CNS 59/2018

Opinion in relation to the consultation of a health center about the agreement in charge of the treatment with the companies that monitor clinical trials

A query from a health center (hereinafter referred to as the Hospital) is presented to the Catalan Data Protection Authority regarding the access by the external monitor of clinical trials to the personal data of the subjects participating in it.

Specifically, the inquiry asks whether access to personal data by the external monitor of clinical trials would be legitimated indirectly by virtue of the information sheet and informed consent signed by the people participating in the trial. In this case, the consultation asks whether the Hospital could no longer require the signature of a contract of treatment manager between the Hospital and the external monitor and whether, in this case, some type of additional safeguard should be established.

Having analyzed the request, which is not accompanied by other documentation, in view of the current applicable regulations, and the report of the Legal Counsel, the following is ruled.

I

(...)

II

The consultation explains that the Hospital carries out clinical trials with medicines in its facilities, regulated by Royal Decree 1090/2015, of December 4, at the request of the promoting entities or companies (hereinafter, the Promoter).

According to the consultation, the Promoter appoints the monitor of the trial, who, in order to perform his functions, must access personal data identified by the subjects of the trial that are under the control of the Hospital. According to the query, the Promoter can appoint an internal monitor (from the Trial Promoter's staff), or an external monitor (hereinafter, External Monitor).

In relation to the appointment of an External Monitor, according to the consultation, "the Hospital requires the signing of a data processing contract between the Hospital and the External Monitor in terms of article 28 of the RGPD."

In this context, the Hospital asks the following questions:

"1.- Could the Hospital understand that the External Monitor's access to the identified personal data of the subjects of the trial under the control of the Hospital is legitimated indirectly by virtue of the HIP/CI that legitimizes direct access of the Promoter to this data?

2.- If the answer to the previous question is affirmative, could the Hospital no longer require the signature of a treatment contract between the Hospital and the External Monitor?

3.-If the answer to the previous question is affirmative, should the Hospital establish some type of additional safeguard before allowing the External Monitor access to personal data under the control of the Hospital?"

III

According to Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection (hereafter, RGPD), personal data is: "all information about an identified natural person or identifiable ("the interested party"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person; (art. 4.1 RGPD).

The processing of data (art. 4.2 RGPD) of natural persons who participate in clinical trials carried out by the Hospital at the request of the promoters, is subject to the principles and guarantees of the personal data protection regulations (RGPD, as well such as Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD)).

Participation in clinical trials entails the processing of health data (art. 4.15 RGPD) of patients ("interested persons", ex. art. 4.1 RGPD) and, therefore, it must be taken into account that information relating to the health of natural persons are subject to special protection.

Thus, article 9 of the RGPD regulates the general prohibition of the processing of personal data of various categories, among others, data relating to health (section 1). Section 2 of the same article 9 provides that this general prohibition will not apply when one of the following circumstances occurs:

"a) the interested party gives his explicit consent for the treatment of said personal data with one or more of the specified purposes, except when the Law of the Union or Member States establishes that the prohibition mentioned in section 1 cannot be lifted by the interested party;

h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation of the labor capacity of the worker, medical diagnosis, provision of assistance or treatment of a sanitary or social type, (…);

(…)

j) the treatment is necessary for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89, paragraph 1, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the fundamental interests and rights of the interested party.".

According to article 89.1 of the RGPD:

> **"1. The treatment for archival purposes in the public interest, scientific or historical research purposes or statistical purposes will be subject to adequate guarantees, in accordance with this Regulation, for the rights and liberties of the interested parties. These guarantees will require that technical and organizational measures are available, in particular to guarantee respect for the principle of minimization of personal data. Such measures may include pseudonymization, provided that in that way said ends can be achieved. As long as those goals can be achieved through further processing that does not allow or no longer allows the identification of the interested parties, those goals will be achieved in that way."**

The clinical history (henceforth, HC) is regulated and protected by a specific regulation (Law 21/2000, of December 29, on the rights of information concerning the patient's health and autonomy, and clinical documentation, and Law 41/2002, of November 14, basic, regulating patient autonomy and rights and obligations in the field of information and clinical documentation). Article 16.3 of Law 41/2002 (modified by the ninth final provision of the LOPDGDD), provides for access to the HC, among others, for research purposes, in the following terms:

> **"3. Access to clinical history for judicial, epidemiological, public health, research or teaching purposes is governed by the provisions of current legislation on the protection of personal data, and Law 14/1986, of 25 April, General of Health, and other rules of application in each case. Access to the clinical history for these purposes requires the preservation of the patient's personal identification data, separate from those of a clinical and healthcare nature, so that, as a general rule, anonymity is ensured, unless the patient himself has given his consent to don't separate them.**
>
> **The investigation cases provided for in Section 2 of the Seventeenth Additional Provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights are excluded. (…). Access to clinical history data and documents is strictly limited to the specific purposes of each case. (…)".**

According to section 2 of additional provision 17a, mentioned, of the LOPDGDD:

> **"2. The treatment of data in health research will be governed by the following criteria: a) The interested party or, as the case may be, their legal representative may grant consent for the use of their data for health research purposes and, in particular, biomedicine Such purposes may include categories related to general areas linked to a medical or research specialty.**
>
> **b) The health authorities and public institutions with powers to monitor public health may carry out scientific studies without the consent of those affected in situations of exceptional relevance and seriousness for public health. c) The reuse of personal data for health and biomedical research purposes will be considered lawful and compatible when, having obtained consent for a specific purpose, the data is used for research purposes or areas related to the area in which the initial study was scientifically integrated.**

(...).

d) It is considered lawful to use pseudonymized personal data for the purposes of health research and, in particular, biomedical research.

The use of pseudonymized personal data for research purposes in public and biomedical health will require:

1.º A technical and functional separation between the research team and those who carry out the pseudonymization and keep the information that makes re-identification possible. 2.º That the pseudonymized data are only accessible to the research team when: i) There is an express commitment of confidentiality and not to carry out any re-identification activity.

ii) Specific security measures are adopted to avoid re-identification and access by unauthorized third parties.

(...).”

Finally, the fifth final provision of the LOPDGDD has added a new article 105 bis to Law 14/1986, of April 25, general health, according to which: "The treatment of personal data in health research is will be governed by the provisions of the seventeenth additional provision of the Organic Law for the Protection of Personal Data and Guarantee of Digital Rights.”

According to article 58.1 of the 2015 Law on Guarantees and Rational Use of Medicines and Health Products (Royal Legislative Decree 1/2015, of July 24), a clinical trial means: "all research carried out on human beings with the in order to determine or confirm the clinical, pharmacological and/or other pharmacodynamic effects, and/or to detect adverse reactions, and/or to study the absorption, distribution, metabolism and elimination of one or more drugs under investigation in order to determine its safety and/or its effectiveness. (...).”

In relation to clinical trials, it is necessary to refer to article 3 of Royal Decree 1090/2015, of 4 December, which regulates clinical trials with medicines, the ethics committees of research with medicines and the Spanish register of clinical studies, according to which:

"1. A clinical trial subject to this regulation may only be initiated when the CEIM and the Spanish Agency for Medicines and Health Products have considered that all of the following conditions are met:

(...)

c) The informed consent of each of the test subjects, freely expressed, is obtained and documented, before their inclusion in the test in the terms provided for in articles 4 to 8. d) The rights are respected of the subject to his physical and mental integrity, and his privacy, and the personal data that concern him are protected, in accordance with Organic Law 15/1999, of December 13, on the Protection of Personal Data, and his development regulations, as well as with the current European regulations on the matter. (...).”

In short, the regulatory framework studied enables the treatment of health data for medical research purposes, specifically, for the performance of clinical trials,

on the basis of the informed consent of the participating patient, in the terms indicated.

IV

It is responsible for data processing: "the natural or legal person, public authority, service or other organism that, alone or together with others, determines the purposes and means of the treatment; if the Law of the Union or of the Member States determines the purposes and means of the treatment, the person responsible for the treatment or the specific criteria for his appointment may be established by the Law of the Union or of the Member States;" (art. 4.7 RGPD).

It is responsible for the treatment: "the natural or legal person, public authority, service or other organism that treats personal data on behalf of the person responsible for the treatment;" (art. 4.8 GDPR).

From the perspective of data protection, we start from the basis that the processing of personal data must have a person in charge, who consequently assumes a series of responsibilities and obligations regarding the processing that is carried out.

On the other hand, the Promoter is: "the individual, company, institution or organization responsible for initiating, managing and organizing the financing of a clinical trial" (article 2.1.s) R. decree 1090/2015).

The Monitor is the "qualified professional with the necessary clinical and/or scientific training and competence, chosen by the promoter, who is responsible for the direct monitoring of the trial. Serves as a link between the promoter and the main researcher, when they are not the same person. Under no circumstances should the monitor be part of the research team." (art. 2.2.i) R. decree 1090/2015).

The appointment of the Monitor is the function and responsibility of the Promoter (art. 39.3.h) R. decree 1090/2015). According to article 40.1 of the same R. decree 1090/2015, the functions of the monitor are, among others: "a) Work in accordance with the promoter's standard work procedures, visit the researcher before, during and after the trial , depending on the type of study, to check compliance with the protocol, ensure that the data are recorded correctly and completely, as well as ensure that the informed consent of all subjects has been obtained before their inclusion in the trial. "

According to article 39 of R. decree 1090/2015:

> **"4. The promoter of a clinical trial may delegate all or part of its tasks to a private individual, contract research organization (CRO), institution or body, which must have a quality assurance and control system.**
>
> **5. The promoter's obligations established in the rules of good clinical practice that have been delegated will apply to the individual, CRO, company, institution or contracted body. However, in these cases, the promoter will continue to be responsible for guaranteeing that the clinical trial and the final data generated in said study conform to the provisions of this Royal Decree. Any delegation of functions of the promoter in relation to one**

clinical trial must be specifically documented in a contract between both parties."

Thus, the Promoter can hire a "contract research organization" (CRO), to carry out the monitoring functions provided for in the studied regulations ("External Monitor"), to which the query refers.

We note that, according to section 49 of the "Documento de instrucciones de la Agencia Española de Medicamentos y Productos Sanitarios para la ensayos clínicos en España" (available on the website: www.aemps.es):

"The data related to health are considered by the LOPD to be specially protected data, which deserve a stricter protection regime, (...)
For this reason, the data collection notebook must only include a code that does not allow the identification of the subject. In addition, it will not be able to collect identifying data from the subjects participating in the study: (...)."

As the query mentions, the AEMPS document "Annex VIIIC. Revised instructions for updating the Protection of personal data section in the subject information sheet (HIP/CI) in relation to General Regulation (EU) nº 2016/679 on Data Protection", (attached to the instruction document of the AEMPS, cited), provides for the following:

"Both the Center and the Promoter are respectively responsible for the treatment of their data and undertake to comply with the data protection regulations in force. The data collected for the study will be identified by means of a code, so that no information that can identify you is included, and only your study doctor/collaborators will be able to relate said data to you and your clinical history. Therefore, your identity will not be revealed to any other person except to the health authorities, when required or in cases of medical emergency. The Research Ethics Committees, the representatives of the Health Authority in inspection matters and the staff authorized by the Promoter, will only be able to access to check personal data, the procedures of the clinical study and compliance with the norms of good clinical practice (always maintaining the confidentiality of the information)."

Although this document refers to Organic Law 15/1999, of December 13, on the protection of personal data (LOPD), repealed by the LOPDGDD, for the relevant purposes it is clear from this document that, as pointed out by consultation, and in line with the aforementioned regulatory framework, the Hospital is responsible for the treatment of the HC data of patients participating in clinical trials.

As can be seen from the consultation, the Hospital is, for the purposes of data protection regulations and sectoral regulations (Law 21/2000 and Law 41/2002), the person responsible for the data processed in the HC of patients it treats, including those who, through the provision of their consent, decide to participate in a clinical trial. As for the main researcher, it would be "the researcher responsible for a team of researchers who carry out a clinical trial in a clinical trial center" (art. 2.1.u) R. decree 1090/2915).

However, according to the consultation, "both the Hospital and the Promoter are legitimated as respectively responsible for the processing of the personal data that participate in the trial. The Hospital is responsible for the treatment of identified data and the

is responsible for the processing of pseudonymized data." The consultation adds that "also the staff authorized by the Promoter is authorized to access identified data of trial subjects to carry out monitoring or auditing tasks."

It should be borne in mind that, for the purposes of data protection regulations, pseudonymised data are personal data. Thus, according to Recital 26 of the RGPD: "The principles of data protection must apply to all information relating to an identified or identifiable natural person. Pseudonymized personal data, which could be attributed to a natural person through the use of additional information, must be considered information about an identifiable natural person.(...)."

According to the available information, both the Hospital and the Promoter are responsible for the processing of personal data (whether identified or pseudonymized) related to the conduct of clinical trials.

Based on this premise, we cannot rule out that it should be considered that both the Hospital and the Promoter decide what treatment should be done of the personal data related to the clinical trial.

If so, and it is both (Hospital and Promoter) who determine which personal data processing will be carried out for the trial (cohort of affected patients, objectives and scope of the study, personal information that may be necessary treat, etc.), it would seem reasonable to establish a shared responsibility or co-responsibility for the treatment of personal data (identified or pseudonymized) necessary to carry out the clinical trial, a possibility that article 4.7 of the RGPD foresees.

Thus, according to article 26 of the RGPD:

> **"1. When two or more persons responsible jointly determine the objectives and means of the treatment, they will be considered co-responsible for the treatment. The co-responsible parties will determine transparently and by mutual agreement their respective responsibilities in fulfilling the obligations imposed by this Regulation, in particular regarding the exercise of the rights of the interested party and their respective obligations to provide information referred to in the articles 13 and 14, except, and to the extent that, their respective responsibilities are governed by the Law of the Union or of the Member States that applies to them. Said agreement may designate a point of contact for those interested.**
>
> **2. The agreement indicated in section 1 will duly reflect the functions and respective relationships of the co-responsible parties in relation to the interested parties. The essential aspects of the agreement will be made available to the interested**
>
> **3. Regardless of the terms of the agreement referred to in paragraph 1, the interested parties may exercise the rights recognized by this Regulation against, and against, each of those responsible."**

In line with these provisions, article 29 of the LOPDGDD provides that: "The determination of the responsibilities referred to in article 26.1 of Regulation (EU) 2016/679 will be carried out taking into account the activities that each one actually carries out of those responsible for the treatment."

In short, in relation to clinical trials in which both the Hospital and the Promoter "determine the purposes and means of the treatment" (art. 4.7 RGPD), a model of co-responsibility of both regarding the processing of related personal data could be articulated with the essays. In this case, the treatment must be reflected and specified in the corresponding agreement, in the terms provided for in articles 26 and 28 of the RGPD.

Based on the establishment of a co-responsibility scheme in data processing, the following should be noted in relation to the role of the Monitor.

The Monitor will have to access certain information, not only pseudonymized information for which the Promoter who commissions the trial is responsible, but specifically personal information (HC) of the patients of the Hospital, in order to fulfill the functions it has attributed (R. decree 1090/2015). This, regardless of whether this Monitor is internal or external, since in both cases its functions are the same.

The Monitor of the trial would act in the case raised on behalf of not one, but two persons responsible for the treatment (Hospital and Promoter), since it will be both persons responsible who will indicate to the Monitor the scope and conditions of the treatment of 'patient information that you are authorized to do, and for what purpose. It must be understood, then, that the conditions for the processing of data by the Monitor will have to be established jointly and in a coordinated manner by both responsible parties, since the Monitor processes personal information on behalf of the two responsible parties.

Therefore, it will be the two responsible (Hospital and Promoter) who establish an agreement or commissioning contract with the Monitor. In fact, it seems that it could be established in a single agreement or contract, in which the three parties involved (Hospital, Promoter and Monitor) participate, the conditions of the treatment that will be carried out by the Monitor, as the person in charge of the treatment, on behalf of the two responsible

For all that has been said, the use of this co-responsibility scheme in the context of clinical trials (and the articulation of a single treatment contract with the Monitor, by both responsible parties) seems reasonable enough, from the perspective of personal data protection regulations.

However, in the event that a co-responsibility model is not established in the terms indicated and it must be understood that the Hospital is solely responsible, for the purposes of the data protection regulations, of the personal information in what the Monitor must have access to, it will be necessary for the Hospital to establish a treatment order with the Monitor, as will be specified later.

v

Given these considerations, we refer to the first question posed: "Could the Hospital understand that the External Monitor's access to the identified personal data of the subjects of the trial under the control of the Hospital is indirectly legitimized by virtue of the HIP/CI that legitimizes the Promoter's direct access to this data?".

According to the query, when the Promoter appoints a company as a monitor as a External Monitor, even if the Promoter and this External Monitor have signed a data processing contract, the Hospital understands that the External Monitor is not authorized to access the personal data identified of the trial subjects in

by virtue of the HIP/CI and, therefore, "the Hospital requires the signing of a data processing contract between the Hospital and the External Monitor under the terms of Article 28 of the RGPD".

At this point, it should be borne in mind that article 28.1 of the RGPD provides the following:

> **"1. When a treatment is to be carried out on behalf of a person responsible for the treatment, he will only choose a person in charge who offers sufficient guarantees to apply appropriate technical and organizational measures, so that the treatment complies with the requirements of this Regulation and guarantees the protection of the rights of the interested party."**

Due to the information available, the External Monitor of the trial will have to access data from the HC of the patients, in order to check and monitor the clinical trial carried out in the Hospital itself. Therefore, based on the information available, it is the Hospital in which the trial is carried out, as responsible for the HC of the patients, who would be responsible for determining the conditions for this access of the Monitor, to the extent that it may result relevant for the aforementioned monitoring tasks, provided for in the regulations (R. decree 1090/2015).

The task of treatment that the Promoter may have established with the external Monitor, would not be sufficient for the purposes of the Monitor being able to access non-pseudonymized data that are treated under the responsibility of the Hospital, as it should correspond to the Hospital – and not to the Promoter - the specification of the conditions of access and treatment that can be done by the HC Data Monitor, for the fulfillment of its functions.

Thus, an assignment contract established solely between the Promoter and the external Monitor, in which the Hospital does not participate, would be insufficient for the purposes concerned, since the Hospital would not have participated in the designation or in the establishment of its obligations, in the terms required by the regulations (art. 28 RGPD).

Article 28.1 of the RGPD requires the controller to designate only those in charge who offer sufficient guarantees that the data will be treated in accordance with the regulations.

This would mean that, in the event that there is only an assignment contract between the Promoter and the Monitor, the Hospital would be authorizing the treatment of patient health data by a person in charge (the External Monitor) in the designation of the which would not have participated, in order to ensure that it offers sufficient guarantees. This is another element that could make it advisable to assess the establishment of a co-responsibility model regarding the processing of data (eg art. 26 RGPD), to which we have already referred.

In any case, taking into account that the External Monitor of the trial would carry out access to HC data on behalf of the Hospital in which the trial is carried out, the Hospital must necessarily articulate the 'access and processing of HC data by the Monitor, for the fulfillment of its functions, through a processing order, as required by the provisions of article 28.1 RGPD. This, without prejudice to the assignment that the Promoter has established with the Monitor, or cases in which joint responsibility is established between the Hospital and the Promoter, in the terms indicated in the previous Legal Basis.

In any case, said contract must comply with the provisions of article 28.3 of the RGPD.

Having said that, it is necessary to take into account the provision of the fifth transitional provision of the LOPDGDD, in relation to the treatment commission contracts that, where appropriate, the Hospital has signed prior to May 25, 2018. About this , the RGPD has introduced modifications to the minimum content of the contract that regulates the assignment of the treatment, which affect both the obligations of the person in charge and those of the person in charge (the Hospital and the External Monitor, respectively), which are they will have to take into account in the case at har

In relation to said signed contracts, it may be of interest to consult the Guide on the person in charge of the treatment in the RGPD prepared by the data protection authorities to help those in charge and those in charge in adapting to the requirements of the RGPD, available on the Authority's website http://apdcat.gencat.cat/ca/inici/.

In any case, this conclusion is not distorted by the fact that the External Monitor of the trial's access to HC data has a sufficient legal basis based on the informed consent signed by the patient participating in the trial through the clause to which the query refers (HIP/CI), and based on the regulatory provisions studied, which enable access to HC data by the Trial Monitor, for the fulfillment of its functions (R. decree 1090/2015).

As has been said, the regulatory framework studied enables the processing of health data for the performance of clinical trials, on the basis of the informed consent of the patient who participates (art. 6 and 9 RGPD and additional provision 17a LOPDGDD, regulations of patient autonomy and R. decree 1090/2015). However, this does not detract from the need for this access to be articulated through the corresponding treatment order (e.g. art. 28.1 RGPD), given that the treatment is carried out on behalf of the person responsible for the patient's HC, that is , on behalf of the Hospital, in the terms indicated

VI

Given the considerations set out, we refer to the second question posed: "If the answer to the previous question is affirmative, could the Hospital no longer require the signature of a treatment contract between the Hospital and the External Monitor?" .

As has been explained, the Hospital, as responsible for the HC, is the one who determines the purposes and means of processing the data of the HC (art. 4.7 RGPD), to which the consultation refers, without prejudice that, given the participation that the promoter must have in the clinical trial, models of co-responsibility for the treatment should be articulated. When treatment is carried out on behalf of the person in charge (such as that which would be carried out, in the case at hand, by the External Monitor regarding the test carried out at the Hospital), this treatment must be articulated necessarily through the corresponding treatment contract (art. 28.1 RGPD).

VII

Below we refer to the third Question: "If the answer to the previous question is affirmative, should the Hospital establish some type of additional safeguard before allowing the External Monitor access to personal data under the control of the Hospital?".

As has been explained, given the information available, we start from the basis that it would be appropriate to sign the corresponding agreement or contract for the treatment

between those jointly responsible for the treatment - the Hospital and the Promoter - and the External Monitor as responsible (art. 26 RGPD), in the terms of article 28 of the RGPD.

Therefore, at the outset, in response to the query formulated, the establishment of "additional safeguards" would not replace the need to articulate the assignment of the treatment through the corresponding contract.

Apart from the fact that the contract between the Hospital and the External Monitor must include the provisions of Article 28.3 of the RGPD, the treatment of the HC's personal data must comply with the rest of the principles and obligations of the personal data protection regulations.

Among others, in relation to the treatment of personal information of participants in the clinical trial, special mention should be made of the following issues:

The processing of information for research purposes must comply with the principles established in the RGPD.

At the outset, it is necessary to reiterate the need to apply to data processing the requirements derived from the principle of minimization (art. 5.1.c) and art. 89 GDPR). In this sense, in the context of medical research and the performance of clinical trials, from the perspective of data protection, the use of information pseudonymization mechanisms is of particular interest (art. 89 RGPD), as a mechanism to reinforce compliance with said principle.

Given that in the field of clinical trials coded or pseudonymized information will be treated which, as has been said, remains personal information for the purposes of data protection regulations, special attention must be paid to the provisions on pseudonymization procedures and measures to prevent re-identification.

In this sense, it is also appropriate to take into account the specific requirements established by the second section of the seventeenth additional provision of the LOPDGDD for the treatment of data in health research, especially with regard to the evaluation of the impact regarding data protection.

It is also necessary to refer to the principle of integrity and confidentiality (art. 5.1.f) RGPD). The information of those affected must be treated by all those involved (the Hospital itself, the researchers, the Promoter and the Monitor), either in their capacity as responsible or in charge of the treatment, in accordance with this principle.

According to article 24 of the RGPD: "1. Taking into account the nature, the scope, the context and the purposes of the treatment as well as the risks of varying probability and severity for the rights and freedoms of the physical persons, the person responsible for the treatment will apply appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the treatment complies with this Regulation. These measures will be reviewed and updated when necessary. (...)".

The RGPD imposes the obligation on the data controller to adopt the necessary technical and organizational measures to guarantee the security of the personal data that will be processed. Obligation that also extends to the person in charge of the treatment (art. 28.3.c) RGPD).

The GDPR sets up a security system that is no longer based on the basic, medium and high security levels that were foreseen in the LOPD Deployment Regulation,

approved by Royal Decree 1720/2007, of December 21 (RLOPD), but by determining, based on the characteristics of the treatment and a prior assessment of the risks, which security measures are necessary in each case (Recital 83 and article 32 GDPR).

Therefore, by applying the provisions of the personal data protection regulations (articles 24 and 32 RGPD), it would be required to prepare an analysis and assessment of the risks involved in the processing of data, which aims to determine the technical and organizational measures that must be applied by those responsible and in charge of the treatment (eg art. 28.3.c) RGPD).

It will be necessary to take into account, where appropriate, the provision of the first additional provision of the LOPDGDD, relating to security measures in the public sector, according to which:

> **"1. The National Security Scheme will include the measures that must be implemented in the case of personal data processing to prevent its loss, alteration or unauthorized access, adapting the criteria for determining the risk in data processing to that established in article 32 of Regulation (EU) 2016/679.**
>
> **2. The responsible persons listed in article 77.1 of this organic law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in the companies or foundations linked to them subject to private law.**
>
> **(…).”**

In accordance with the considerations made so far in relation to the query raised, the following are made,

Conclusions

Given that the External Monitor of the trial must access data from the HC on behalf of the person in charge (the Hospital), this must articulate the access and processing of data by said Monitor, for compliance of its functions, necessarily through a processing order.

This conclusion is not distorted by the fact that the External Monitor of the trial's access to data from the HC of the participants in the trial has a sufficient legal basis, based on the informed consent of the persons affected.

The assignment contract between the Hospital and the External Monitor of the trial cannot be replaced by other types of "additional safeguards", without prejudice to compliance with the principles and obligations of the data protection regulations.

Barcelona, January 11, 2019