European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp 17-31
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 03

*European Data Strategy. An Approach to the European Health Data Space. The Role of the Regulation (Eu) 2022/868 of the European Parliament and of the Council of May 30, 2022 Relating to European Data Governance**

Nieves de la Serna Bilbao
(Ph Dr. Administrative Law at Universidad Carlos III de Madrid)

Fernando Fonseca Ferrandis
(Ph Dr. Administrative Law at Universidad Carlos III de Madrid)

ABSTRACT European law has enshrined for years the dogma of the confidentiality of personal data. However, in recent years it wants to modulate the strict rules that configured this right and accepts certain data traffic. Along with reasons of general interest, it is not possible to forget the economic reasons.

1. *Problem planning*

As is well known, in recent years there has been a change of focus in the data protection policy developed in the European Union. From a practically absolute sacralization of the right to data protection, the aim is now to modulate the scope of this right in such a way that its material object, i.e. data, can be put to some use for the benefit of society - we are told-.[1] This, logically, articulating the actions taken by the Member States of the European Union from this perspective. In short, the aim is to create a single European data market and, at the same time, to develop common european data spaces, all in order to promote the exchange and sharing of data. It should be emphasized that these objectives are consistent with the Treaty on the Functioning of the European Union (TFEU), which provides for the creation of an internal market and the establishment of a system to prevent distortion of competition in this market. It should be emphasized that these objectives are consistent with the TFEU, which provides for the creation of an internal market and the establishment of a system to prevent distortion of competition in that market. Let us recall that the European Data Strategy (Communication of February 19, 2020) already envisaged a so-called common European data space in which data could be used regardless of where they were physically stored within the European Union. And within this common space, the creation of common European data spaces was proposed in specific areas and, specifically, in the field of health, a circumstance that more than justifies the treatment in this context of the DGA, since, let us remember that such data are nothing other than information content, in our case, health information.[2]

Specifically, the objective of the European Health Data Space (EHDS) is to establish a

* Article submitted to double-blind peer review.

[1] On this traditional perspective see L. Cristea Uivaru, *La protección de datos de carácter sensible: Historia clínica digital y big data en salud,* Bosch, Barcelona, 2019. Vv. Aa*., Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales*, vol. I-II, Cizur Menor, Civitas/Thomson Reuters, 2021.

[2] J. Valero Torrijos, *La propuesta europea sobre gobernanza de los datos, ¿un paso adelante?* https://datos.gob.es/es/blog/la-propuesta-europea-sobre-gobernanza-de-los-datos-un-paso-adelante, 2020 and *Implicaciones jurídicas de los espacios de datos,* https://datos.gob.es/es/blog/implicaciones-juridicas-de-los-espacios-de-datos, 2023. Likewise, J. Valero Torrijos and R. Martinez Gutierrez (eds), *Datos abiertos y reutilización de la información del sector público*, Comares, Granada, 2022.

European governance framework - through the articulation of a series of common rules, criteria and practices - in relation to both a primary use of health data - use of health data to provide care to a subject - as well as with a secondary use of the same - use of data for research purposes or the development of public policies -. And from this perspective, the EHDS establishes a series of objectives aimed at this end; essentially the following: a) reinforce the patient's control over his or her data; b) regulate electronic health record systems so that they are trustworthy, secure and interoperable; c) regulate secondary use of data; d) establish two types of cross-border infrastructure depending on whether it is the primary use of secondary data or its secondary use. In short, as various authors have shown, this is a particularly ambitious policy because we are talking about specially protected data, subject to special regulation because it affects a more intimate area of the person. However, at the same time, adequate and coherent management of this information in electronic and interoperable format between the different health centers, whether they are from the same State of the European Union or from different ones, can be a benefit for the interested party themselves, for the industry and for the development of public policies.[3] We are therefore faced with the development of an essential policy given that - there is no doubt about this- the use of the economic and social potential of data - data economy - allows for a more correct and efficient reuse of the same, which, in turn, must facilitate the increase in the volume of data made available for the different uses that we mentioned above - and there is no doubt about this- taking advantage of the economic and social potential of data - data economy - allows for a more correct and efficient reuse of data, which, in turn, should facilitate the increase in the volume of data available for the different uses that we mentioned above. Note the potential that such a policy can have as a basis for transnational cooperation in certain fields of medicine such as transplantology;[4] it would be a decisive tool in the hands of organizations dedicated to the coordination of transplants such as the National Transplant Organization (ONT) or, at the European level, Eurotransplant.

However, the fact that it is ultimately about creating a market - of data and European but, in the end, a market -, a teleological purpose of whose reality is good proof of the normative provision of instrumental mechanisms - because they are at the service of the data policy analyzed in these brief pages and in which for-profit organizations can participate - and whose purpose even reaches to enable commercial use of the data obtained, raises important doubts of viability, legitimacy and legality.[5] Basically, due to the compatibility between what should be the development of a public policy such as the development and management of data protection, especially in an area such as health governed by the principle of objective service to the general interest and initiative. private sector whose cornerstone is, on the contrary and legitimately, its free development. A very basic example. When, in the context of regulated data exchanges, it is necessary to anonymize or a definitive dissociation of certain data, will the natural or legal person for commercial purposes act accordingly, in order to safeguard the right to data protection and take extreme precautions so that said anonymization or definitive dissociation is true and real? Regardless of even the economic cost of ensuring said result? Or, on the contrary, will you care more about your profits and therefore care less about the absolute protection of the right to data protection? Remember that we are talking about organizations that act for commercial purposes. We are certainly not talking about anything new. This is a problem that has manifested itself years ago in the different processes of privatization and deregulation of certain economic areas operated in all the countries around us and in which European law has had a resounding impact.[6] The new element is the area in which it is raised. As we already know, the field of data protection and,

[3] In this sense, see F. García Pérez*, Introducción al espacio europeo de datos sanitarios: un nuevo horizonte en la Gobernanza de Datos Sanitarios en la Unión Europea*, in *Actualidad Jurídica Uría Menéndez*, vol. 61, 2023, 183-196. Also, J. Marcus Scott, *The European Health Data Space, Think Tank European Parlament*, PE 740.054, December 2022.

[4] Concept used by R. Matesanz Acedos, *El milagro de los trasplantes*, Madrid, *La Esfera de los Libros S.L.*, 2006, 39.

[5] D. Ruano Delgado and N. Philipia, *Tratamiento seguro de datos como factor de integración europea: implicaciones legales en el ámbito de la salud pública en Georgia*, in *Revista de derecho y genoma humano*, no. 1, 2019, 525-546.

[6] On these issues see M.N. De La Serna Bilbao, *La privatización en España. Fundamentos Constitucionales y Comunitaruios*, Aranzadi, Pamplona, 1995.

in our case, in a particularly delicate area due to its relationship with our strictest personal privacy such as health.

On the other hand, even in the data exchange procedures that are developed based on the principle of altruism or gratuity - it would be good for the standard under development to specify the scope of said concepts - we are going to find that society - which is the source of all processed health data, whatever the scope of said treatment, will be deprived of the economic benefit produced by the mere possession of health data and which we can consider as "Informational Value." It is enough to know what happened in Iceland in the late 1990s to realize the magnitude of the problem. Indeed, it is not only that instruments are not provided to ensure that society also enjoys a certain return on achievements obtained with its data free of charge - this is not even considered. The enjoyment will be in the vast majority of cases through compensation, either direct, if the patient directly uses certain medical treatments - precisely those that derive from research developed from data obtained free of charge- or indirect, if the patient uses the benefits of public health services which, in turn, will have purchased the corresponding treatments from the different laboratories involved in the research. In accordance with the norm and apart from some health benefits that are a consequence of the development of certain public health policies, the only case in which citizens can avail themselves free of charge of the medical advances produced from the information that they themselves generate is that they participate in a clinical trial. There's no more. Surely, given the prevalence of community law, this paradigm shift must be accepted; that the right to our health data protection is not going to be what it was. But you have to be aware of it. However, it is surprising that this is the case, when the European Union has never played a relevant role in health matters.

In this context, Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1714 (Data Governance Act) [DGA] makes sense, which seeks to introduce common standards and practices among the Member States of the European Union that allow the creation of a harmonized framework in which to develop a common data governance policy, in addition, fully respectful of fundamental rights.[7] In any case, it should be noted that the European data governance policy does not oblige public sector bodies to allow the transfer of data, nor does it exempt them from their confidentiality obligations. For this reason, the development of this policy should be without prejudice to the law of the European Union, the national law of each Member State or international agreements relating to the protection of the data that constitute the material object of the EDPR and to which the European Union or its Member States are party. Furthermore, the development of this policy should be without prejudice to European Union or national law on access to documents, as well as to the obligations of public sector bodies to authorize the re-use of data under European Union or national law of the Member States (art. 3.3 DGA).[8]

[7] About this question see A. Cerrillo i Martinez and M. Ascensión Moro Cordero, *El Reglamento de Gobernanza de Datos y su impacto en las administraciones públicas, Consultor de los ayuntamientos y de los juzgados*, in *Revista técnica especializada en administración local y justicia municipal*, no. 8, 2022, 1128-1135; C. Fernández Hernández*, Estructura y contenido del Reglamento (UE) 2022/868, de 30 de mayo, relativo a la gobernanza europea de datos o Reglamento de Gobernanza de Datos*, Diario La Ley nº 62 (Sección Ciberdecho), 7 de junio de 2022, Wolter Kluwer, 96; S. Leguinagoicoa García*, Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo Europeo y dle Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de dato sy por el que se modifica el Reglametno (UE) 2018/1274 (Reglamento de Gobernanza de Datos)*, in *Revista Vasca de Gestión de Personas y Organizaciones públicas*, no. extra 5, 2023, 166-169; R. Martínez Martínez, *Data Governance Act: La construcción de un espacio europeo del dato*, in *Ley de Privacidad*, no. 9, 2021, 3 and R. Martínez Martínez, G. López Serrano, A. Padín Vidal and I. del Hoyo Alegria, *HealthData 29: un modelo de compartición de datos de investigación en salud en el contexto del futuro Espacio Europeo de Datos de Salud*, in *Comunicaciones en propiedad industrial y derecho de la competencia*, vol. 93, 2021, 5-30.

[8] It should be noted that the analyzed rule is without prejudice to Regulations (EC) n. or 223/2009, (EU) 2018/858 and (EU) 2018/1807, as well as Directives 2000/31/EC, 2001/29/EC, 2004/48/EC, 2007/2/EC, 2010/40/EU, (EU) 2015/849, (EU) 2016/943, (EU) 2017/1132, (EU) 2019/790 and (EU) 2019/1024 of the European Parliament and of the Council, and any other sectoral Union legislation regulating access to and re-use of data, as well as without prejudice to Union and national law on access to and use of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as international cooperation in that context. Likewise, the EDPR should be without prejudice to the competences of the Member States with

It should be noted that in this paper we focus our attention on the three central pillars of the regulation, i.e. the reuse of certain categories of data held by public sector bodies, the provision of data intermediation services and, finally, the transfer of data for altruistic purposes. In doing so, we wish to highlight these truly substantive institutions outside the regulation of other matters of a purely instrumental nature. Let us now analyze each of them.

2. *The Reuse of certain categories of data held by public sector organizations*

2.1. *Definition and material scope*

The European Union has traditionally considered that data generated from public budgets should benefit society. It is for that reason that Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and reuse of public sector information (DDA) mandates the public sector to make as much data as possible readily available for use and use. Despite that desire, there are certain categories of data - for the time being, commercially confidential data, data covered by statistical confidentiality, data protected by third party intellectual property rights and personal data - protected both by European Union law and by the domestic law of the Member States that are logically not available for general use.[9]

It is precisely these categories of data that constitute the object of the first of the three data transfer mechanisms analyzed. This concerns the reuse of certain categories of protected data held by public sector bodies, i.e. the use, by natural or legal persons, of such data for commercial or non-commercial purposes other than the initial purpose encompassed in the public service mission for which the data were produced. An exception is made for the exchange of data between public sector bodies for the sole purpose of carrying out their public service activities. Specifically, such a re-use mechanism applies to data protected for the following reasons:

a) Commercial confidentiality, including commercial, professional or business secrets.
b) Statistical confidentiality.
c) Protection of intellectual property rights of third parties.
d) Protection of personal data, insofar as such data are excluded from the scope of Directive (EU) 2019/1024.

In parallel, a significant number of categories of data are excluded from the material scope of the DGA; expressly the following categories of data:

a) Data held by public companies - given that these organizations are not part of the definition of public sector body.
b) Data held by public broadcasting organizations, and their subsidiaries, as well as data held by other organizations and their subsidiaries for the performance of a public service broadcasting mission.
c) Data kept by cultural centers - libraries,

regard to their activities in the field of public security, defense and national security. For example, the re-use of data protected on those grounds and held by public sector bodies, including data obtained in public procurement procedures falling within the scope of Directive 2009/81/EC of the European Parliament and of the Council, should not be covered by this Regulation.
Furthermore, the DGA is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 of the European Parliament and of the Council, as well as Directives 2002/58/EC and (EU) 2016/680 of the European Parliament and of the Council and corresponding provisions of national law, including personal data and non-personal data in a data set that are inextricably linked. In particular, the GDPR should not be interpreted as establishing a new legal basis for the processing of personal data for any of the regulated activities or modifying the information requirements provided for in Regulation (EU) 2016/679. Its application should not prevent cross-border transfers of data in accordance with the provisions of Chapter V of Regulation (EU) 2016/679. In the event of a conflict between the provisions of this Regulation and Union law on the protection of personal data or national law adopted in accordance with Union law on the matter, the Union or national law applicable in the matter should prevail.

[9] Thus, along with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, we have to cite Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA]. At the domestic level, it is necessary to abide by the provisions of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights and Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and enforcement of criminal penalties.

archives, museums, orchestras, operas, ballets and theaters - and educational institutions. In these cases, the works and other documents in their possession are mainly protected by the intellectual property rights of third parties.

d) Data kept for reasons of national security, defense or public safety.
e) Also excluded are data the provision of which is an activity outside the scope of the public service mission of the public sector bodies concerned as defined in the legislation or other binding rules of the Member State or, in the absence of such rules, as defined in accordance with the common administrative practice of that Member State, provided that the scope of the public service mission is transparent and subject to review.

It seems appropriate to specify, for the purpose of delimiting our object of study, that public sector organizations are understood to be any organization that meets the following characteristics:

a) First, it must have been created specifically to satisfy needs of general interest and not be of an industrial or mercantile nature;
b) Secondly, it must be endowed with legal personality;
c) Finally, it must be financed, for the most part, by State, regional or local authorities or other bodies governed by public law, the management of which is subject to the supervision of such authorities or bodies, or more than half of the members of its administrative, management or supervisory body must have been appointed by State, regional or local authorities or by other bodies governed by public law.

Although it does not seem necessary to have an impact on this issue, in our we have to be to the provisions of Law 40/2015, of October 1, on the Legal Regime of the Public Sector in order to finalize the concurrence in the specific case of such teleological, subjective and financial requirements.

It is, on the contrary, to specify that the data re-use regime must be applied to data whose provision is part of the entrusted public service mission - defined, case by case or in general - of the public sector bodies concerned, as provided for in the domestic legislation of the Member States. In the absence of such rules, the public service mission should be defined in accordance with the common administrative practice of the Member States, provided that the scope of the mission is transparent and subject to review. In any case, due to the nature of these data - sensitive data- the DGA subjects their transfer to strict compliance with legal and technical requirements, aimed at safeguarding the rights of the data subjects, which we analyze below.

2.2. *Applicable legal regime*

In determining how the re-use of data held by public sector bodies should be carried out, the essential idea of the European data governance policy is, as we already know, respect for competition law. For this reason, the conclusion of agreements that may have as their direct or indirect object the recognition of exclusive rights for the reuse of data must be avoided. This is provided for in Article 4.1 of the DGA when it expressly states "Agreements or other practices relating to the reuse of data held by public sector bodies containing categories of data in Article 3.1 granting exclusive rights or having the effect of granting exclusive rights or restricting the availability of the data for reuse by entities other than the parties to such agreements or practices are prohibited". Recall that the categories of data referred to in Article 3.1 of the DGA are those retained by public sector bodies that are protected for reasons related to commercial confidentiality, statistical confidentiality, intellectual property and personal data protection.

There is, however, a very qualified exception to this general rule. Indeed, where it is necessary for the provision of a service or a product of general interest, it is possible to grant an exclusive right for the re-use of this kind of data, where the provision of such a service or supply would otherwise not be possible (Art. 4.2 DGA). Recital 13 gives a concrete example of the legal provision and refers to the hypothesis that the exclusive use of the data is the only way to optimize its social benefits; for example, when there is only one entity - specializing in the processing of a specific set of data - capable of providing the service or offering the product that allows the public sector body to provide an advanced digital service in the interest of all. This possibility is equally plausible in the biomedical field where only a small number of laboratories or industries are able to articulate the highly complex treatments based on artificial intelligence. In any case, the recognition of such exclusive rights is not

free. It can be done by means of an administrative act or contractual provision but in accordance with the applicable Union or national law of the Member States - including the relevant State aid rules - and in compliance with the principles of transparency, equal treatment and non-discrimination (Art. 4.3 DGA).

These are not the only precautions established in this regard. The following should also be noted:

a) First, the maximum duration of an exclusive right to reuse data is twelve months, which is a substantial reduction with respect to the period initially in the proposal, which was three years. This is a provision that is more in line with the general rule and with the principle of competition. When a contract is concluded, the duration of the contract must be the same as that of the exclusive right (art. 4.4 DGA).
b) The granting of an exclusive right in application of the above considerations - including the reasons why it is necessary to grant it - must be made in a transparent manner and must be publicly disclosed online, in a manner consistent with the relevant Union law on public procurement (Art. 4.5 DGA).
c) Agreements should be subject to a periodic review based on a market analysis in order to determine whether such exclusivity is still necessary.

Where an exclusive right to re-use data does not comply with this Regulation, such exclusive right should be considered as null and void.

On the other hand, it should be emphasized that since the re-use of some categories of protected data - we already know, those referred to in Art 3.1) DGA- constitutes the teleological element of the European Data Governance Policy and given, also, that the development of the same cannot be developed freely except in accordance with the provisions of the European Union and of the Member States themselves, it seems clear that a core element of such a policy must be the establishment of the criteria or conditions to be met in order to make possible the intended reuse of data, aimed at protecting the rights and interests of third parties, safeguarding the interests of those who reuse the data and without this entailing a disproportionate effort for the public sector. Such regime is understood, moreover, without prejudice to the rights and obligations of the regime of access to such data

Public sector bodies which, under national law, are competent to grant or refuse access for re-use of one or more of the categories of data referred to in Article 3.1) of the DGA must publish the conditions under which re-use is allowed. For this purpose, they may be assisted by the competent bodies referred to in Article 7.1). In addition, Member States must ensure that the public sector bodies referred to have the means and resources to perform this function. It is, therefore, an instrumental obligation - insofar as it is aimed at making the conditions for the re-use of data feasible - but, at the same time, directly related to legal certainty.

As regards the actual wording of the conditions for reuse, it should be pointed out that, in general, they must be non-discriminatory, proportionate, objectively justified in terms of the categories of data, the purposes of reuse and the nature of the data in question and, furthermore, they may not be established to restrict free competition. However, public sector bodies may impose the use of certain technical means aimed - exclusively - at guaranteeing the rights and interests of third parties in relation to the data. Hence, the possibility of imposing the obligation that only pre-processed data be used for re-use, when the purpose of the pre-processing is to anonymize or pseudonymize personal data or to delete confidential commercial information, in particular trade secrets.

Likewise, public sector bodies must ensure, in accordance with Union and national law, that the protected nature of the data is preserved and, in this regard, may impose the following obligations:

a) That access for re-use of the data is granted only where the public sector body or competent body, following a request for re-use, has ensured that the data have been anonymized, in the case of personal data, and modified, aggregated or processed by any other method of disclosure control, in the case of commercially sensitive information, including trade secrets or proprietary content.
b) That the remote access and reuse of the data is carried out in a secure processing environment provided or controlled by the public sector body.

c) That the access and re-use of the data is carried out in the physical premises where the secure processing environment is located in accordance with strict security standards, provided that remote access cannot be enabled without jeopardizing the rights and interests of third parties.

Where re-use is permitted - in accordance with paragraph 3 b) and c) above- public sector bodies should impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body must reserve the right to verify the process, means and results of data processing carried out by the reuser in order to preserve the integrity of data protection and must reserve the right to prohibit the use of those results that contain information endangering the rights and interests of third parties. The decision to prohibit the use of the data must be understandable and transparent to the reuser.

3. *Data Exchange Services*

3.1. *Definition and material scope*

The DGA establishes a comprehensive legal regime applicable to data intermediation activities, which is generally applicable except in the case of recognized data management organizations for altruistic purposes or other non-profit entities, provided that their activities consist of the collection of data provided for altruistic purposes by natural or legal persons for the fulfillment of general interest purposes. This exception to the general rule does not apply, however, when the purpose of such organizations and entities is to establish commercial relations between an undetermined number of data subjects and data owners, on the one hand, and data users, on the other. Well then, going into the matter properly, it should be stated that, in accordance with the provisions of the DGA, the following services are considered to be data intermediation services:

a) Intermediation services between data owners and potential data users, including the provision of technical or other means to enable such services. These services may include the bilateral or multilateral exchange of data or the creation of platforms or databases that enable the exchange or sharing of data, as well as the establishment of other specific infrastructure for the interconnection of data owners with data users;
b) Intermediation services between data subjects wishing to provide their personal data or natural persons wishing to provide non-personal data and potential data users, including the provision of the technical or other means necessary to enable such services, and in particular to enable the exercise of data subjects' rights provided for in Regulation (EU) 2016/679;
c) Finally, Data cooperative services. We still don't know very well how this system will operate.

3.2. *Applicable legal regime*

It should then be noted that the above-mentioned intermediation services are also subject to a notification procedure, the regime of which is described below. It should be noted that any data brokering service provider intending to provide the data brokering services referred to above (Article 10 DGA) must submit a notification to the competent authority for data brokering services. According to the text of the DGA, this is an unavoidable obligation; only after the data brokering service provider has submitted the notification can it start its activity, and it should be noted that it entitles it to provide data brokering services in all EU Member States. For these purposes, a data brokering service provider established in more than one Member State is considered to be subject to the legal system of the Member State of its main establishment, without prejudice to Union law governing cross-border actions for damages and related proceedings. Providers of data brokering services which are not established in the Union and which offer in the Union the data brokering services referred to in Article 10 of the DGA must appoint a legal representative in one of the Member States in which such services are offered.[10]

[10] In accordance with the provisions of Article 11 DGA "For the purposes of this Regulation, a data intermediation services provider with establishments in more than one Member State shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment, without prejudice to Union law regulating cross-border actions for damages and related proceedings". Likewise "The data intermediation services provider shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative by the data intermediation services provider shall be without prejudice to any legal actions which could be initiated against the data intermediation services provider".

The notification must include the following information:

a) Name of the data brokering service provider.
b) The legal nature of the data brokering service provider, as well as its legal form, ownership structure, relevant subsidiaries and, where the data brokering service provider is registered in a commercial register or similar national public register, its registration number.
c) Address of any principal place of business of the data brokering service provider in the Union and, where applicable, of any branch in another Member State, or address of its legal representative.
d) Public website containing complete and up-to-date information on the data brokering service provider and on its activities, including at least the information referred to in points a), b), c) and f) of Article 11 of the DGA.
e) Contact persons of the data brokering service provider and contact details.
f) Description of the data brokering service that the data brokering service provider intends to provide and indication of the categories listed in Article 10 to which the data brokering service corresponds.
g) An estimate of the date of commencement of the activity, if different from the date of notification.

Likewise, any modification of the information submitted must be notified, as well as the cessation of activity.

The competent authority for data intermediation services is subject to a series of obligations to be fulfilled at the request of the data intermediation service provider. First, it must issue - within one week of the notification being duly and fully submitted - a standardized statement confirming that the data brokerage service provider has submitted the notification and that the notification contains the required information. Secondly, it must confirm that the data brokerage service provider complies with the provisions of the DGA. Only thereafter, upon receipt of such confirmation, the data brokerage service provider may now use, in its oral and written communications, the designation "data brokerage service provider recognized in the Union", as well as a common logo. Finally, it must inform the Commission electronically and without delay of each new notification. To this end, the Commission must keep a regularly updated public register of all data brokering service providers providing services in the Union. The information required in paragraph 6 a), b), c), d), f) and g) must be published in the public register. In any case, the competent authority for data brokering services must ensure that the notification procedure is non-discriminatory and must not distort competition.

Apart from the above, the provision of data brokering services by the relevant providers is subject to compliance with the following conditions:

a) They may not use the data in relation to which they provide their services for purposes other than making them available to data users and shall provide the data brokering services through a separate legal entity.
b) The commercial contractual terms, including those relating to pricing, for the provision of data brokering services to a data subject or data user may not depend on whether the data subject or data user uses other services provided by the same data brokering service provider or by an entity related to it, and, if used, may not depend on the extent to which the data subject or data user uses such services.
c) Data collected on any activity of a natural or legal person for the purpose of providing a data brokering service, including date, time and geolocation, duration of the activity and connections that the user of the data brokering service establishes with other natural or legal persons, may only be used for the performance of that data brokering service, which may involve the use of data for fraud detection or cybersecurity purposes and must be made available to data subjects upon request.
d) Data should be exchanged in the same format in which they are received from the data subject or data owner. As an exception to this general rule, specific formats may only be adopted for the purpose of improving intra- and inter-sectoral interoperability; when requested by the data user; if required by Union law; or when necessary for the purpose of harmonization with international or European data standards. In all such cases, data subjects or data subjects should be offered an opt-out possibility in relation to

such conversions, unless such conversion is required by Union law; or where necessary for the purpose of harmonization with international or European data standards. In all such cases, data subjects or data subjects should be offered an opt-out possibility in relation to such conversions, unless such conversion is required by Union law.

e) Data brokering services may include the offer of additional specific tools and services to data subjects or data subjects for the specific purpose of facilitating the exchange of data, for example, temporary storage, organization, conversion, anonymization and pseudonymization, provided that such tools and services are only used upon the express request or approval of the data subject or data subject and that the third-party tools offered in this context are not used for other purposes.
f) It should be ensured that the procedure for access to data brokering services, including prices and terms of service, is fair, transparent and non-discriminatory, both for data subjects and for data subjects and data users.
g) Data brokering services should have procedures in place to prevent fraudulent or abusive practices by parties seeking access through their data brokering services.
h) Providers of data brokering services should ensure, in the event of insolvency, reasonable continuity in the provision of their data brokering services and, where such data brokering services include the storage of data, should have in place the necessary safeguards to enable data subjects and data users to access, transfer or retrieve their data and, where they provide such data brokering services between data subjects and data users, to enable data subjects to exercise their rights;
i) appropriate measures should also be taken to ensure interoperability with other data brokering services, inter alia, through open standards commonly used in the industry in which data brokering service providers operate.
j) Data brokering service providers should implement appropriate technical, legal and organizational measures to prevent access to or transfer of non-personal data where such access or transfer is unlawful under Union law or the national law of the Member State concerned.
k) Data subjects should be informed without delay in case of unauthorized transfer, access or use of non-personal data that they have shared.
l) Necessary measures must be taken to ensure an adequate level of security in relation to the storage, processing and transmission of non-personal data. Likewise, they must ensure the highest level of security in relation to the storage and transmission of competitively sensitive information.
m) Where data brokering service providers offer services to data subjects, they should act in the best interests of the data subjects when facilitating the exercise of their rights, in particular by informing and, where appropriate, advising them in a concise, transparent, intelligible and easily accessible manner about the intended uses of the data by data users and the general conditions applicable to such uses before the data subjects give their consent.
n) Where data brokering service providers provide tools to obtain data subjects' consent or permission to process data provided by data subjects, they shall specify - where applicable - the territory of the third country in which the data are intended to be used and shall provide data subjects with tools both to grant and withdraw their consent, and data subjects with tools both to grant and withdraw permissions to process data.
o) Finally, data brokering service providers must keep a record of the data brokering activity artificial intelligence

In any case, the competent authorities for data intermediation services must control and supervise compliance with the requirements to be met by data intermediation service providers. Likewise, at the request of a natural or legal person, they may control and supervise such compliance by data brokering service providers. To this end, they are empowered to request from data brokering service providers or their legal representatives any information necessary in order to verify compliance with the requirements of this Chapter. Requests for information must be proportionate to the performance of their duties and be reasoned. To this end, the DGA provides that when the competent authority for data intermediation services considers that a data intermediation service provider does not comply with one or more of the requirements of this chapter, it must notify it

of its observations and the latter must express its opinion on the matter within thirty days of receipt of the notification. Likewise, the competent authority for data intermediation services is empowered to require the cessation of infringements involving non-compliance with the legal requirements within a reasonable period of time or, in the case of serious infringements, immediately, taking appropriate and proportionate measures to ensure compliance. In this regard, the competent authority for data intermediation services is empowered to adopt the following measures:

a) Impose, through administrative proceedings, dissuasive financial penalties, which may include periodic penalty payments and penalties with retroactive effect, initiate legal proceedings for the imposition of fines, or both.
b) Require a postponement of the commencement or a suspension of the provision of the data brokering service until the conditions have been modified as requested by the competent authority for data brokering services.
c) Demand the cessation of the provision of the data brokering service in case of serious or repeated breaches that have not been corrected despite prior notification.

In such cases, the competent authority for data brokering services must request the Commission to cancel the registration of the data brokering service provider from the register of data brokering service providers, once it has ordered the cessation of the provision of the data brokering service. However, if the data brokering services provider remedies the infringements, it may make a new notification to the competent data brokering services authority, which must be communicated by the competent data brokering services authority to the Commission.

In adition, it should also be noted that where a data brokering services provider that is not established in the Union fails to designate a legal representative or the legal representative of the latter fails to provide, upon request of the competent data brokering services authority, the necessary information comprehensively demonstrating compliance with the DGA, the competent data brokering services authority may postpone the commencement or suspend the provision of the data brokering service until a legal representative is designated or the necessary information is provided. These authorities must promptly notify the data brokering service provider concerned of the measures imposed, the grounds on which they are based and the necessary measures to be taken to remedy the deficiencies concerned, and set a reasonable period of time, not exceeding 30 days, for the data brokering service provider to comply with the measures imposed.

If the principal establishment or the legal representative of a data brokering services provider is located in a given Member State but the provider provides its services in other Member States, the competent authority for data brokering services of the Member State of its principal establishment or in which its legal representative is located and the competent authorities for data brokering services of the other Member States shall cooperate with each other and provide mutual assistance. Such assistance and cooperation may cover the exchange of information between the competent authorities for data brokering services concerned for purposes related to their functions under the GDPR and reasoned requests for the measures referred to in the DGA to be taken.

It should be noted that where a competent authority for data intermediation services of one Member State requests assistance from a competent authority for data intermediation services of another Member State, it must submit a reasoned request. The competent data intermediation authority receiving such a request shall respond without delay and within a time limit proportionate to the urgency of the request.

4. *The Altruistic Transfer of Data*

4.1. *Definition and material scope*

Irrespective of all the above possibilities, the DGA nevertheless facilitates the transfer of certain types of data when such transfer is altruistic in nature and therefore free of charge. To this end, the DGA establishes a general empowerment in the sense that the Member States may establish organizational and/or technical provisions to facilitate the altruistic transfer of data, and may even draw up national policies on the altruistic transfer of data aimed at assisting data subjects in the voluntary transfer, for altruistic purposes, of personal data relating to them held by public sector bodies and at establishing the necessary

information to be provided to data subjects in relation to the re-use of their data for purposes of general interest. To this end, the DGA establishes a series of provisions that we analyze below.

4.2. *Applicable legal regime*

All authorities competent for the registration of data management organizations for altruistic purposes must periodically update a national public register of recognized data management organizations for altruistic purposes. Provided that the entities are entered in the national public register of recognized data management organizations for altruistic purposes, they may use, in their oral and written communications, the designation "data management organization for altruistic purposes recognized in the Union", as well as a common logo.[11] Likewise, the Commission should keep a public register of recognized data management organizations for altruistic purposes in the Union, albeit for information purposes.

In any case, in order for data management organizations for altruistic purposes to be entered in a national public register, they must meet the following requirements:

a) Exercise altruistic data transfer activities.
b) be a legal entity established under national law to fulfill objectives of general interest, as provided for in national law, where applicable.
c) It shall operate on a not-for-profit basis and shall be legally independent of any entity operating on a for-profit basis.
d) To carry out the altruistic data transfer activities through a structure that is functionally separate from its other activities.
e) Comply with the regulatory code referred to in Article 22, paragraph 1, no later than eighteen months after the date of entry into force of the delegated acts referred to in that paragraph.

It should also be noted that any entity that meets the requirements of Article 18 of the analyzed rule may apply for registration in the national public register of recognized data management organizations for altruistic purposes in the Member State in which it is established. In addition, when these entities have establishments in more than one Member State, they may apply for entry in the national public register of recognized data management organizations for altruistic purposes in the Member State in which they have their main establishment. In the case of entities that meet the requirements of Article 18 but are not established in the Union, they must designate a legal representative in one of the Member States in which they offer their altruistic data management services.

For the purpose of ensuring compliance with the DGA, the entity must give a mandate to the legal representative to be addressed by the competent authorities for the registration of data management organizations for altruistic purposes or by data subjects and data subjects instead of or in addition to the entity, in all matters concerning the entity. From this perspective, the legal representative has to cooperate with the competent authorities for the registration of data management organizations for altruistic purposes and must demonstrate to them in a comprehensive manner, upon request, the measures and arrangements taken by the entity to ensure compliance with the DGA. The entity is deemed to be subject to the legal system of the Member State in which its legal representative is located. Such an entity may apply for registration in the national public register of recognized data management organizations for altruistic purposes in that Member State. The designation of a legal representative by the entity should be without prejudice to any legal action that may be brought against the entity.

The applications for registration referred to in the preceding paragraphs should include the following data:

a) Name of the entity.
b) Legal nature of the entity, as well as its legal form and, when it is registered in a national public registry, its registration

[11] Let us remember that in accordance with the provisions of Article 17 DGA "The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes. Provided that an entity is registered in the public national register of recognised data altruism organisations in accordance with Article 18, it may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as a common logo […]. In order to ensure that recognised data altruism organisations are easily identifiable throughout the Union, the Commission shall, by means of implementing acts, establish a design for the common logo. Recognised data altruism organisations shall display the common logo clearly on every online and offline publication that relates to their data altruism activities. The common logo shall be accompanied by a QR code with a link to the public Union register of recognised data altruism organisations".

number.
c) Statutes of the entity, if applicable.
d) Sources of income of the entity.
e) Address of any principal establishment of the entity in the Union and, where appropriate, of any branch in another Member State, or address of its legal representative.
f) Public website containing complete and up-to-date information about the entity and its activities, including at least the information referred to in points a), b), d), e) and h) above.
g) The entity's contact persons and contact details.
h) Objectives of general interest that the entity intends to promote with the collection of the data.
i) Nature of the data that the entity intends to control or process and, in the case of personal data, indication of the categories of personal data.
j) Any other document evidencing compliance with the requirements of Article 18.

Once the entity has submitted all this information and once the competent authority for registration of data management organizations for altruistic purposes has assessed the application for registration and found that the entity meets the requirements, the authority must proceed to register the entity in the national public register of recognized data management organizations for altruistic purposes within twelve weeks after receipt of the application for registration and must be notified to the Commission. In addition, it must be included in the Union's public register of recognized data management organizations for altruistic purposes. The registration is valid in all Member States.

In any case, the recognized data management organizations for altruistic purposes must notify the corresponding competent authority for entry in the register of data management organizations for altruistic purposes of any modification of the information submitted within fourteen days from the day of the modification. Likewise, the competent authority for the registration of data management organizations for altruistic purposes has to inform electronically and without delay the Commission of each such notification which must update without delay the Union public register of recognized data management organizations for altruistic purposes.

For the purposes of compliance with the transparency policy, it should be noted that the DGA establishes a twofold obligation for recognized data management organizations for altruistic purposes. On the one hand, they must keep a complete and accurate record of the following elements:
a) All natural or legal persons who have been permitted to process data held by that recognized data management organization for altruistic purposes, and their contact details.
b) The date or duration of the processing of personal data or the use of non-personal data.
c) The purpose of the data processing declared by the natural or legal persons to whom the data processing has been permitted.
d) Any fees paid by the natural or legal persons carrying out the data processing.

Irrespective of the above, the aforementioned organizations must prepare and transmit to the relevant authority competent for registration in the register of data management organizations for altruistic purposes an annual activity report, which must include at least the following data:
a) Information on the activities of the recognized data management organization for altruistic purposes.
b) A description of the manner in which the general interest purposes for which the data were collected have been promoted during the financial year in question.
c) List of all natural and legal persons who have been allowed to process data held by the entity, including a brief description of the general interest purposes pursued by the processing of the data and a description of the technical means employed for this purpose, with a description of the techniques applied to preserve privacy and data protection.
d) Summary of the results of the data processing permitted by the recognized data management organization for altruistic purposes, if applicable.
e) Information on the sources of income of the recognized non-profit data management organization, in particular, all income derived from providing access to the data, and on its expenses.

Specific requirements to protect the rights and interests of data subjects and data owners

with regard to their data.

All recognized data management organizations for altruistic purposes must also inform data subjects or data subjects, in a clear and easy to understand manner, prior to any processing of their data, about two circumstances. First, about the general interest purposes and, where appropriate, the specific, explicit and legitimate purposes for which the personal data will be processed, and for which they allow their data to be processed by a data user. Secondly, in relation to the location of any processing activity carried out in a third country and the general good purposes for which it is permitted, where the processing is carried out by the recognized altruistic data management organization itself. Data obtained by such organizations should not be used for purposes other than those in the general interest for which the data subject or data subject permits the processing, nor should they use misleading marketing practices to solicit the provision of data. They must provide tools to obtain data subjects' consent or permission to process data provided by data subjects and also provide tools to easily withdraw such consent or permission.

Whatever the case, these organizations must take the necessary measures to ensure an adequate level of security in relation to the storage and processing of non-personal data that they have collected for the purpose of altruistic data transfer. And, from the same perspective, they must inform data subjects without delay in case of unauthorized transfer, access or use of the non-personal data they have shared. It should be emphasized that when the recognized altruistic data management organization facilitates the processing of data by third parties, in particular by providing tools to obtain the consent of data subjects or permission to process data provided by data subjects, it shall specify, where appropriate, the territory of the third country in which the data are intended to be used.

It is foreseen that by means of delegated acts issued by the Commission, a regulatory code complementary to the DGA will be created, which for these purposes should be comprehensive of the following issues:

a) Adequate information requirements to ensure that data subjects and data subjects are provided, prior to granting their consent or permission for altruistic data transfers, with sufficiently detailed, clear and transparent information on the use of the data, the tools for granting and revoking consent or permission, and the measures taken to prevent misuse of data shared with the data management organization for altruistic purposes.
b) Adequate technical and security requirements to ensure an appropriate level of security of data storage and processing, as well as tools for granting and withdrawing consent or permission.
c) Communication roadmaps adopting a multidisciplinary approach to raise awareness among relevant stakeholders, in particular data subjects and data subjects who might share their data, about altruistic data sharing, the designation as a "Union-recognized altruistic data management organization" and the regulatory code.
d) Recommendations on relevant interoperability standards. Competent authorities for the registration of altruistic data management organizations.

The competent authorities for the registration of data management organizations for altruistic purposes are those designated by each Member State and must comply with the general requirements established by the DGA. The identity of each of these authorities, as well as their subsequent modification, must be notified to the Commission. In any case, they must perform their functions in cooperation with the relevant data protection authority, where such functions relate to the processing of personal data, and with the relevant sectoral authorities of that Member State.

It should be noted that these authorities are also the competent bodies to monitor and supervise compliance with the requirements of the DGA by recognized data management organizations for altruistic purposes, either ex officio or at the request of a party. To this end, they are also empowered to request from the recognized data management organizations for altruistic purposes all the information necessary to verify compliance with the requirements of regulation analyzed in these brief pages. In this regard, it provides that when a competent authority for the registration of data management organizations for altruistic purposes considers that a recognized data management organization for altruistic purposes does not comply with one or more of the requirements provided for in the DGA, it must notify it of its observations and grant it a period - of thirty days from the

receipt of the notification - to express its opinion on the matter. If a breach is found to exist, it may require cessation of the breach, either immediately or within a reasonable period of time, and must take appropriate and proportionate measures to ensure compliance.

Recognized altruistic data management organizations that fail to comply with one or more of the requirements determined in the DGA, even after having received from the competent authority for registration in the register of altruistic data management organizations is subject to the following consequences:

a) Loss of the right to use the denomination "data management organization for altruistic purposes recognized in the Union", in its oral and written communications;
b) Cancellation of its registration in the corresponding national public register of recognized data management organizations for altruistic purposes and in the Union public register of recognized data management organizations for altruistic purposes.

In any case, it should be noted in this regard that decisions to revoke the right to use the name of a data management organization for altruistic purposes must be made public. In addition, it should be specified that where a recognised altruistic data management organisation has its head office or its legal representative in a Member State but carries on its activities in other Member States, the competent authority for entry in the register of altruistic data management organisations of the Member State of its head office or legal representative and the competent authorities for entry in the register of altruistic data management organisations of those other Member States should cooperate with each other and assist each other. Such assistance and cooperation may cover the exchange of information between the competent authorities for the registration of the data management organisations for altruistic purposes concerned for purposes related to their tasks under European regulation and to reasoned requests for appropriate measures to be taken. All information exchanged in the context of the request and the provision of assistance should be used only in relation to the matter for which it was requested.

Finally, it should be noted that in order to facilitate the collection of data transferred for altruistic purposes, a "European Consent Form for Altruistic Data Transfer" - adopted by Commission delegated acts - is foreseen to enable data subjects to prove consent and its withdrawal in respect of a specific data processing operation in accordance with the requirements of Regulation (EU) 2016/679. The form should be made available in a way that allows it to be printed on paper and is easy to understand, as well as in an electronic and machine-readable format. Furthermore, it must allow its adaptation to specific sectors and different purposes.

5. *Conclusion*

European Data Governance and specifically in the field of health data, has proceeded to rethink its core ideas that have traditionally informed it. In effect, the new community rules aim to create a European data market - based on the so-called common European spaces - that allow the exchange of data and its sharing - we are told - in a manner that is fully respectful of the fundamental rights of the person. With this objective, the DGA has foreseen three legal mechanisms of different scope and intention but that can operate complementary, such as the Reuse of certain categories of data held by public sector organizations, the Data Exchange Services and the Altruistic Transfer of Data.

It is necessary to highlight that these data exchange systems introduce different elements of the market and that they give rise to private initiative, which, while not objectionable in themselves, while they can effectively contribute to energizing the data market, can introduce important distortions. in the operation of what a data protection policy should be, especially in an area as delicate as health. Indeed, as such a market will be governed by the expectation of profit. There is no need to be deceived in this assessment. However, remember that, in our case, we are talking about a special category of data due to its greater connection with the personal privacy of the person and, for this reason, it has traditionally enjoyed reinforced protection.

Experience shows that it is very difficult to marry public policy - data protection and health - and private interest. The stimuli of both, general interest, on the one hand, and free development and benefit, on the other hand, are in themselves contradictory. In our case, it is clear that the general interest must

prevail. But this is how it is combined with the spirit of the norm. On the other hand, when medical data is made available to some of the private organizations provided for by data intermediation systems, for example, in the reuse of certain categories of data held by public sector organizations - when organizations act for commercial purposes -, an additional economic value that society has generated and from which it will not be able to benefit is directly attributed to the private sector. There are only well-intentioned and highly ethereal claims that the progress generated by this data exchange will benefit society. No concreteness.

In short, from our perspective, only data exchange systems are viable in the field of health where the altruistic spirit prevails and where society is rewarded for the use of data that it itself has generated.