Machine Translated by Google

Ref. CNS 3/2020

Opinion in relation to the consultation of a health center about the legality of a Clinical trial management platform

A letter from a health center (hereinafter referred to as the Hospital) is submitted to the Catalan Data Protection Authority regarding the legality, in accordance with data protection regulations, of a Clinical Trials Management Platform (hereinafter, the Platform).

The consultation is accompanied by a copy of the document "Acuerdo de red de organização sanitarias" which, based on the information provided, the Hospital would sign with the company responsible for the Platform, and a copy of the document "Addendum on data processing" , which complements the previous document. Likewise, the query is accompanied by information about the Platform (...).

Having analyzed the request and the attached 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 Platform is a private initiative that arises from a project financed by public and private funds under the European call IMI (Innovative Medicines Initiative) to promote the design and execution of clinical trials based on obtaining aggregated data of the electronic medical history, applicable to any center that uses this electronic format, as is, according to the consultation, the case of the Hospital. According to the consultation, the platform aims to "build a pan-European/global network of centers that want to maximize their participation in clinical research with industry and academia."

According to the consultation, the Platform, from the company (...), is a tool that allows to identify, automatically and based on the data of the electronic clinical history, the patients who meet certain criteria, coinciding with the 'a certain clinical trial. The consultation explains that if the criteria match or are of interest to third parties, "the Hospital will receive an alert and contact the patients, offering the possibility of participation in the study or clinical trial."

The document accompanying the consultation explains that the Platform is the largest European network for the reuse of data from electronic clinical histories for medical research. According to this information, among the services that the Platform offers to hospitals is the recruitment of patients to be able to carry out clinical research.

The consultation adds that the software would be installed on the Hospital's server, and that the mandatory contract for the person in charge of the treatment would be signed. In relation to this contract and the processing of data subject to consultation, a copy of the document "ACUERDO DE RED DE ORGANIZACIONES SANITARIAS" (hereinafter, the Agreement) and the document "ADENDA SOBRE TRATAMIENTO DE DATOS" is attached to the consultation (hereinafter, the Addendum), as well as other complementary information about the Platform.

Located the consultation in these terms, according to Regulation (EU) 2016/679, of Parliament and the European Council, of April 27, 2016, General Data Protection

Machine Translated by Google

(henceforth, RGPD), are personal data: "all information about an identified or identifiable natural person ("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, whether patients or Hospital professionals who will be users of the Platform, is subject to the principles and guarantees of the personal data protection regulations (RGPD , as well as Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD)).

III

It must be said that despite the breadth of documentation provided when making the inquiry, the documents are not very specific, and sometimes even contradictory, both in terms of the system used and in terms of the definition of the treatments that are intended to be carried out, the definition of the roles that each of the agents involved will play and their responsibilities. In this sense, the use of two documents and an addendum is particularly confusing, where aspects related to data that would be treated under co-responsibility are often treated in a mixed manner, with other aspects related to data that would be treated as part of an order from the treatment. It should be clearly differentiated.

In any case, this lack of clarity prevents us from making a precise statement on these issues.

However, given the content of the documentation provided, referring to the Hospital's participation in the Platform, from the perspective of data protection it is appropriate to analyze different aspects, specifically:

1. Description of the treatment of personal data 2. Need to carry out a Data Protection Impact Assessment 3. Scheme of attribution of responsibilities 4. Legitimation of the treatment 5. Application of the principle of minimization

6. Exercise of rights 7. International data transfers (TID) 8. Security measures

Description of the processing of personal data

a) Treatment of patient data:

In summary, according to the document "Acuerdo de organização sanitarias Network", the company (...) owns a cloud-based IT platform to facilitate research, specifically to "allow users to analyze aggregated populations of patients from participating healthcare organizations and other data sources".

According to the Agreement, the healthcare organization (OS) - which would be, in the case at hand, the Hospital making the inquiry - would access the Platform through a license provided by the company, which includes access to the Global Research Network

Machine Translated by Google

the company. Section 1.16 of the agreement defines the Network as "the cloud-based computing platform ... to facilitate research, such as, but not limited to, enabling users to analyze aggregate patient populations of healthcare organizations. "

The use of expressions such as "for example, but not limited" prevents knowing exactly what the treatment of patient data carried out by the platform will consist of.

There are other examples of issues that are not sufficiently well defined. Thus, for example, according to point 2.1 of the Agreement, the Hospital "owns and retains the right to control the transfer and use of OS data in relation to the company's Global Research Network . Personal data relating to OS patients is retained within the OS environment and is not transferred outside of the OS environment, except as provided in Section 2.2 (of the Agreement)."

It would be necessary to specify the reference to "the environment of the OS" (which is also not clearly defined in the definition given in section 1.5 of the Agreement), given that it is not clear what is being referred to (the servers of the OS, the treatment under their responsibility with the collaboration of the person in charge of the treatment ...).

There are also certain confusions or contradictions in the company's treatment of pseudonymised information. According to point 2.4 of the Agreement: "OS represents and warrants that OS data sent to the company will be pseudonymized in accordance with the RGPD and all privacy laws before being transferred to (the company). Without prejudice to this, each of the Parties will carry out all the activities described in the Agreement and will protect the privacy and security of all personal data in accordance with the RGPD."

It would seem, based on this and what is explained in the text of the consultation, that the OS will deliver health information of its patients, previously pseudonymized to the company.

The treatment of pseudonymised patient data, which the Hospital has for medical research purposes, is positively assessed without prejudice to what will be said later.

As explained in the text of the query (although not as clearly explained in the attached documents), it seems that, at least initially, the company's role is to identify matching patients with the patient profile on which a certain study is to be carried out.

In this phase, the results that could be given to third parties ("third parties and promoters" in the terms expressed in the query) would be anonymous results. In this sense, point 1.9 of the Agreement refers to the "anonymous results of queries in (the company's) data networks, such as patient counts, prevalence metrics, incidence rates and other aggregated statistical data, which is provided to users of the platform.". It appears that this reference is to be understood as being made to aggregate query results that cannot be linked in any way to specific individuals. Only in this case would it be appropriate to refer to anonymous information.

It must be remembered that only information that is irreversibly separated from the patient can be considered anonymous, which is precisely not the case with pseudonymised information. The distinction is relevant from a data protection perspective, as pseudonymised information is for all intents and purposes personal information protected by the GDPR, while anonymous information loses this status (recital 26 GDPR).

Machine Translated by Google

At this point, it is necessary to make an indentation, because in some points of the documents provided it seems that this distinction is not taken into account. Thus, for example, according to point 2.1 of the Agreement, it is stated that personal data relating to patients of the OS is kept in the environment of the OS and is not transferred outside the environment of the OS OS, except as provided in Section 2.2 (of the Agreement).” . When in reality, as stated in the same documents, the pseudonymized data of the patients are transferred

Based on this pseudonymised information, and if the criteria match the interest of the third party or promoter, the consultation indicates that the center would contact the patients offering the possibility of participating in the study.

It is not sufficiently specified in the available documentation, what type of third party recipients could request and receive pseudonymized information from the Hospital's HCs, the geographical scope that these third parties could have, if it is limited to the European area (entities that, in principle, could be subject like the Hospital to the provisions of the RGPD), or if the recipients could be hospitals or research centers in other countries. In any case, to the extent that it is anonymized information, it would not be subject to the provisions of the RGPD.

It should be borne in mind that there are different types of research provided for by Law 14/2007, of July 3, on biomedical research (LIB), but also other types of research that are excluded from the scope of application of the LIB, such as observational studies (art. 58.2 of the Guarantees and Rational Use of Medicines and Health Products Act of 2015 (Royal Legislative Decree 1/2015, of July 24)), clinical trials, which are not the LIB applies, and which, as mentioned in recital 161 of the RGPD, are regulated by its specific regulations (EU Regulation 536/2014, of April 16, on clinical trials of medicinal products for human use) , or epidemiological studies (provided for in the patient autonomy legislation (art. 16.3 Law 41/2002 and art. 11.3 Law 21/2000).

Considering that the types of medical research are very varied, depending on the type of study that you want to carry out, it may or may not be necessary to identify the patients.

Thus, in the case of clinical trials, given the regulatory regulations, it would be necessary for the person in charge or promoter of the trial to contact the patients who have been checked, based on the initial screening of pseudonymized information that the Platform allows, who may be potential participants in the trial. In this case, it may obviously be necessary for the Hospital to contact these patients, in order to offer them the possibility to participate. However, in other cases, it may be that a research center can carry out a study with pseudonymised data (section d) of DA 17ª of the LOPDGDD) without it being strictly necessary to contact the patients. But this does not seem to be the case presented in the consultation, given that it is limited to indicating that "the data accessible by third parties would be anonymised".

In this sense, a contradiction is also observed with section 2.3 of the Agreement, in which the company is granted the right "to "access, use, host, copy, translate, distribute and format the OS data”. The use of the term "distribute" seems contradictory to the object defined in the query and to the content of clause 2.2 of the Agreement.

It should be noted at this point that the exposition of the inquiry incurs a contradiction, because while on the one hand it indicates that "the data accessible by third parties would be anonymized" it then indicates that "(the third parties could not know to whom they correspond)". And both expressions are not equivalent. The first expression refers to anonymous data. The second could also refer to pseudonymised data. In any case, given that in the texts of the attached documents it is not

Machine Translated by Google

foresees that the company provides third parties with sets of pseudonymised data, it must be understood that it refers only to anonymous data.

The recruitment of participants for a clinical trial based on participation in the Platform could be enabled as long as it is the Hospital, as responsible for the HC, who re-identifies the patient.

Despite what is exposed in the consultation, it is no less true that sections 2.1 and 2.2 of the Agreement open the door, within what are called advanced functions of the platform, to which patient data can be transferred to third parties In this case this communication of data would be subject to the RGPD. In any case, this opinion will not analyze this issue, since the consultation only refers to this issue in passing, without making a precise statement and that these sections reserve the control and decision of these transfers to the OS and expressly state that the principles of personal data protection must be applied.

- User data processing:

It is planned to use identifying data of the Hospital professionals who use the Platform. The processing of this data will be the subject, according to the available information (point 1.6 of the agreement), of a processing order (art. 28 RGPD).

In principle, it seems that these data would not be pseudonymized, although section 2 of the addendum, dedicated to the general provisions (therefore also applicable to user data), provides that among the obligations of the OS "provide solo datos pseudonymized on the server of (the company)" (section b)).

Obviously, this data is personal data subject to the principles and guarantees of the RGPD.

According to section 1.1 of the Addendum, the company "acts as a processor under the control of the Hospital regarding the processing of personal data of the Hospital's users of the products and services provided under agreement This personal data consists of the typical information used to implement access control (...).

According to section 8.2 of the Addendum, the company "will only process the personal data of the users of the hospital necessary to provide the services under the Agreement, specifically to provide the users of the Hospital with access to the products of (the company)", specifically: Full name; professional contact information, including email addresses; professional level/status (positions); information about the use of the platform; audit log information, including IP address.

This specification is positively evaluated regarding the processing of user data.

It cannot be ruled out that some of this data may be processed, not by the person in charge (the company), but by other third parties. In principle, it does not seem that this must necessarily be the case, although section 4.1 of the addendum would allow access by the sub-processor (Amazon web services) that would host the platform.

IV

Need to carry out a Data Protection Impact Assessment (AIPD)

Machine Translated

Machine Translated by Google

According to article 35 of the RGPD:

"1. When it is likely that a type of treatment, in particular if it uses new technologies, by its nature, scope, context or purposes, entails a high risk for the rights and freedoms of physical persons, the person responsible for the treatment will, before the treatment, an evaluation of the impact of the processing operations on the protection of personal data. A single evaluation may address a series of similar treatment operations that involve similar high risks.

2. The data controller will seek the advice of the data protection officer, if appointed, when carrying out the data protection impact assessment.

3. The data protection impact assessment referred to in section 1 will be required in particular in the event of:

a) systematic and comprehensive evaluation of personal aspects of natural persons that is based on automated processing, such as the creation of profiles, and on the basis of which decisions are taken that produce legal effects for natural persons or that significantly affect them in a similar way;

b) large-scale processing of the special categories of data referred to in article 9, paragraph 1, or of personal data relating to convictions and criminal offenses referred to in article 10, or

c) large-scale systematic observation of a public access area."

If we look at the characteristics of the treatment of pseudonymised data subject to consultation, which are health and genetic data (art. 9 RGPD), that the treatment will predictably occur on a large scale (not only by the entities that will process it but because it could dealing with a qualitatively and quantitatively very significant set of HHCC data), in the case at hand it is essential to carry out an AIPD.

In this sense, the Working Group of Article 29 ("Guidelines on the evaluation of impact relative to data protection (EIPD) and to determine if the transaction probably entails a high risk for the purposes of the RGPD") has explained that it is necessary to carry out an AIPD when, among others, these characteristics occur in the treatment: the elaboration of profiles and predictions based on health data, among others; treatment of categories of sensitive data; large-scale data processing; data related to vulnerable people; and innovative use of technologies, among others. Not only that, but in this case it is necessary to mention again that the possibility of re-identification of personal data always entails a certain risk, which must be anticipated and mitigated as much as possible.

All these characteristics come together in the treatment we are dealing with and therefore the completion of an AIPD prior to treatment is essential.

In addition, according to section 2.f) of DA 17a of the LOPDGGD:

> **"f) When, in accordance with the provisions of article 89 of Regulation (EU) 2016/679, a treatment is carried out for the purposes of public health research and, in particular, biomedical research, it will proceed to:**
>
> **1.º Carry out an impact assessment that determines the risks derived from the treatment in the cases provided for in article 35 of Regulation (EU) 2016/679 or in those established by the control authority. This evaluation will include**

Machine Translated by Google

specifically the risks of re-identification linked to the anonymization or pseudonymization of the data.

2. To submit scientific research to quality standards and, where applicable, to international guidelines on good clinical practice.

3.º Adopt, where appropriate, measures aimed at guaranteeing that researchers do not access identification data of the interested parties.

4. To appoint a legal representative established in the European Union, in accordance with article 74 of Regulation (EU) 536/2014, if the promoter of a clinical trial is not established in the European Union. Said legal representative may coincide with that provided for in article 27.1 of Regulation (EU) 2016/679."

The specific mechanisms of pseudonymization, as well as those established to minimize the risk of improper re-identification of patients by other participants in the Platform, are matters that must be defined and planned prior to the start of the treatment, and which will need to be specified in the data protection impact assessment (35 RGPD and art. 2.f.1 LOPDGDD).

For all of the above, it is necessary to carry out an impact assessment in the terms provided for in article 35 of the RGPD, before the start of the treatment.

We refer, in this regard, to the Practical Guide "Impact assessment relative to data protection", available on the website www.apd.cat.

v

Responsibilities attribution scheme

It is necessary to start from the basis that the Hospital is responsible for the personal information of patients contained in their clinical history (HC), in the terms of Law 21/2000, of December 29, on information rights concerning the health and autonomy of the patient, and the clinical documentation, and of Law 41/2002, of November 14, basic, regulating the autonomy of the patient and rights and obligations in the matter of information and clinical documentation .

In the documentation provided (Agreement and Addendum) it is planned to establish two distinct relationships between the company that owns the Platform (hereafter, the company) and the Hospital making the inquiry (OS), depending on the personal information object of treatment. According to section 1.1 of the Addendum, this aims to "differentiate the responsibilities of the parties as joint data controllers, and as data processors". This same section specifies the following:

The company "acts as a processor under the control of the OS with regard to the processing of personal data of the users of the Hospital of the products and services provided under the Agreement. (...).
The company "and the Hospital are jointly responsible for the treatment with regard to the treatment of the clinical data of patients (...)."

In this sense, the Addendum foresees some "general provisions on the processing of personal data" (point 2), and forecasts referring, on the one hand, to the responsibilities of the parties in relation to the processing of data in which the company is in charge of the treatment ("PART I" of the Addendum (point 8)) and, on the other hand, the responsibilities of

Machine Translated by Google

the company and the Hospital in the treatment of pseudonymised patient data, for which both are jointly responsible ("PART II" of the Addendum (point 9)).

- About the co-responsibility regime

According to article 4.7 RGPD, the person responsible for the treatment is "the natural or legal person, public authority, service or other organism that, alone or together with others, determines the ends and means of the treatment;"

The regulations also provide for the possibility of establishing co-responsibility for the treatment, that is, for two or more responsible parties to jointly determine the objectives and means of the treatment (art. 4.7 and art. 26 RGPD and art. 29 LOPDGDD).

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 party.**
>
> **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."**

When a co-responsibility model is established, the RGPD requires the signing of an agreement that clearly determines the respective functions and relationships of the co-responsible parties in relation to the interested parties, who must know the essential aspects of the agreement (art. 26 GDPR). In the case at hand, the available documentation foresees that the Hospital and the company will be jointly responsible for the processing of pseudonymised data of the Hospital's patients. If this is the case, the co-responsible parties would need to establish a specific agreement (in terms of art. 26 RGPD) and inform the affected persons.

Now, although the possibility of joint responsibility is foreseen by the RGPD itself, the description of the responsibilities in the documentation provided does not seem to obey precisely this scheme.

"

Thus, point 2.1 of the Agreement indicates that the OS has and retains the right to control the transfer and use of OS data in relation to the Global Research Network (of the company). Personal data relating to patients of the OS are kept in the environment of the OS, except as provided in Sección 2.2 siguiente."

For its part, Section 2.2 foresees "If the OS decides, at its sole discretion, to activate certain advanced functions of the Global Research Network, it is possible that it would be necessary to transfer certain personal data ...."

Machine Translated by Google

Section 3.6 of the Agreement ("Collaboration Network") explains that the Hospital can request authorization from the company to display the results of consultations carried out with other collaborators of the network This same section provides that the Hospital can close access to the data of other collaborators.

In other words, according to the information available, it is the Hospital that can decide to use the Platform to conduct research and manage the pseudonymised information of the Hospital's HCs, or it can decide to share the information with other "collaborators" ” of the “private collaboration network”, which voluntarily form the Hospital and other healthcare organizations that participate in the Platform, according to section 1.4 of the Agreement.

This would correspond more to a processing order scheme, from the Hospital as responsible to the company as in charge, not only to treat the data of the workers, users of the platform, but as in charge of carrying out the process screening of patients likely to participate in a study).

Those responsible for the treatment would rather seem to be the different entities that participate in the network by providing information, as well as the entities that carry out the research projects.

It is therefore necessary to clarify what is the chosen model and the decision-making capacity of each of those responsible regarding the personal information processed.

- **Determination of the role as responsible and in charge of the treatment of the different stakeholders**

With regard to the treatment carried out by the company as the processor (in principle the data of the users, but as we have just pointed out it could also affect the pseudonymised data of the patients), it is necessary to ensure that the platform offers sufficient guarantees , in terms of article 28.1 of the RGPD, according to which “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."

Although there are different provisions of article 28.3 of the RGPD that are collected throughout the Addendum, there are other provisions that are not made explicit in the documentation provided.

PART I of the Addendum (referring specifically to the processing of user data) only confirms that "the company acts as the processor and following the instructions of the Hospital", specifies the personal data of the users that will be subject of treatment, and foresees that, once the Agreement has expired or been terminated, the Hospital will indicate whether the data must be returned or destroyed (in correspondence with the provisions of art. 28.3.g) RGPD).

However, the documentation is confusing since there are other provisions of article 28.3 of the RGPD that are included in different sections of the Addendum (specifically, in section 2 of the Addendum, in which include "General provisions on the processing of personal data" such as the obligation to refrain from processing personal data for other purposes, or the general commitment to fulfill its obligations "in accordance with the documented instructions of l'Hospital", which can be deduced to refer to the assignment of the treatment, but which could also refer to the co-responsibility model for the treatment of HHCC. In any case, given the provisions of article 28.3. a) RGPD should also refer to the fact that the company must follow these

Machine Translated by Google

instructions regarding international data transfers, which is not made clear at this point. The obligation of confidentiality (art. 28.3.b)) is included in section 1.3 of the Addendum. We can also consider the provision of article 28.3.h) to be included in section 3.6 of the Addendum.

Regarding other sections of article 28.3 that should be made explicit in the commission contract, given the information available in various sections of the Addendum, we highlight the following:

Regarding section 28.3.c) RGPD (obligation of the person in charge to take the necessary security measures ex. art. 32 RGPD), section 2 of the Addendum includes several measures in relation to the data that are revealed to him by the Hospital, so it could be understood that they are measures that will be applied in the commission contract. In any case, it would be convenient to provide for it explicitly in the order contract. The company's security measures specified in sections 3.1 and 3.2 of the Addendum must also be included, if applicable, in the order contract.

Regarding article 28.3.d), point 4.1 of the Addendum makes it clear that the Hospital "recognizes and accepts" the subcontractor (Amazon Web Services), as well as the appointment of the company's subsidiaries as subcontractors . In this regard, the treatment order must specify that the company is obliged to inform the Hospital of any change in the subcontractors (eg art. 28.3.2 RGPD) and that the subcontractors are obliged under the terms of the article 28.3.4 RGPD. In any case, the fact that the Addendum specifies the use of this subcontractor does not exempt the person in charge of the treatment from ensuring that he meets the necessary guarantees in accordance with the RGPD to carry out the treatment (paragraphs 1 , 2 and 4 of article 28 RGPD).

With regard to the provision of article 28.3.e) RGPD - to assist the person in charge in handling rights requests -, as specified in FJ VIII of this opinion, it is necessary that the commission contract of the specific treatment how the requests to exercise rights that may arise to the person in charge will be conveyed.

Therefore, it is necessary to clearly distinguish in the Addendum the obligations required by article 28.3 RGPD to the person in charge (the company), in relation to the treatment that is carried out as part of the treatment order, and which will have to be subscribed to in the corresponding contract or agreement, of all those forecasts that refer to the treatment of pseudonymized data that, due to the information provided, are treated under a co-responsibility regime. It is necessary to systematize the content of the order contract, so that the different obligations are grouped together more clearly, following the instructions of the responsible Hospital, the company as responsible must comply.

In relation to the commissioned contracts signed, it may be of interest to consult the Guide on the data controller in the RGPD, available on the Authority's website http:// apdcat.gencat.cat/ca/inici/.

VI

Legitimation of the treatment

According to point 2.3 of the Agreement, the Hospital grants the company the right to "access, use, host, copy, translate, distribute and reformat the OS data, as well as to create and publish derivative works of these, exclusively for the purpose of providing them for use on the Platform. (...). The data license granted is for research purposes only."

Machine Translated by Google

The processing of personal data must have, to be lawful, an appropriate legal basis (art. 6.1 RGPD). Among others, the processing of data for research purposes may be lawful if the consent of the affected is available (art. 6.1.a) RGPD), or if it is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers by the controller (Article 6.1.e) RGPD), or also if it is necessary to satisfy the legitimate interests of the controller or a third party (Article 6.1.f) RGPD).

On the other hand, article 5.1.b) RGPD states that "the further processing of personal data for archiving purposes in public interest, scientific and historical research purposes or statistical purposes will not be considered incompatible with the initial purposes".

It must be positively assessed that, based on the information available, the data processing that will occur with the use of the Platform by the Hospital, is clearly within the scope of medical research purposes (points 2.3; 2.5; 6.3 of the Agreement ; points 9.1, 9.2 and especially, 9.5 of the Addendum, among others). Section 1.12 of the Agreement specifies what is meant by "research", for the purposes of the contract or agreement signed between the Hospital and the company. This definition refers, specifically, to research in the health field and to the treatment of health data (art. 4.15 RGPD) and genetic data of patients (4.13 RGPD), for the purposes of medical research.

With regard to the processing of categories of data subject to special protection, Article 9 of the RGPD regulates the general prohibition of the processing of personal data of various categories, among others, data relating to health and data genetics (section 1). Section 2 of the same article 9 provides that this general prohibition will not apply when any of the circumstances provided for in this article occur, among others:

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

According to article 89 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 purposes can be achieved through further processing that does not allow or no longer allows the identification of the interested parties, those purposes will be ach**
>
> **(...)."**

As has been agreed by this Authority on previous occasions (Opinions 15/2019, 18/2019, or 59/2018, among others), the RGPD supports the processing of special categories of data for research purposes, in particular in the health field, with some flexibility, as is clear, among others, from recital 52 of the RGPD.

Machine Translated by Google

The fifth final provision of the LOPDGDD has added a new article 105 bis) to Law 14/1986, of April 25, general health (LGS), according to which: "The treatment of personal data in the investigation in health 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."

Law 41/2002, modified by the LOPDGDD, provides for the treatment of health data for research purposes and starts from the general rule (as already established by the patient autonomy legislation, prior to the entry into force of the RGPD and the LOPDGDD), that the clinical care data and the patient's identifying data must be treated separately, unless the latter's consent is available.

Based on this general rule, article 16.3 of Law 41/2002 itself refers to additional provision 17a, section 2, of the LOPDGDD (DA 17a), regarding the criteria applicable to the processing of health data for research purposes.

The processing of health data for research purposes, foreseen in the regulatory framework of the State, can find coverage in different exceptions (art. 9.2.g), h), i) ij) RGPD), which lift the prohibition of process data from special categories, such as health data, and enable their processing (art. 9.1 RGPD).

More specifically, and for the purposes of interest, according to section 2 of DA 17a of the LOPDGDD:

> **"2. Data processing 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 the purposes of health research 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.**
>
> **In such cases, those responsible must publish the information established by article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with respect to treatment of your personal data and the free circulation of this data, in an easily accessible place on the corporate website of the center where the research or clinical study is carried out, and, where appropriate, on that of the promoter, and notify the existence of this information by electronic means to those affected. When these lack the means to access such information, they may request its referral in another format.**
>
> **For the treatments provided for in this letter, a favorable prior report from the research ethics committee will be required.**

Machine Translated

Machine Translated by Google

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

The use of pseudonymized personal data for the purposes of public health and biomedical research 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 to confidentiality and not to carry out any re-identification activity. ii) Specific security measures are adopted to prevent re-identification and access by unauthorized third parties.

The re-identification of the data at its origin may be carried out, when due to an investigation that uses pseudonymized data, the existence of a real and concrete danger to the safety or health of a person or group of persons is appreciated, or a serious threat para sus derechos or necessary to guarantee adequate health care. (…)

f) When, in accordance with the provisions of article 89 of Regulation (EU) 2016/679, a treatment is carried out for the purposes of public health research and, in particular, biomedical research, it will proceed to:

1.º Carry out an impact assessment that determines the risks derived from the treatment in the cases provided for in article 35 of Regulation (EU) 2016/679 or in those established by the control authority. This evaluation will specifically include the risks of re-identification linked to the anonymization or pseudonymization of the data. 2. To submit scientific research to quality standards and, where applicable, to international guidelines on good clinical practice. 3.º Adopt, where appropriate, measures aimed at guaranteeing that researchers do not access identification data of the interested parties. 4. To appoint a legal representative established in the European Union, in accordance with article 74 of Regulation (EU) 536/2014, if the promoter of a clinical trial is not established in the European Union. Said legal representative may coincide with that provided for in article 27.1 of Regulation (EU) 2016/679.

g) The use of pseudonymized personal data for the purposes of public health and, in particular, biomedical research must be subject to the prior report of the research ethics committee provided for in the sectoral regulations.

In the absence of the aforementioned Committee, the entity responsible for the investigation will require a prior report from the data protection delegate or, failing that, from an expert with previous knowledge in article 37.5 of Regulation (EU) 2016/679. (…)"

The Agreement provides that the Hospital, responsible for the patients' HHCC, must pseudonymize the patient information that must be processed through the Platform.

Thus, section 2.4 of the Agreement provides that "The OS declares and guarantees that the data of the OS that is sent to (the company) will be pseudonymized in accordance with the RGPD before being transferred (...)."

Machine Translated by Google

The principles and guarantees of data protection are fully applicable to pseudonymised data which are, for all purposes, personal data (recital 26 RGPD).

According to article 4.5 of the RGPD, it is necessary to understand by pseudonymization: "the treatment of personal data in such a way that they can no longer be attributed to an interested party without using additional information, provided that said additional information appears separately and is subject to measures technical and organizational techniques aimed at ensuring that personal data are not attributed to an identified or identifiable natural

The RGPD configures pseudonymization as an adequate guarantee for data protection (art. 6.4.e), 25.1, and 32.1.a) RGPD, among others), without excluding from the scope of the protection regulations of data the pseudonymized personal information.

This regulatory provision that we are examining considers the processing of pseudonymized data lawful for health research purposes, as long as appropriate guarantees are applied, without making explicit the requirement for the provision of consent on the part of those affected (art. 6.1. a) and 9.2.a) RGPD).

In short, for the purposes of interest, it is clear that the treatment of pseudonymized data for biomedical research purposes can find sufficient authorization based on the provisions of section 2.d) of DA 17 of the LOPDGDD, in relation to articles 9.2, section j) and 89.1, of the RGPD.

When the circumstances provided for in section 2.d) of DA 17a) of the LOPDGDD occur, the consent of those affected will not be essential to carry out the processing of pseudonymized health data of the Hospital's patients.

VII

Application of the minimization principle

According to article 5.1.c) of the RGPD, the data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Section 9.2 of the Agreement provides for dealing with "all information related to the state of health of natural persons (including demographic, diagnostic, procedure, laboratory, genetic, medication information...)" .

According to the Addendum, “information about healthcare professionals relating to the assistance or treatment provided or in relation to patients (for example, medical interventions carried out, relationship between the doctor and a patient...)” can also be processed. . It should be clarified whether this information is also treated as pseudonymised. But even if it were, it is not clear that it could be relevant or pertinent information for the purposes of medical research, include information about the doctor's relationship with the patient or, simply, personal information of the professionals treating the patient. This forecast should be revised.

In any event, it appears that all patient health and genetic information, that is, the entire content of the health and genetic data of HHCCs, could be affected by the Agreement.

The principle of minimization must be present in the Hospital's prior assessment when specifying which categories of health and genetic data it considers necessary to pseudonymize and share. Valuation that must respond to a prior analysis from the perspective of the minimization principle, and which does not appear to need to include

Machine Translated by Google

necessarily all of the HHCCs, for any research study that you want to do. Before carrying out any treatment, it is necessary to determine the relevant information for the purposes of the research.

In any case, it is necessary to evaluate positively the express provision of section 9.4 of the Agreement, in the sense that the Hospital determines which pseudonymized patient data is provided to the company and the methods with which the treatment is carried out prior (we understand that it refers to pseudonymization) to the communication of the data.

This general forecast is appropriate if it is interpreted in the sense indicated, to assess in advance which health and genetic data may be appropriate to pseudonymize in view of the specific research studies that could be carried out.

VIII

Exercise of rights

With regard to the exercise of rights by interested parties regarding the processing of pseudonymized data (arts. 15 et seq. RGPD), section 9.6.1 of the Addendum provides that the company must send all the requests that may be made to the Hospital, so that it can respond to them.

Section 9.6.2 of the Addendum provides that the Hospital "maintains the responsibility to respond to the requests of the interested parties, since the data is provided to (the company) in pseudonymized form and (the company) therefore it cannot respond to these requests.", And section 3.4 of the Addendum provides that the company will immediately notify the Hospital and cooperate with it if a complaint or request is presented regarding the exercise of rights of the interested party under the GDPR. Section 6.1.3 of the Addendum specifies the rights of those affected, in accordance with the provisions of the RGPD.

The concreteness, both of the rights provided for by the RGPD for those affected, and the provision according to which the company will communicate these requests to the Hospital, regarding the pseudonymized information, is positively valued.

However, it would be appropriate to include a provision regarding the possibility that Hospital users (whose data are not pseudonymised), who use the platform, exercise the rights provided for by the RGPD, not only in front of the Hospital itself (which can attend to them and solve them as the person responsible for the processing of their employees' data), but also for the case that the request is raised before the company, a possibility that we cannot rule out.

It is therefore appropriate to foresee how these requests for rights from users of the platform will be conveyed.

IX

International data transfers (TID)

According to clause 6 of the Addendum, the parties (Hospital and Company) are subject to the "Type Contractual Clauses", approved by the European Commission for the transfer of personal data between those responsible and those in charge of the treatment and between those responsible for the treatment which are included in annexes I and II of the Addendum.

With regard to the provisions on international data transfers (TID), in article 44 of the RGPD, the RGPD establishes, at the outset, that "a transfer of

Machine Translated by Google

personal data to a third country or international organization when the Commission has decided that the third country, a territory or one or several specific sectors of that third country, or the international organization in question guarantee an adequate level of protection", assumptions in that the TID "will not require any specific authorization" (article 45.1).

According to the information available, the company in charge of the treatment, the company, based in the United States, is included as an entity adhering to the Privacy shield. At the link https://www.privacyshield.gov/list you can consult a list with the entities adhering to the Privacy shield. According to section 1.5 of the Agreement, the subsidiary company acts as the company's representative in the European Union.

By application of article 46.2 of the RGPD, given the information available, it can be considered that the adoption of the standard contractual clauses of the European Commission in relation to the commission contract that concerns us, allows us to offer adequate guarantees for to the processing of the data.

Annex 1 of the Addendum includes, among other aspects, the definitions found in article 3 of the Commission's Decision (clause 1 of Annex 1), as well as the exporter's obligations , that is to say, the person in charge (clause 4 of Annex 1) and of the importer, that is to say, the person in charge (clause 5 of Annex 1), as provided for in the Commission's Decision.

In any case, the following questions should be clarified:

We note that, according to clause 5.c) of Annex 1 (obligations of the person in charge), it is foreseen that the person in charge guarantees that he has implemented the technical and organizational measures "specified in Appendix 2 before dealing with the personal data transferred". Now, Appendix 2, again makes a general and imprecise mention of the security measures taken, in the following terms: "The data importer will maintain administrative, physical and technical safeguards to protect security, confidentiality and integrity of personal data, as described in the "Healthcare Organization Network Agreement." Given that the content of this Agreement is unknown, it is not possible to check whether its content conforms to what is required by standard contractual clauses. It would therefore be appropriate to review this issue.

According to Appendix 1 of the Addendum (corresponding to said standard contractual clauses to which the parties submit the task of processing), in the "data subjects" section, the following categories of affected are indicated, the whose data could be the subject of communication to the person in charge: "prospects, customers, patients, website visitors, business partners and vendors of data export. Employees or contact persons of data exporters (...)."

Taking into account that Appendix 1 refers to the treatment contract that the Hospital would sign with the company to process the data of the Hospital's users who would use the Platform, the description of the categories of affected is excessive.

Above all, due to the reference made to patient data, which should not be the subject, due to the information consulted, of said treatment order (which only affects data of users who use the Platform from the Hospital). This section should be reviewed that, in principle, given the information available, it should only refer to Hospital workers who must be users of the Platform.

X

Machine Translated by Google

Information security measures

The treatment of risks associated with data security must be based on an analysis of the risk associated with the loss of confidentiality, integrity and availability of data. Standard risk analysis methodologies (eg ISO) may be appropriate for the purposes of the intended treatment.

Beyond this, the person responsible for the treatment (or the co-responsible persons, in this case, ex. art. 26 RGPD), must articulate the technical and organizational measures that are necessary in order to ensure the lawfulness of the treatment of the health data, in the terms required by article 9.2.j) and 89.1 of the RGPD, taking into account recital 53 of the RGPD, according to which: "(...). The Law of the Union or Member States must establish specific and adequate measures to protect the fundamental rights and personal data of individuals. Member States must be empowered to maintain or introduce other conditions, including limitations, with respect to the treatment of genetic data, biometric data or health-related data. However, this should not be an obstacle to the free circulation of personal data within the Union when such conditions apply to the cross-border processing of those data."

Thus, even in the case that the treatment is framed in the case of article 2.d) of DA 17a) of the LOPDGDD, the compatibility provided for in article 89 of the RGPD does not act as automatically but is subject to the adoption by those responsible for the treatment of the appropriate guarantees to ensure the protection of personal data.

The RGPD sets up a security system that is no longer based on the basic, medium and high security levels that were provided for in the Regulation for the deployment of the LOPD, approved by Royal Decree 1720/2007, of December 21 (RLOPD) , but by determining, based on the characteristics of the treatment and a prior risk analysis, which security measures are necessary in each case (recital 83 and article 32 RGPD).

The Addendum includes generic references to the adoption of security measures, as in section 2.e) of the general provisions ("adopt appropriate technical and organizational measures against all unauthorized or illegal treatment and evaluate periodically the suitability of said security measures, modifying them when necessary (...)").

This provision, together with others from the same section 2 of the Agreement, may be relevant from the perspective of data protection. More specifically, section 3 of the Addendum referring to "Security measures", provides that: The company "has ISO 2700:2013 certification and will maintain it during the term of validity of the Agreement and "Addendum on the treatment (...)". This same section provides, among others, that the company guarantees the control of access to information only by authorized personnel, the use of appropriate physical and logical entry controls, measures that may be appropriate in the case that concerns us It is also worth highlighting the provision of specific technical measures during the installation and maintenance of the company's server in the Hospital's premises, where they will be physically locate

Section 3.2 of the Addendum explains that the company has ISO 2700:2013 certification, and that "it will maintain this certification during the entire term of validity of the Agreen It is added that, in case of request, the company will provide the Hospital with the documentation proving this certification. Regarding this, since it is the responsibility of the person in charge to ensure compliance with the data protection regulations in matters of security, by the person in charge of the treatment, the Hospital should carry out the necessary checks not only on the availability and validity of this certification, but to ensure its adequacy and sufficiency given the risks inherent in both the nature of the data processed, the volume of information processed, the consequences it ma

Machine Translated by Google

to the persons affected by inadequate treatment or the other circumstances of the treatment.

We add that, aside from the processing of pseudonymized data from the HHCCs, the use of the Platform also involves the processing of identifying data of the users of the Platform (as part of the processing order between the Hospital and the company). It would also be appropriate to explain more clearly the technical and organizational measures tending to protect this information.

- The risk of re-identification must be avoided

The legality for the use of pseudonymized data for research purposes necessarily requires compliance with the measures established by the RGPD (article 9.2.j), in connection with article 89.1 of the RGPD).

While the RGPD considers the use of pseudonymization as a security measure that can provide an adequate guarantee for the processing of personal information (among others, recitals 28 and 156, and art. 6.4.e) and 25.1 RGPD), it is necessary to highlight, in line with what the Article 29 Working Group (WG 29) sets out in Opinion 5/2014, on anonymization techniques, that the risk of re-identification is inherent in any technique of 'anonymization, so the privacy and protection of the owner's data (in this case, especially of the Hospital's patients), could be compromised, in the event that an unauthorized reversal of the pseudonymization occurs (recitals 75 and 85 RGPD).

For each request that may be made for pseudonymised data, it will be the responsibility of the data controller to analyze prior to the communication which measures should be taken to minimize the risk of re-identification of personal information. Thus, in the event that there is a risk of re-identification, it will be necessary to deny the request or otherwise introduce sufficient guarantees to make this risk disappear.

The special nature of the information treated requires a prior analysis and a concretization by the Hospital in the choice of pseudonymization mechanisms, as it has done following the opinion of GT 29, cited, and this Authority on different occasions (CNS Opinions 34/2014 and CNS 20/2015). Given that the purpose of use by Hospital de la Plataforma consists in the treatment of pseudonymized data for research purposes (DA 17a, section 2.d) LOPDGDD), the person responsible for the treatment (in this case, the co-responsible), must articulate the technical and organizational measures necessary to guarantee, among others, respect for the principle of minimization of personal data and to avoid the risk of re-identification of the information in the terms provided for in the RGPD, given the referral to the law of the States, in DA 17a, section 2 d) f) ig) of the LOPDGDD, issues that are not sufficiently specified in the available documentation.

In accordance with the considerations made in this opinion the following are made,

Conclusions

The processing of health data of the Hospital's patients for medical research purposes by the Hospital, through the use of the Platform, may find sufficient authorization in article 5.1.b) RGPD and the Provision additional 17ª LOPDGDD, in connection with articles 9.2, section j) and 89.1 RGPD, as long as the appropriate guarantees required by the regulations are applied.

Machine Translated by Google

It is confusing to use two documents and an addendum where aspects related to data that would be treated under co-responsibility, with other aspects related to data that would be treated as part of a processing order, are often treated in a mixed manner. It should be clearly differentiated.

Specifically, the following issues should be reviewed, in the terms specified herein Opinion:

- It would be better to specify the information flows provided, especially with regard to the "advanced functions" referred to in point 2.2 of the Agreement.

- It would be advisable to better define the responsibilities of the parties involved and, where appropriate, review the use of the co-responsibility regime.

With regard to the assignment of the treatment between the Hospital and the company, and, where appropriate, the co-responsibility agreement (e.g. art. 26 RGPD), it would be advisable to systematize its content, so that they are grouped by it makes clearer the different obligations of the Hospital and the company, in both cases. It is necessary that the processing order incorporates all the sections of article 28.3 of the RGPD, in a clear and precise manner.

- An impact assessment must be carried out in the terms provided for in article 35 of the RGPD, before the start of the treatment.

- The person responsible or persons responsible must establish which specific technical measures will be used to avoid or, at least, minimize the risk of re-identification of patients by the company or by third parties (hospitals, research centers, etc.), participants in the Network, both in cases where aggregated information is provided, and in the event that, eventually, using the "advanced functions" pseudonymized information is provided.

- It is appropriate to foresee the mechanism to attend to the rights (arts. 15 et seq. RGPD) that users of the Platform can exercise, if these are addressed to the company.

Barcelona, March 31, 2020

Machine Translated