpose of uniquely identifying an individual
- Health data[9]

Processing special personal data is in principle prohibited, except if a specific exception applies such as explicit consent.[10] All other personal data is considered to be regular personal data.

In clinical trials both regular and special data are being processed. One should think of a trial participant's name and address, results from

8 Article 4(1) GDPR.
9 Article 9(1) GDPR.
10 Article 9(2) GDPR.

"Needless to say, the impact of misuse of special data can be much bigger, compared to regular data"

physical evaluations, measurements of vital signs, and samples of the participant (which may be studied and validated as biomarkers). It is a mixture of genetic data, health data, and regular data.

As stated on the previous page, an important obligation of both the controller and processor is to take appropriate measures to protect the data. Needless to say, the impact of misuse of special data can be much bigger, compared to regular data. This is an important reason why the bar is set higher for special data when it comes to implementing protection measures. The GDPR has included some standard security measures as a basis, like pseudonymization.

Pseudonymization

One of the measures controllers and processors should at least take according to the GDPR, is the pseudonymization of data. This means that personal identifiers are replaced by one or more artificial identifiers. These artificial identifiers make it impossible to directly identify an individual. However, this 'coding' can be reversed, meaning that the identification of an individual is enabled again by de-identifying a coding. The GDPR is *fully* applicable to pseudonymized data, because it is still classified as personal data. It remains possible to identify an individual.

Anonymization

Unfortunately, people often tend to confuse pseudonymization with anonymization. This is, however, something very different. Anonymization irreversibly prevents re-identification and allows for a much wider use of the information. An important consequence of anonymized data is that the GDPR does not apply. This is very convenient of course. However, even though anonymization seems technically possible, it is legally almost impossible. This is due to the fact that identification is usually a possibility by combining data sets. This will not be further elaborated on in this paper, because of its complexity. But one should take note that anonymization is not a realistic option for clinical trials since health data, like DNA, may lead to an identification of an individual.[11]

Now that the different types of personal data of the GDPR are clear, one should keep in mind that each type of personal data should be protected in an appropriate way. Regular data requires less protection than special data. In clinical trials there is always health data involved, which qualifies as special data. This means that this data should be protected accordingly by implementing adequate measures, like pseudonymization.

11 P. Quinn & L. Quinn, 'Big genetic data and its big data protection challenges', *Computer Law & Security Review* 34 2018, 1000–1018, p. 1002-1004.

3. Determine the purpose of data processing within clinical trials

When the study's protocol is completed, it is clear what the purpose of the trial will be. However, the protocol does not explain what the purpose is of data processing within clinical trials. Therefore, the next step should be to identify what the purpose is of the data processing. The purpose is the core of a processing activity. Many aspects depend on the purpose, such as what personal data you need to achieve the purpose in a processing activity, and for how long you need to store it.

The Clinical Trial Regulation (CTR)[12], which is effective from 31 January 2022, offers a great starting point for deciding which purpose applies to your clinical trial. The CTR's general aim is to achieve a harmonized internal market, just like the GDPR, specifically for clinical trials and medicinal products for human use.[13] The European Data Protection Board (EDPB)[14] used this aim to narrow down the scope to two relevant data processing purposes in clinical trials in her recent Opinion[15]:

1. **For the protection of health**
   To protect health, clinical trials include data processing operations for reliability and safety related purposes. Standards of quality and safety for medicinal products are set by generating robust and reliable data. This is often required by a legal obligation, such as articles 41 to 43 of the CTR, related to the performance of safety reporting. Another example is article 58 CTR, which mandates the archiving of the clinical trial master file and the medical files of individuals, to be kept for at least 25 years. One should bear in mind that countries may implement the CTR into national legislation, which allows countries to deviate in some topics within the scope of the CTR.
2. **For scientific research**
   Clinical trials also include data processing operations that are purely related to research activities. Eventually, the purpose is to generate the study data that is needed for your study.

All data processing activities within a clinical trial can be categorized in these two data processing purposes.

12 Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use (CTR).

13 Recital 82 CTR and Article 3(b) CTR.

14 *The European Data Protection Board (EDPB) is an independent European body. It contributes to the consistent application of data protection rules throughout the EU, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor.*

15 Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)), Adopted on 23 January 2019, p. 4-5.

4. Assess what lawful processing grounds apply to the clinical trial

The next step is to assess which lawful grounds can be used to process personal data. The GDPR provides multiple but limited lawful grounds that you must use as a legal basis. It is therefore important to understand which lawful ground may apply to your specific process. The relevant grounds will be further discussed based on each purpose of processing activities in clinical trials. But first, it is good to understand which lawful processing grounds are provided in the GDPR.

Lawful processing grounds based on the GDPR

The GDPR includes lawful processing grounds for both regular and special personal data. In order to process both types of personal data there are two relevant articles in the GDPR, one devoted to regular personal data, and another article devoted to special personal data. These two articles both work in conjunction with one another. To have a basic understanding of what the relevant lawful grounds for clinical trials entail, the lawful grounds are briefly described in Table 2 on the next page.

Table 2: Lawful processing grounds

Lawful processing grounds regular data	In conjunction with	Lawful processing grounds special data
Article 6(1)(a) GDPR: An individual might give consent to processing personal data for one or more specific purposes.		Article 9(2)(a) GDPR: An individual might give explicit consent to process personal data for one or more specific purposes.
Article 6(1)(c) GDPR: Personal data may be processed if it is necessary for compliance with a legal obligation.		Article 9(2)(i) GDPR: When the processing of personal data is necessary for reasons of public interest in the area of public health.
Article 6(1)(e) GDPR: When processing is necessary for the performance of a task carried out in the public interest or to exercise official authority.		Article 9(2)(j) GDPR: In case processing personal data is necessary for purposes of archiving in the public interest, scientific or historical research and statistics.
Article 6(1)(f) GDPR: Processing personal data is allowed in case the legitimate interests of the organization overrides the interests of the individual.		

Every clinical trial must process personal data based on the lawful processing grounds described above. Because of the fact that clinical trials consist of a combination of different types of data, both regular and special lawful grounds will be used in conjunction with each other.

Now we will zoom in on each purpose of data processing activities to understand what lawful grounds apply to process personal data in a GDPR compliant manner.

Processing activities for the protection of health

Many national and international laws determine that every clinical trial should aim for a proper protection of the health of individuals. That is why the following grounds apply:

- **Compliance with a legal obligation**
  Examples of obligations for the protection of health on an international level can be found in Articles 41,43, and 58 of the CTR,

as discussed in the previous chapter. This means that the sponsor and/or investigator are subject to comply with the legal obligations in both international and national law. Consequently, personal data may be processed related to safety reporting or inspection by a national competent authority, or the retention of clinical trial data in accordance with archiving obligations set up by the CTR or national laws.

- **Necessary for reasons of public interest**
  When clinical trials include processing activities for the protection of health, there is only one applicable lawful ground for the processing of regular data, and one applicable ground for special data. Important conditions are that it is prescribed by international or national law, and that it benefits the public interest with regard to public health.

Processing activities for scientific research

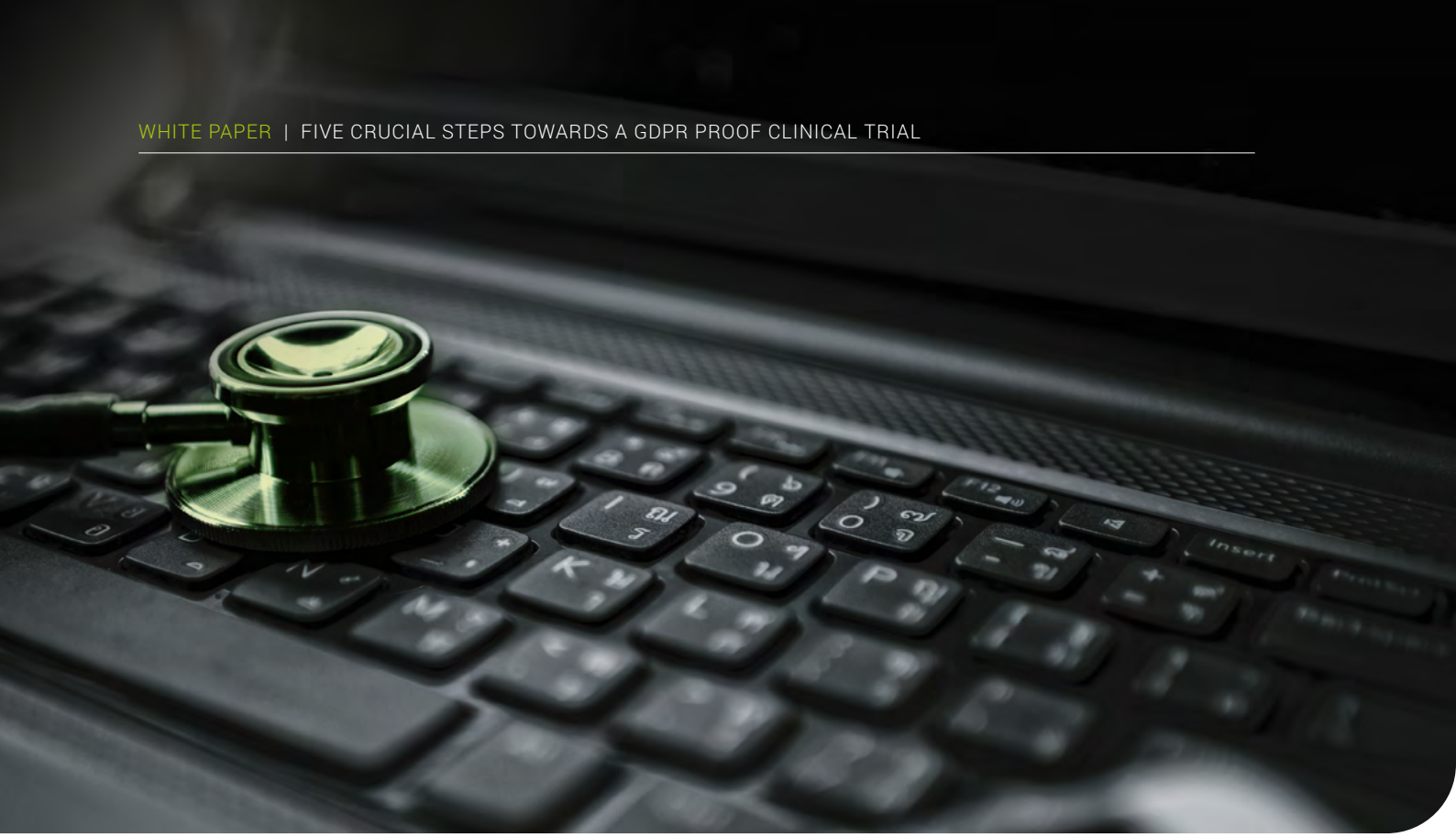
Besides the purpose of compliance with legal obligations for the protection of health in clinical trials, there are also processing operations that purely focus on scientific research itself. Depending on the specific data processing activities and circumstances of the clinical trial. There are two possible variations of lawful grounds which may apply:

- **A task carried out in the public interest**
  This legal ground is a more appropriate lawful ground than GDPR-consent because you do not have to deal with all the strict requirements and conditions of GDPR-consent in this case. Article 6(3) GDPR prescribes that the lawful ground should be further laid down by national laws, and it should also include the specific purpose of the processing activity. This means that conducting clinical trials may directly fall within the mandate, missions and tasks vested in a public authority by national law. Meaning, they may thus be considered as necessary to perform a task carried out in the public interest.[16] It can be concluded that if you are able to use this lawful processing ground it is more appropriate and convenient to use.

- **The legitimate interests in conjunction with reasons of public interest in public health, and necessary for purposes of archiving in the public interest, scientific or historical research or statistics**
  For all other situations in clinical trials, in which you cannot use the previous lawful ground on carrying out a task in the public interest, you may use the legitimate interests ground[17]. This is the most flexi- ble ground to use. However, you always have to assess the interests of both the organization, and the individuals involved. This

16 *Recital 45 GDPR states that a law may be sufficient to use as a basis for several processing activities based on the performance of a task carried out in the public interest.*

17 Article 9(2)(i) Legitimate interests in conjunction with reasons of public interest in public health, and necessary for purposes in archiving in the public interest, scientific or historical research and statistics.



part is done by performing a legitimate interest assessment. This assess- ment helps you to:

- Identify a legitimate interest.
- Demonstrate that processing the data is necessary to achieve the specific purpose.
- To balance your interests against the individual's interests, rights and freedoms.

If the outcome of the assessment shows that your interests override the interests of the individual, you may use the legitimate interest ground because you indeed have a legitimate interest.

When it comes to special personal data, there may be two appropriate lawful grounds. This concerns processing activities necessary for reasons of public interest in the area of public health, or processing activities necessary for purposes of archiving, in the public interest, scientific or historical research and statistics.[18]

- **Is consent considered to be a third lawful ground?**
  A third lawful ground which is often being used is *regular GDPR-consent* in conjunction with *explicit GDPR-consent*. This should not be confused with informed consent. Although this is a common lawful ground to use in clinical trials, and even recommended to use by national Committees, like the Central Committee on Research Involving Human Subjects (CCMO), it is not considered to be a lawful ground.[19] The main reasons for this can be found in the background information section on the next page.

18 *Opinion 06/2014 on the notion of legitimate* interests of the data controller under Article 7 of Directive 95/46/EC adopted on 9 April 2014, WP 217, p. 21-22.

19 Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)), Adopted on 23 January 2019, p. 5-7.

Different definitions of consent

1. Informed consent: informing a patient about the proposed treatment in an understandable and complete manner. *An example: informing a participant in a clinical trial through an informed consent form.*
2. GDPR-consent: providing a lawful ground to process personal data of an individual. *An example: all clinical trials contain special data, such as health data, and therefore need to comply with the requirements of both types of consent (regular and explicit).*
   a. Regular GDPR-consent provides a lawful ground to regular personal data (article 6 GDPR).
   b. Explicit GDPR-consent provides a lawful ground to special data, such as health, genetic, biometric data (article 9 GDPR).

GDPR-consent in conjunction with GDPR-explicit consent

As you have read on the previous page, informed consent and GDPR-consent are often confused with one another in the life sciences industry. To have a reasonable understanding of what the two different types of GDPR-consent are, it is good to elaborate on the differences between informed consent based on the CTR, and consent based on the GDPR.

In the life sciences industry, informed consent[20] is a well-known concept that is widely used. The purpose is to inform the patient in an understandable and complete manner about the proposed treatment in an informed consent form. Unfortunately, in the life sciences industry this type of consent is often confused with GDPR-consent. It is important to understand that the purpose of GDPR-consent is to provide a lawful ground to process personal data, not to inform a patient about the proposed treatment. Therefore, this purpose is very different from the purpose of informed consent.

What is also important to comprehend, is that in order for GDPR-consent to be valid, it must meet other specific conditions in comparison to informed consent. GDPR-consent must be freely given, specific, informed, and unambiguous.[21]

Additionally, in the processing activities of special data, like health data, explicit GDPR-consent is required. This means, that besides meeting all the specific conditions of regular GDPR-consent, an individual should also expressly confirm GDPR-consent in a clear

20 Articles 28-35 CTR.
21 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 7-18.

statement, whether oral or written.[22] Obviously, a written statement in which consent is expressly confirmed, would be the best way to go. In the end, every organization should duly take into account all the requirements of both regular and explicit GDPR-consent, and check if all the conditions for valid consent are met in a particular trial.

Now that you are aware of the different types of GDPR-consent, it may appear this offers a valid lawful ground for processing data in your clinical trial. Unfortunately, this is not the case. In the next section the issues with GDPR-consent will be explained.

"One of the major issues with GDPR-consent in clinical trials is that it is not considered to be *freely given*"

The issues with GDPR-consent

One of the major issues with GDPR-consent in clinical trials is that it is not considered to be *'freely given'*. Freely given means that individuals should have a real choice, and should not feel compelled to consent, or should endure negative consequences if consent is not given. In clinical trials this is nearly impossible since there is a clear imbalance of power between the individual and the sponsor/investigator involved. This is due to the fact that a patient's health may depend significantly on one's participation in a clinical trial.[23] Every party involved in clinical trials should conduct a really thorough assessment of the circumstances before one can rely on GDPR-consent as a lawful processing ground for the purposes of the research activities of a trial.[24] In addition, the CTR addresses these risks also by requiring that the investigator takes into account all the relevant circumstances.[25] Elaborating on the standard included in the CTR, it may therefore be concluded that GDPR-consent may not be considered to be freely given in most clinical trials if:

- An individual is not in a good health condition.
- When individuals belong to a socially or economically disadvantaged group or in any other situation of institutional or hierarchical dependency.[26]

A complicating factor of consent is that one of the fundamental conditions of consent is that it may be *withdrawn*. Also in this case, the withdrawal of informed consent should not be confused with the withdrawal of GDPR-consent. There is a big difference between the two forms. In case informed consent is withdrawn it will not affect activities that are already carried out before the withdrawal,

22 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 20.
23 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 7-13; Recital 43 GDPR.
24 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 6.
25 Recital 31 CTR.
26 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 6.

meaning data already processed before the withdrawal may still be used. Under the GDPR however, individuals may withdraw their GDPR-consent at any given time (Article 7(3)), and all the data is affected. This means there is no exception to keep using the pre-existing data before the withdrawal for scientific research.[27]

As a rule of thumb, all data processing activities based on GDPR-consent remain lawful in accordance with Article 7(3) GDPR. However, the controller should stop all processing activities, and if there is no other lawful processing ground to justify the further retention of the data, all personal data should be deleted (Article 17(1)(b) and (3) GDPR).

The use of GDPR-consent in clinical trials may be only limited to processing activities that are purely related to research activities. Whenever an individual withdraws its consent, it will affect all personal data involved in the research activities related to that particular individual. The only personal data that shall not be affected in this case, is the data that is processed on the basis of legal obligations to which the sponsor/investigator are subject to.

The conclusion can be made that in general GDPR-consent is often wrongly used in the life sciences industry as a lawful processing ground. One should be aware that the other relevant lawful processing grounds are more appropriate and convenient to use in clinical trials.

"GDPR-consent is often wrongly used in the life sciences industry as a lawful processing ground."

27 Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, p. 23-24.

5. Perform a DPIA on high-risk processing activities

Before you start your processing activities, you need to identify the risks involved in the processing activities, with an emphasis on the high-risks. The reason is that you want to mitigate as many risks as possible to prevent negative consequences, like for example being fined by the data protection authority because of a data breach. In order to perform a risk-based assessment, article 35 of the GDPR requires each controller to perform a data protection impact assessment (DPIA) on all high-risk processing activities. In clinical trials this means that a sponsor/ CRO is responsible for performing a DPIA.

Meaning and purpose of a DPIA

Where a processing activity is likely to result in a high risk to the rights and freedoms of individuals, a DPIA is required. It is an instrument to provide insight into what risks are imposed to the individuals, and what measures should be taken to reduce the risks.

It may be however, that there are still high risks remaining to the rights and freedoms of individuals. In that case it may be needed to request a prior consultation with your national data protection authority before the processing activity starts.

Criteria of high-risk processing activities

Article 35 of the GDPR explains some situations that are considered to always be high-risk processing activities. An example is the processing on a large scale of special personal data, like health data.

Besides the examples provided in the GDPR, the European Data Protection Supervisor[28] has also created a list of nine criteria to assess if you deal with a high-risk processing activity. National Data Protection Authorities have elaborated on this list and have created their own list of high-risk processing activities that may include more examples. One should be aware that there are in principle nine criteria

28 *The European Data Protection Supervisor (EDPS) is the EU's independent data protection authority.*

to evaluate if a DPIA is needed, although this might slightly differ between countries.[29]

Responsibility

The controller, the sponsor/CRO, is responsible for performing the DPIA. If there is a designated DPO, the controller must obtain his advice when performing a DPIA. This provides additional assurance that the DPIA provides sufficient insight into the identification of risks, and that appropriate measures are taken to mitigate them.

Now that it has been made clear what a DPIA is, and what it entails, it should be noted that a controller is responsible for performing a proper assessment on risks in processing activities. Clinical trials may include high-risk processing activities for which DPIA's need to be performed. In that case, one should perform a DPIA first.

Are you ready for a GDPR-proof clinical trial?

In the previous chapters you have learned that before conducting a clinical trial, the following steps are crucial in your journey to achieve GDPR compliance:

1. Determine your role in the data processing.
2. Assess what personal data you process and how you protect it.
3. Determine the purpose of data processing within clinical trials.
4. Assess what lawful processing grounds apply to the clinical trial.
5. Perform a DPIA on high-risk processing activities.

These five steps provide a good high-level overview for a GDPR proof clinical trial. There are many steps to take in between, but also once the processing activity has started. GDPR compliance requires consistent and thorough privacy governance within an organization. Designating a DPO is a great start to conduct GDPR proof clinical trials. We, at DPO Consultancy, are experts in data privacy and can provide you the tailored advice and guidance that you may need. It is important to become, but also stay GDPR compliant in the long run.

Does your organization have GDPR-proof clinical trials? To check whether your organization is ready you may fill in the form provided in Annex 1.

29 Decision of the EDPS of 16 July 2019 on DPIA Lists Issued Under Articles ON 39(4) and (5) of Regulation (EU) 2018/1725.

Annex 1

Question	**Answer**
What is your role in the data processing?	Controller/Joint-controller/Processor
What personal data do you process and how do you protect it?	Special category of data/regular personal data Measures taken:
What are the purposes of the data processing activities within your clinical trial?	

Question	**Answer**
What lawful processing grounds apply to your clinical trial?	
What are the most prominent risks in your clinical trial? And how do you mitigate them?	Most prominent risks: Mitigating measures:

DPO Consultancy
Privacy Experts for Life Sciences

Europalaan 28b
5232 BC 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com