COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

GOVERNANCE PROFILES OF SECONDARY USE OF HEALTH DATA IN THE EHDS

Raffaele Ambrosino

TABLE OF CONTENTS

This contribution offers a critical analysis of the governance framework for the secondary use of electronic health data established by Regulation (EU) 2025/327 on the European Health Data Space (EHDS), situating it within the broader context of the European data strategy. The author starts from the observation that the growing economic valorisation of health data risks fostering the emergence of a lex mercatoria of data, potentially at odds with the sensitive nature of health information and with the protection of individual rights. From this perspective, the EHDS is interpreted as a regulatory response aimed at removing the health data market from purely private-law logics and reorienting it towards a model of public governance grounded in the pursuit of collective interests. The paper focuses in particular on the opt-out mechanism provided for the secondary use of data, highlighting its ethical and legal shortcomings. According to the author, the presumption of consent to data reuse—subject to the exercise of a right to exclusion—is problematic in light of the conditions of vulnerability under which consent to the collection of health data is typically given. The opt-out mechanism thus results in a downsizing of the role of informed consent, which is recovered only ex post, and marks a further step towards overcoming consent as the central legal basis for the processing of health data. Considerable attention is devoted to the analysis of data access bodies, identified as the core actors in the governance system for secondary use. These public bodies are characterised as true second-level data controllers and as providers of a public service of data access, formalised through administrative decisions and authoritatively determined tariffs. This institutional design reflects, in the author's view, a process of progressive "administrativisation" of data protection, which strengthens the public-law dimension of data reuse and legitimises processing on the basis of an important public interest. Finally, the contribution examines the delicate balance between collective objectives and the protection of individual rights, focusing on the principles of transparency and data minimisation, on anonymisation and pseudonymisation techniques, and on the use of secure processing environments. While acknowledging the regulation's overall guarantee-oriented approach, the author points out that the broad margins of discretion left to Member States and to data access bodies may result in uneven implementation, thereby placing strain on the objective of achieving a genuinely uniform European health data space

Keywords: European Health Data Space (EHDS); Secondary use of health data; Data governance; Health data regulation

I. THE EUROPEAN HEALTH DATA SPACE AS A NEMESIS TO THE *LEX MERCATORIA* OF HEALTH DATA.

One of the main effects of the implementation of the use of technology is the exponential enhancement of data, an element that, in its digital declination, represents both the product and the main source of supply of digital innovation systems whose operation and

development depend on algorithmic information[1] processors. And so even data, which has become an indispensable resource for the progress of the community, are at the center of a real market.

With the natural development of a bargaining area having as its object the exchange of data, however, it becomes necessary to interface, both with the legal implications related to the ontological characteristics of the commodity in question, and with the purposes that animate the user of the data to its procurement. In fact, it must be considered that the transfer of data, which takes the form of the well-known activities of communication and/or sharing of information, if it is attributable to a natural person, involves subjective interests partly extraneous to the purely patrimonial dimension of the activity underlying them, interests which, due to the particular sensitivity of which they are characterized, postulate another (r)o[2] degree of legal protection. It therefore seems unfortunate to run the risk of consigning these exchanges to the evolution of a peculiar *lex mercatoria.*

The European legislator, aware of these circumstances, but in particular of the strategic role inherent in the circulation of data, has therefore decided to focus its political agenda precisely on the regulation of data. As some scholars observe, "with the 'European strategy for data' the European Union aims to obtain a leading role in the data economy"[3] and, focusing on the phenomenon of data sharing[4], aims at the substantial construction of "data spaces"[5] that are cross-border, interoperable and, in a holistic vision, suitable to become technically secure environments and compatible with the protection of the aforementioned subjective interests on a legal level.

The construction of data spaces at the European level is based on the EU's duty to ensure the well-being of the community and to encourage, through its regulatory intervention, the development of certain strategic activities, among which the protection of public health and the advancement of scientific research stand out[6].

With respect to the latter sectors, Regulation (EU) 2025/327 of the European Parliament and of the Council was issued last February with the declared "aim of establishing the European Health Data Space (EHDS)". There seem to be two cornerstones on which the

[1] Recently, the framing of "data" as a form of digital representation of information has been addressed by A. Iannuzzi, *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act,* in *La regolazione europea della società digitale,* (ed.) P. Pizzetti, Turin, 2024.

[2] In the face of the process of commodification of the data, the personalistic aspects linked to the ontological dimension of the sensitive information found in it, requires forms of protection more suited to the protection of subjective rights than the mere recourse to the classic means of asset protection relating to contractual relationships.

[3] Thus D. Sborlini, *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in Contratto e Impresa, 2024, I, 223.

[4] The activity of "data sharing" is expressly defined in Article 2, no. 10, EU Reg. 868/2022 (*Data Governance Act*) as "the provision of data by a data subject or a data subject to a data user for the purpose of the joint or individual use of such data, on the basis of voluntary agreements or Union or national law, directly or through an intermediary, for example in the context of open or commercial licences, for remuneration or free of charge".

[5] The definition of "data spaces" is not provided for at the legislative level, it is the result of doctrinal elaboration, in particular see E. Curry, S. Scerri and T. Tuikka, *Data Spaces: Design, Deployment, and Future Directions*, Berlin/Heidelberg, 2022; M. Franklin, A. Halevy and D. Maier, *From databases to dataspaces: a new abstraction for information management*, in SIGMOD Record, Vol. 34, IV, 2005, 27 et seq.

[6] About it see T. Petrocnik, *Health data between improving health (care) and fueling the dataeconomy,* in Technology and Regulation*,* 2022, 124.

EHDS is based: the secure management of electronic health data, which can be subsumed in the category of the so-called. sensitive data; and the expansion of the hypotheses of reuse of the same; In other words, not only that individual use consisting in the use of health data for the purposes for which it is *naturaliter* formed and originally collected (so-called primary use) must be favored and regulated, but in particular the so-called "primary use". "secondary use", i.e. reuse - in aggregate form and in a collective information dimension - for the pursuit of purposes unanchored from the activity that led to its direct formation [7]. Article 53 of the Regulation expressly identifies the purposes in question corresponding to the achievement of collective interests, including: the protection of public health, statistical production, scientific research and the development of artificial intelligence algorithms.

More generally, it should be noted that the regulation, in line with the aforementioned political purposes, aims to establish a framework for structuring an organic discipline of data management activity, thereby transforming itself into an application model that can be adopted in the future in sectors other than healthcare. This is demonstrated by the detailed regulations governing each phase of the shared management procedure for electronic health data.

Due to the expansive scope of the so-called "S.p.A. secondary use, through which it is envisaged that actors belonging to sectors of social life unrelated to public health are expected to participate in the procurement of digital health data, it seems necessary to review the governance profiles

processed for the management of access to data by subjective categories other than the "data subject" and the data subject. The work aims to examine the presence of any structural obstacles to the uniform application of the discipline dictated by the regulation, in order to verify in a comparative key whether the spaces of discretion left to national legislators in the field of governance can be harbingers of unequal treatment between subjects belonging to another subjective category placed at the center of the electronic health data market: the so-called. "data users".

II. THE OPT-OUT: THE (POSTHUMOUS RETRIEVAL OF) CONSENT TO THE SECONDARY USE OF ELECTRONIC HEALTH DATA.

The analysis of the health data governance system provided for by Section 2 of Chapter IV of the Regulation requires some preliminary clarifications on issues impacting the substantive profiles of secondary use. First of all, it should be noted that the regulation *in question* refers to a specific category of health data, the "electronic" one[8], a concept

[7] See in particular A. Cabrio, *La seconda vita dei dati. Luci e ombre della normativa privacy in materia di secondary data use*, in *Il futuro della sanità. Strumenti per una reale innovazione*, (edited by) F. Frattino - F. Massimino, 2024, 21; M. Ciancimino, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche*, in Il diritto di famiglia e delle persone, 2022, I, 37.

[8] As observed by S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in Le Nuove Leggi Civili Commentate, III, 2025, 563, with the introduction of the regulation a new category of data is defined, since "Not only is there no coincidence between the notion of electronic health data and that of health-related data, but not even between health-related data and personal electronic health data:

verbatim declined in the double definition of "personal electronic health data" identified (pursuant to letter a), art. 2 co. 2 of the regulation) in the "data relating to health or genetic data processed in electronic format"; and of "non-personal electronic data" which is instead the electronic health data other than the personal one that can include both the (totally) anonymized data and that by its nature "never" referable to a data subject[9]. Remaining in the space dedicated to definitions, it should then be emphasized that secondary use is identified as an activity of "processing" of the data[10].

Hence, the important classification approach: the secondary use of data in the EHDS is, in general, an activity of processing health data in electronic format, a framework confirmed by the express provision of coordination based on which the regulation in question is in a relationship of subsidiarity with EU Regulation 2016/679[11]. In fact, from the point of view of the European legislator, the EHDR regulation "specifies and integrates" the rights of natural persons guaranteed by the GDPR[12].

It is now useful to point out that - on a functional level - secondary use, although it is ontologically distinct and is conceived in terms of autonomy with respect to primary use, cannot be separated from the latter. In the genesis of the raw material, i.e. the electronic health data, the primary use represents the source of the original materialization of the same which, in most cases[13], comes into existence when the patient's electronic medical

Thus, in order for a data relating to health to be considered personal electronic health data, it is necessary that it be processed in electronic format and, conversely, for a personal electronic health data to be considered data relating to health, it must not be a genetic data. In fact, the definition of "personal electronic health data" includes both health data and genetic data". For a legal framework of data in the specific sector of scientific research, even before the approval of the regulation, see P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Editoriale Scientifica, 2021 and G. Bincoletto, *Scientific research processing health data in the European Union: data protection regime vs. open data*, in Journal of Open Access to Law, II, 2023, 1.

[9] L. Ruggeri, *La dicotomia dati personali e dati non personali: il problema della tutela della persona nei c.dd. dati misti,* in Dir. fam. pers., 2023, 808.

[10] Pursuant to Article 2(d) of Regulation (EU) 2025/379, the definition of 'secondary use' corresponds to the 'processing of electronic health data for the purposes set out in Chapter IV of this Regulation, which are different from the initial purposes for which such data were collected or produced';

[11] EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data, in the Official Gazette, Law 119, 4 May 2016; on this point R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (eds.),), *Codice della privacy e data protection*, Milan, 2021; P. Guarda*, Il diritto alla protezione dei dati personali in Europa ed il Regolamento Generale sulla Protezione dei Dati*, in P. Guarda – G. Bincoletto, *Diritto comparato della privacy e della protezione dei dati personali*, Milan, 2023, 55.

[12] The European legislator in the context of secondary use (both in Article 1 par. 8 where it states that "access to electronic health data for secondary use agreed within the framework of contractual or administrative agreements between public or private entities remains unaffected", as well as in Article 52 par. 3 where it is provided that data access bodies when issuing data authorizations "may include contractual agreements between health data holders and health data users for sharing data containing information or content protected by intellectual property rights or trade secrets.") it clears the use of the contract as a tool for the circulation of electronic health data, paving the way for the idea of a real market for electronic health data. In this regard, C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in Tecnologie e diritto*,* II, 2024, 485.

[13] Access to data for secondary use in accordance with the provisions of Article 51 of Regulation (EU) 2025/379 concerns not only information in digital format from electronic health records but also other categories of electronic health data: personal electronic health data automatically generated by medical devices; data from wellness applications; data from clinical trials, clinical trials, clinical investigations and performance studies subject to Regulation (EU) No 536/2014, Regulation (EU) 2024/1938 of the European Parliament and of the Council, Regulation (EU) 2017/745 and Regulation (EU) 2017/746; data from medical records and mortality registers; other health data from medical devices. With the exception of those

record is constructed. A moment that generally coincides[14] with the formation or sharing of the personal health information of the data subject in the constancy of a medical care or assistance activity conducted by a health professional. So, if these data, incorporated in the electronic medical record[15], represent in their individual dimension the substrate of primary use in the EHDS, they, as a result of the transfer mechanisms conceived in terms of legal obligations by EU Regulation 2025/327, represent, in a "collective" dimension, the main source of supply for secondary use. But be careful; if we consider that primary use presupposes the formation of the data on an individual level, it must still be recognized that the data thus formed represents a necessary but insufficient element for the purposes of secondary use, as the achievement of the purposes referred to in Chapter IV of the Regulation requires a *quid pluris*, i.e. a large-scale aggregation of individual data relating to individual medical[16] records; aggregation that presupposes an activity of further processing of the set of data collected. For these reasons, secondary use should be identified as a "second-level" treatment of electronic health data already acquired for primary use. This close genetic interconnection is evidenced, on a textual level, by the Community legislator itself which, aware of the uniqueness of the data, already at the time of its formation (in the context of primary use) is concerned with introducing the necessary legal basis for the processing of health information for secondary use.

The issue of the legal basis is important because, in addition to reflecting on the standards of adequacy and proportionality guiding data governance, it represents one of those matters in which the European legislator has left some margin of discretion to state legislators[17]. Firstly, since the purposes characterizing secondary use imply, on an ontological level, a "collective" destination of the patient's personal information - not

included in public registers and biobanks, the source of most health data intended for reuse is in any case an activity that can be subsumed in the so-called "Renewable Environment". primary use. It is quite rare, and moreover hindered by anonymization obligations, that electronic health data can be created *from scratch* for a mere secondary use.

[14] Electronic health data for primary use is not always the product of a technically clinical activity, just think of the data generated by applications for the well-being of smart electronic devices, the subject of attention of the Regulation together with electronic medical records.

[15] For an examination of the various positions and obligations relating to the subjects involved in the processing of medical record data, please refer to C. Perlingieri, A. Cocco, *'Primary' and 'Secondary' Use of Electronic Health Data*, in Italian Law Journal, X, 2024, 275, where the authors highlight the need for coordination between the discipline introduced with the approval of the EHDS Regulation and the provisions of the minister's decree EHR 2.0 of 20 May 2022.

[16] According to Recital (53) of EU Reg. 2025/327 as "Electronic health data used for secondary use can bring great benefits to society. The use of real-world data and evidence, including information on patient-reported outcomes, should be encouraged for evidence-based regulatory and policy purposes, as well as for research, health technology assessment and clinical objectives." In order to achieve this objective, recital (53) states that "it is important that the datasets made available for secondary use under this Regulation are as complete as possible."

[17] Pursuant to Article 51, paragraph 4 of EU Reg. 2025/327, member states are given the possibility to "introduce stricter measures and additional guarantees at national level aimed at protecting the sensitivity and value of the data falling under paragraph 1, letters f), g), i) and q)."; Furthermore, with reference to the power to exclude access to data for secondary use, art. Article 71, paragraph 4 of the Regulation provides that, under certain conditions, "a Member State may provide in its national law for a mechanism to make available the data for which the right of exclusion has been exercised". A systematic reading of the two rules leads us to believe that in some circumstances the legal basis for secondary use provided for at a general level by European legislation can be integrated or even deactivated by individual national states, generating inhomogeneity in the governance of electronic health data.

contemplated by the purposes of medical assistance and treatment - it is necessary to protect the autonomy of the subjects to whom the health data belong in the light of their sensitive nature. For these reasons, the reuse of data would presuppose a specific decision by the natural person on the processing of the same for the specific purposes incorporated in the so-called secondary use.

Such a decision implies, of course, the manifestation of a consent that must be collected by the data controller at the time the data comes into existence, which also corresponds to that of the production of the information for "individual" clinical purposes. However, the path taken by the European legislator on this point is that of the so-called mechanism. opt-out, a (relative) presumption according to which in the absence of an express exclusion by the data subject, the health data formed for primary use can also be used for secondary uses provided for by the regulation[18]. Following this approach, the consent to the processing of the data by the data subject assumes its relevance, as it can affect, even if *ex post*, the secondary use. It is also important to note the strong dogmatic force of the opt-out, whose implementation could theoretically resurface the question of the data subject's consent as a basis for the lawfulness of processing sensitive data[19]. However, in the case of health data, this issue seems to have long been superseded, given the super-individual needs underlying and protected by the combined provisions of Articles 9(2)(h) and (i) and 89 of the GDPR. From an interpretative perspective, the provision seems to highlight an atavistic need to retrieve an expression of will from the data subject "upstream" in order to authorize a "downstream" use whose legal basis is entirely different from that for which the data is being processed[20].However, caution should be exercised because, as will be

[18] Before the entry into force of the regulation, with reference to the hypotheses of reuse of health data contained in an electronic health record for so-called "electronic health record" activities. In the case of proactive medicine developed in the autonomous province of Trento, the Italian Data Protection Authority has taken a radical position, denying the possibility of considering the reuse in question lawful in the absence of an autonomous expression of consent by the data subject. According to the supervisory authority, a healthcare professional subject to professional secrecy may only use the data for treatment purposes when this is necessary and essential for the patient's health. Whenever one is outside the ontological perimeter of primary use, any further data processing activity must be expressly and autonomously authorized.

[19] According to the majority doctrinal approach, in the matter of personal data we are faced with subjective legal situations that can be declined as personality rights. At the dawn of the introduction of Law no. 675 of 31 December 1996, E. Giannantonio, *Dati personali (tutela dei),* in *Enciclopedia del diritto,* Aggiornamento III, Milan, 485, reconstructed the law on personal data, as a sort of *habeas corpus* of the cybernetic era; consequently, only the consent of the data subject, which can always be revoked, could have made lawful any operation relating to the use of such information by by a person other than its owner. As recently stated by P. Gallo, *Dati personali (diritto allo sfruttamento economico),* in *Digesto delle discipline privatistiche,* Turin, Update 2022: "taking into account the unavailability of the rights in question, the consent of the entitled party fulfills the important function of making the processing of personal data lawful, just as in general the consent of the entitled party is valid for discriminating certain intrusions into the sphere of others personal, such as the publication of the image, intrusions into privacy and so on". On this point, see also A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto,* Naples, 2017; S. Thobani, *Diritti della personalità e contratto,* Milan, 2018; F. Bravo, *Il diritto a trattare dati personali nello svolgimento dell'attività economica,* Padova, 2018; G. Resta, V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Rivista trimestrale di diritto e procedura civile*, 2018, 411; G. Resta, *I dati personali oggetto del contratto*, in *Annuario del contratto,* 2018; V. Ricciuto, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in Rivista di diritto civile, 2020, 642.

[20] It is useful to point out that, in Italy, in application of art. 110-bis of the GDPR, if there are particular cases in which obtaining the consent of the data subject for the reuse of personal data for the purposes of scientific research appears complicated, the data subject is given the opportunity to request an authorization for reuse directly from the Data Protection Authority, subject to the adoption of precautions aimed at

further specified below, this approach is actually geared towards definitively overcoming consent as a necessary means of legalizing processing[21].

The point deserves a reflection which, in the opinion of the writer, makes the choice of the opt-out tool ethically questionable. If the sharing and consequently the processing of personal data must be considered lawful activities only if assisted by the consent of the data subject, which is therefore a necessary condition of the entire operation, it is equally essential that such consent, in order to be binding, be expressed in a conscious and free manner. It should also be remembered that in health matters the so-called consent. privacy often goes hand in hand with consent to health treatment itself, which is strengthened in its ontological traits by being "informed".[22] Precisely in the case of processing health data, the psychological condition in which this consent matures must be taken into account. The concrete context of reference, as mentioned, is almost always that of the patient who discloses his or her sensitive information to the professional as part of an individual health

eliminating any danger of re-identification of the data subject. ("The Garante may authorise the further processing of personal data, including those of the special processing referred to in Article 9 of the Regulation, for scientific research or statistical purposes by third parties who mainly carry out such activities when, due to particular reasons, informing the data subjects is impossible or involves a disproportionate effort, or risks making impossible or seriously jeopardizing the achievement of the purposes of the research, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subject, in accordance with Article 89 of the Regulation, including preventive forms of data minimization and anonymization"), on point F. Polito, *Il consenso al trattamento dei dati personali in tema di ricerca medica e gli artt. 110 e 110*-bis *del codice privacy*, in *Ricerca in sanità e protezione dei dati personali. Scenari applicativi e proposte future* (edited by) E. Chizzola – P. Guarda – V. Maroni – L. Rufo, Editoriale Scientifica, 2024, 5.

[21] According to S. Corso, in *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327,* cit. 579, with the introduction of an autonomous legal basis for processing for secondary use, as an exception to art. 6 of the GDPR "consent, albeit limited to secondary use, is not only no longer the main legal basis and case of derogation from the prohibition, but can no longer even be an additional condition for the processing of data relating to health, *pursuant to* Article 9(4) (35). In this sense, the EHDS, in the context of secondary use, goes beyond the mere overcoming of any national settings, even more or less consensus-centric, and bans the instrument of consent – understood at least as consent of the data subject or *ex ante consent* – from European legislation". On this point, cf. see also M. Afra, *An Assessment on Innovator's Ability for Consent-Free Health Data Reuse*, *In the Context of the GDPR and EHDS: The Netherlands Case Study*, in European Journal of Health Law, vol. 31, V, 2024, 475; F. Kertesz, *Collaboration in Healthcare: Implications of Data Sharing for Secondary Use in the European Union,* ibid., 497 ff.; C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in Contr. impr., II, 2020, 860.

On the downsizing of the role of consent in the context of the reuse of data relating to health for medical research and statistical purposes, see also F. Polito, *Il consenso al trattamento dei dati personali in tema di ricerca medica e gli artt. 110 e 110*-bis *del codice privacy,* cit. 16 who expresses perplexity about the easy identification of the specific cases in which it is possible to resort to the derogation from consent referred to in art. 110-bis Privacy Code.

[22] Although informed consent to health treatment must be distinguished from the so-called privacy policy, pursuant to Article 4, no. 11 of the GDPR, also in this context the duty to inform is an essential element of the case since the consent of the data subject is "any freely given, specific, informed and unambiguous expression of the will of the data subject, with which the same expresses his consent, by a statement or unambiguous affirmative action, that personal data concerning him or her are being processed". It should be reiterated that "informed consent" in the matter of health treatments, according to the prevailing approach, can in no case be considered presumed. On this point, N. Todeschini, *Liability in Medicine*, Milan, 2023 who, on p. 209, defines the presumption of (informed) consent as a "contradiction in terms". Compliant, Cass. civ., sec. III, 27 November 2011, no. 20984 according to which if it is true that on the evidentiary level informed consent does not require the existence of written evidence *ad substantiam,* on the substantive level it still requires a "real manifestation".

For further information on the relationship between informed consent and privacy, P. Cosomai, *The right to health, informed consent and privacy,* in *EXPLICO – Digital health* (ed.) by P. Cosomai- A. Perrone, Milan, 2020, 98.

care relationship which, in most cases, can be characterized by the existence of a condition of vulnerability (de facto or de jure) of the data subject[23]. Taking into account these conditions, it would be rather risky to suppose the absolute absence of mental reservations on the part of the patient on the awareness of (a possible) reuse of factual data provided for the overcoming of a clinical problem; perhaps it could not even be assumed that there was a mere voluntary disclosure of the data itself, even for primary use. The sharing of information regarding one's state of health is often animated by a psychological (and physical) condition of vulnerability and is based more on the "duty" than on the "wanting(s)" to share in a "contractual" nature. Assuming an equivalence between consent to primary use and consent to secondary use of (personal) data materialized under such conditions appears to be a gamble, even if the consent is preceded by adequate information by the data subject. From this point of view, the retroactivity of which the right of exclusion referred to in art. 71 of EU Reg. 2025/379, which can be exercised at any time, ends up representing a "palliative" solution to the proposed solutions. With the opt-out mechanism, the data subject is allowed to express the desire to limit the use of his or her sensitive data for secondary uses even if consent was originally presumed, recovering only *ex post* an awareness perhaps weakened by a condition of clinical vulnerability.
It is also useful to underline that, also because of the conclusions that will be reached *below*, the hypothesis in question cannot constitute a case of "broad consent"[24] since the so-called broad consent presupposes a priori indefiniteness of the processing purposes which, in the case of reuse, seems to be neutralized by the regulatory taxonomy with which the regulation outlines the purposes in question; and underlies the uniqueness of the data controller receiving the consent of the data subject, a condition, the latter also irreconcilable with the operational structure emerging from the regulation which, on the other hand, concerning the governance of secondary use, provides for mechanisms of joint data controller between several subjects, distinct from each other by nature and functions.

III. DATA ACCESS BODIES: FUNCTIONS AND LEGAL NATURE OF THE ACTORS IN THE PROCESS OF REUSE OF ELECTRONIC HEALTH DATA.

Having established the link between the individual acquisition of health data for primary use and aggregate use for the purposes referred to in art. 53 of the Regulation, it is now

[23] For a complete analysis, see V.V. Cuocci, *The protection of personal data of vulnerable subjects in the digital dimension. A study of comparative law*, Bari, 2022.
[24] This term indicates a newly minted institution whose objective is to integrate a protection measure for the recovery of the lawfulness of the processing of data, if the latter are collected by the owner in the context of a scientific research activity. It is introduced by Recital no. 33 of EU Regulation 679/2016, according to which "Recital no. 33 of the aforementioned Reg., in particular, provides as follows: "[i]n many cases it is not possible to fully identify the purpose of the processing of personal data for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research where there is compliance with the ethical standards recognised for scientific research. Data subjects should be able to give their consent only to certain areas of research or parts of research projects to the extent permitted by the intended purpose.'

possible to focus the investigation on the governance systems designed by the European legislator for the management of health data for secondary use.
Since secondary use technically corresponds to an activity of "processing" electronic health data, governance must be analyzed starting from this classification. As in any processing activity, on the one hand, we have the data controllers of health data who are not the "data subjects", but the data controllers of the data acquired for primary use; on the other hand, are contemplated the so-called data users, i.e. those subjects who intend to access aggregated digital health data for the achievement of the purposes referred to in art. 53. As mentioned, the processing in question is in itself of the "second level": the access requested by users concerns the so-called " dataset, i.e. an information aggregation in which individually purchased data are collated; this operation therefore underlies the execution of those activities of selection, extraction and interconnection indicated by art. 4 of the GDPR. This implies the need to identify an additional figure responsible for carrying out such processing activities not attributable to the individual data subjects. In fact, the latter, in the case of data authorization, become mere taxable subjects of the legal obligation to communicate the data in their possession which, together with those provided by similar data controllers, end up generating a bundle of individual health data that give rise to the so-called "series of the data". data series. In other words, in the EHDS system, each individual controller is required to communicate the data held to a single reference body that acts as a collector and aggregator of the same and carries out an autonomous and specific processing activity.
The data controller in question is identified as the body responsible for access to the data, an entity that represents the nerve center of the governance of health data for secondary use which is delegated a fundamental role in the context of second-level processing. Any dynamic regarding the governance of the matter in question thus passes through the framing of the entire procedure of access to data in which these new state bodies are protagonists.
This decision is an extension of the approach - initially undertaken with the European Data Strategy, and subsequently implemented specifically with the implementation of various sector regulations (Data Act, DGA, etc.) - which has enhanced the role of data access bodies. These bodies, whether already existing or newly created, as in the case of data access bodies, are conceived and configured by the European legislator as "intermediary" institutional entities. Their primary function is to ensure the appropriate performance of the diverse range of activities encompassed in the concept of data processing, particularly in the case of data dissemination and sharing within the market and within the supranational sphere. This approach, while ensuring the greatest possible uniformity in this area and the hope of thus achieving a single data market, is crucial.
First of all, it should be noted that secondary use comes into play when electronic health data are the subject of an access request, an act that triggers an activity of circulation of health data that involves three subjective profiles: the data owner, the applicant and the data access body.
With reference to the first of the three actors in the procedure, it should be noted that the use of the word "controller" must be declined in an atechnical sense in order to avoid the

danger of confusing the data controller with the data subject. Those who own the requested data (so-called data controller) become data controllers in only two moments and circumstances: the one in which they came into possession of the electronic health data (so-called primary use) and the one in which they communicate, (*recte* is required to communicate) the "personal" [25]electronic health data to the access body required. In the context of secondary use, the actual controller is primarily the data access body. It should also be noted that the identification of the data controller is not predefined[26], as it is linked to the operation of two regulatory variables, which are: the obligation to make the data processed for primary use available to data access bodies[27] on the one hand, and, on the other hand, the exclusion positively from Article 50 of the Regulation. This functional approach leads to the exclusion of a one-to-one correspondence between the data controller in the context of primary use and the data subject for secondary use, since, if the former is a natural person (a researcher) or a micro-enterprise, due to the exemption granted by the legislation, it cannot be considered a "data controller" according to the provisions of Chapter IV of the Regulation. However, care should be taken not to overlook the dispositive nature of the rule governing the exemption in question; the European legislator recognises that individual Member States have the power to deactivate the exclusion *in question* and to also oblige natural persons and micro-enterprises within their jurisdiction to provide data. This exception is of important importance in terms of governance since, being left to a purely discretionary assessment of the individual State, it could give rise to cases of unequal treatment in access to datasets between users of individual States, so that the subjective expansion of data holders, while generating an advantage, would nevertheless be an obstacle to the harmonious functioning of the EHDS envisaged by the legislator.

Therefore, excluding the subsumption of the data subject in the figure of the data controller, in the circulatory phenomenon for secondary use the data controller is explicitly assigned to the data access bodies. Well, the legal nature of the figures in question as a "public body" appears symptomatic of the underlying value of the same concept of secondary use. The regulation, by obliging individual States to set up these bodies *from scratch*, in the event that they do not intend to entrust existing public bodies, ends up

[25] Even if the data subject is subject to an obligation, the performance of the same still takes the form of an activity of communication of sensitive data, therefore this fulfilment must also be considered a processing activity if it concerns personal digital health data. At this stage, we are not in secondary use because the data in question has not yet become available to the requesting user. Particular is the case of the so-called. "reliable" data controllers (in depth *below*) framed by art. 74 EU Reg. 2025/327 as data controllers for secondary use when they make the health data in their possession available to users.

[26] There is no classification that takes into account the mere subjective qualities of the data holder, as stated in recital (59) of EU Reg. 2025/327 "Holders of health data in the context of secondary use should therefore be entities that are providers of health care or care or carry out research activities in relation to the health care or care sectors, or develop products or services for the healthcare or care industries. These entities can be public, non-profit or private".

[27] Ex recital (52) EU Reg. 2025/327, "this Regulation introduces the legal obligation, pursuant to Article 6(1)(c) of Regulation (EU) 2016/679, in accordance with Article 9(2)(i) and (j) of that Regulation, that the holder of health data is required to report personal electronic health data to the bodies responsible for access to health data". A legal basis is introduced for the lawfulness of the communication of data from the data subject to the data access body, an activity that constitutes data processing whose data controller pursuant to art. 74 of the Regulation is precisely the subject who collected the data in the context of primary use.

investing the new operational figures with tasks of public interest and in doing so does nothing but raise the very nature of the purposes underlying the reuse of electronic health data to the public level. The public framework of data access bodies then ensures that the issue of the legal basis of the processing (and the mandatory consent of the data subject) is overcome: in fact, from a legal point of view, the subjective nature of the data controller legitimizes the processing activity that ends up falling within the abstract case referred to in letter f) pursuant to Article 6 of the GDPR and elides, the prohibition referred to in art. 9 par. 1 GDPR[28] taking the form of a hypothesis of processing "necessary for reasons of important public interest based on Union or Member State law".

A combined reading of these classificatory approaches and other hermeneutical elements, based on a systematic approach to the provisions of the regulation, can lead us to the exact framing of the entire legal relationship culminating in the granting of the authorization to the data. The interpretative pieces are represented specifically:

a) the qualification of the third party involved in the re-use of electronic health data (the applicant) and;

b) the provision for the payment of pecuniary fees for access to the same.

With reference to the data requester, the use of the word "user" is significant, with which the person requesting authorization to the data is designated. In this regard, it is legal semantics that offer further clarification regarding the exact legal classification of the relationship that is established between the applicant and the body to which the request is addressed. It is in fact known that, in the legal field, the word "user" means the subject of an economic relationship, an active user of a service whose provision is intended either to an indeterminate category of subjects or, more generally, to the community of associates. It follows that even the activity of disseminating electronic health data for secondary use, according to linguistic interpretation, must be classified as a service, which, due to the legal nature characterizing both the object of the service and the subjects responsible for its provision, can be understood, specifically, as a public service.

In support of this framework, the other hermeneutical element comes to the rescue, namely the provision for the payment of a monetary fee for the use of access to the data series. Even with respect to this element, semantics plays a fundamental role as the European legislator qualifies the fees in question as "tariffs", a term that according to the prevailing doctrine[29] refers to the price paid for the use of a good or service whose determination does not depend on the will of the parties but is imposed authoritatively by reason of the collective interest underlying the service.

It should also be noted that - pursuant to Article 2 paragraph 2 letter v) of the Regulation - the "authorization of data" is defined as "an administrative decision"; This implies a further strengthening of the divided hermeneutical reconstruction which, on a legal level,

[28] On the subject of "special" data referred to in Article 9 of the GDPR, see more M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679,* in Le Nuove Leggi Civili Commentate, I, 2017, 165.

[29] On this point, see F. Merusi, *Su alcuni aspetti problematici della determinazione autoritativa dei prezzi*, in Foro Amministrativo, II, 1965, 157; A. Cassone, *Lo stato attuale della teoria delle tariffe*, in *Econ. Pubbl.*, 1978, 288; P. Bilancia, *Determinazione dei prezzi e libertà d'impresa*, Padova, 1986

corroborates the approach[30] according to which, in the matter in question, the European legislator intends to proceed with the progressive "administrativeization" of data protection. A process that, as other authoritative doctrine observes[31], brings with it the succumbing of the rule of private law compared to that of administrative law.

IV. Data governance in the prism of the balance between the achievement of collective purposes and the protection of individual rights.

At this point, the analysis of governance in the context of secondary use must be carried out taking into account the classification of the authorization of data as the provision of a public service, and the circumstance that this service has as its object an activity of processing ontologically "sensitive" data. It should also be noted that the management of electronic health data for reuse can only fulfill its political mission if it is able to transform the data into information that is useful for the purpose for which access is requested[32]. However, the potential conflict of this objective with the prerogatives of protection of confidentiality deriving from the sensitivity of health data makes the governance activity articulated, implying the attribution to data access bodies of a delicate function of balancing the various interests at stake[33].

The governance rules coined with the regulation are, on closer inspection, the result of an arduous compromise between the political objectives of the European legislator and the technical-legal instances put in place to protect confidentiality. From the first point of view, the emphasis on data reuse is a corollary of the main strategic objective of the Data Governance Act which encourages data sharing because of the potential altruistic benefits[34] for fundamental sectors of social life. The technical-legal precautions inherent in the folds of certain structural and procedural aspects of governance are instead to be traced back to the observance of the considerations[35] of the European Data Protection Board and the European Data Protection Supervisor regarding the danger to the

30 S. Corso, *The electronic health record 2.0. Ideas for a critical reading*, in The New Commented Civil Laws, 2024, 334.

31 P. Perlingieri, *La pubblica amministrazione e la tutela della privacy. Gestione e segreto dell'informazione nell'attività amministrativa*, in Annali della Facoltà di Economia dell'Università degli Studi del Sannio, VIII, 2003, 211.

32 The doctrine tends to distinguish the datum from the information, specifying that while the former has an intrinsic and objective cognitive value, in the latter the cognitive value turns out to be the result of a subjective operation of the individual user consisting in an elaboration of the former. In this sense, D.U. Galletta, *Accesso civico e trasparenza della Pubblica Amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in federalismi.it, V, 2016.
For an examination of the ontological difference between data and information in relation to health data, G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Bologna, 2012.

34 "Reuse" and "Altruism" of data represent two of the fundamental principles ordering the implementation of the strategic objectives set by the Data Governance Act. On this point, see F. Caloprisco, *Data Governance Act. Condivisione e "altruismo" dei dati,* in *Annali AISDUE*, 2021; E. Salerno, Il Data Governance Act, *il nuovo Regolamento europeo per il mercato unico dei dati rischia di non essere abbastanza e favorire i grandi della tecnologia*, in Privacy e Cybersecurity, 26 febbraio 2021, 7; A. Sola, *Primi cenni di regolazione europea nell'economia dei dati*, in MediaLaws, 2021, III, 194; E. Cremona, *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in Rivista italiana di informatica e diritto, 2023.

35 This is a joint opinion on the proposal for a Regulation (EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022).

protection of privacy related to the secondary use of digital (personal) [36]health data. The general principles underlying this balance are those of transparency - which guides the entire organizational-institutional structure of the bodies responsible for governance - and data minimization, which instead penetrates the procedural aspects by determining the content of the individual datasets for which authorization is issued.

The implementation of transparent data governance in the EHDS is linked to the public framework of the data access service, and is reflected in the institutional structure of the data access bodies tailor-made by the regulation with the precise aim of avoiding the occurrence of hypotheses of conflict of interest[37]. In this regard, a mere investiture of existing or newly established public bodies seemed insufficient, considering it rather necessary to provide for and regulate (perhaps hypertrophically) certain structural and indefectible characteristics of these entities, and to introduce obligations of a financial nature on the part of the Member States to ensure their managerial autonomy. On the structural side, there is a division of tasks among the various operational sections within the body, each of which is not only autonomous in terms of function and decision-making, but is also independent in terms of organization and economics. Each state body should therefore (be equipped with, or) have a corporate structure in which each body, structurally self-sufficient, is vested with the individual functions assigned by the regulation to the data access body. Only the organic segmentation of corporate bodies would be able to ensure that a request for data is the final product of autonomous institutional steps which, although connected and hinged on the same procedure, remain individually characterized by a decision-making capacity free from reciprocal influences, thus neutralizing potential conflicts of interest. Only through a horizontal diversification within the entity between the body responsible for the selection of data sets, the body responsible for anonymization/pseudonymization, the body responsible for determining the tariff, the body responsible for managing the secure environment for sharing data, etc., will it be possible to defuse mechanisms that manage the processing of data for secondary use that are abstractly conflicting and contradictory with respect for the principle of transparency. It is precisely in this perspective that the obligation for individual States to provide data access bodies with economic and financial resources adequate to the configuration of a compartmentalized organizational structure should be interpreted. The possibility of entrusting the exercise of the functions *in question* to public bodies which, by their nature, are not able to assume a corporative dimension that can guarantee the functional diversification imposed by the European legislator, must therefore be excluded.

As a counterpart to transparency, in compliance with the technical-legal guarantees related to the protection of the privacy of the data subjects, the operation of the principle of data

[36] Scholars have also expressed critical remarks regarding the possibility that the excessive tendency to favor the reuse of data may have as a side effect a loss of control by the data subject over his or her data. In particular L. Marelli et al, *The European health data space: Too big to succeed?*, in Health policy, CXXV, 2023, 104861.

[37] An essential aspect is given by the obligation of individual Member States to notify the European Commission within 24 months of the entry into force of the regulation, the identity of the data access bodies and any changes to them.

minimization is placed[38]. However, the minimization does not affect those "non-personal" electronic health data *ex se* transfused into public databases, available and consultable in the so-called open access mode. The application of this principle governs the initial segment of the data access procedure triggered by a data request submitted to the access body. In fact, the latter, having completed the preliminary step of concrete verification of the specific purpose of use of the requested data and ascertained the absence of the obstructive conditions pursuant to Article 54 of the regulation[39], proceeds with the identification of the data sets useful to meet the user's needs. At this procedural juncture, the collection of the data then made available to the applicant - compulsorily transmitted by the data controllers - undergoes an initial processing activity, consisting of their anonymization or pseudonymization. It should be noted that these activities, although both are the subject of a legal obligation, live in a relationship of functional subsidiarity; According to the intention of the European legislator, anonymization should represent the main path that the body is required to follow in the preparation of the requested data sets, while pseudonymization remains a residual option whose application occurs only if an anonymization of the data nullifies the usefulness of the request in light of the inability of the anonymous data to be transformed, in the concrete case, into information[40]. The

[38] The necessity, adequacy and proportionality of the data requested with respect to the declared purposes are the essential characteristics for a request for access to the data to be accepted by the bodies. Pursuant to art. 5 par. 1 letter c) of the GDPR the data must be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed".

[39] Article 54 of the Regulation prohibits access to health data for: "a) taking decisions detrimental to a natural person or a group of natural persons on the basis of their electronic health data; in order to be considered as 'decisions' for the purposes of this point, they must produce legal, social or economic effects or similarly significantly affect those natural persons; (b) to take decisions, in relation to a natural person or group of natural persons, in respect of job offers, to offer less favourable conditions in the supply of goods or services, including the exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or the terms of loans, o take other decisions, in relation to a natural person or group of natural persons, which result in discrimination against them on the basis of the health data obtained; c) carry out advertising or marketing activities; (d) develop products or services that are capable of harming humans, public health or society at large, such as illicit drugs, alcoholic beverages, tobacco and nicotine products, weapons, or products or services designed or modified in a way that is addictive, violates public policy or morality, or causes a risk to human health; (e) engage in activities contrary to ethical provisions under national law." According to M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, Maggioli Editore, 2025, cit. p. 75 if with specific reference to the use for marketing activities, "the inhibition highlights a prudent and guaranteeist approach, in line with the GDPR, to prevent the commercial exploitation of health data without informed and specific consent. However, one question that could arise is the compatibility of such restrictions with innovation in healthcare, particularly for the development of new drugs and personalised treatments based on large volumes of data."

[40] Although according to L. Rocher, J. M. Hendrickx, Y. A. De Montjoye, *Estimating the success of re-identifications in incomplete datasets using generative models*, in Nature communications, X, 2019, 1, it is impossible to speak in an absolute sense of anonymization, since it would always be possible in the abstract to be able to take the opposite path to the process of depersonalization of data; in any case, The distinction between the two procedures, that of anonymization and pseudonymization, is based on the technical and economic effort required for the re-identification of the data subject, which translates into a gradation of the risk inherent to each type of processing used for the elimination of the identification process. In this regard, cf. E. M. Weitzenboeck, P. Lison, M. Cyndecka and M. Langford, *The GDPR and unstructured data: is anonymization possible?*, in International Data Privacy Law, XII, 2022, 184. European case law is of the same opinion: the Court of Justice of the European Union, in the Scania case of 9 November 2023 (Case C-319/22, Gesamtverband Autoteile-Handel v Scania CVAB, ECLI:EU:C:2023:837) has in fact specified that "In order to determine whether a natural person is identifiable, directly or indirectly, all means that could reasonably be implemented by the controller must be taken into account, pursuant to Article 4 (7) GDPR, or by others,

choice between anonymization and pseudonymization is, on a methodological level, oriented by the objective of favoring the dissemination of data to the extent that their knowledge is suitable for transforming itself into useful information[41]. Utility thus becomes a key concept in the governance activity carried out by data access bodies as it represents a fundamental decision-making parameter regarding the guarantees adopted from time to time; moreover, the evaluation of the degree of usefulness that the different data processing method can confer on the information provided to the user represents a further element of decision-making discretion that is the prerogative of data access bodies, whose operations may hinder a harmonious development of the EHDS. On an ontological level, it should be emphasized that utility, becoming an essential attribute of information, ends up impacting the entire market of personal health data[42]. The value of the latter[43] can no longer be traced back to its essential structure, but will be linked to two variables, to be verified on a case-by-case basis, namely: the degree of processing to which the data is subjected and the specific purpose for which it is requested. It will then be appropriate to assess whether the calculation of the fees provided for in the Regulation will have to take into account the level of "purity" of the dataset made accessible. In the opinion of the writer, it seems difficult to admit that the fee to be paid may depend on the market value of the shared data, since we are talking about a tariff and not a consideration, the determination of the price should by its nature remain insensitive to mercantilist logic and respond exclusively to public reasons.

On a dogmatic level, then, the systematic interpretation of the entire regulation leads us to conclude that anonymization (or pseudonymization) does not seem *ex se* sufficient for the full taxonomic transfusion of anonymized data in the category of "non-personal digital health data" positivized by the European legislator. Therefore, the new regulations on the

to identify such a person, without requiring that all information from which such person can be identified be in the hands of a single entity". Even according to the judges, the anonymization of the data is not suitable to eliminate the personal nature of the same.

41 On a practical level, if access to pseudonymised data is granted, the decryption key of the same useful for the re-identification of the data subjects will be held either by the data access bodies themselves or by a reliable third party designated under national law.

42 About critics' points on theme see J. Thomason, *Big tech, big data and the new world of digital health,* in Global Health Journal, 5, 2021, 165; nonchè C. Dantas, K. Mackiewicz, *Are we ensuring a citizen empowerment approach for health data sharing?*, in A. Cartolovni and others, *Proceedings of the 2022 Good Brother International Conference on Privacy-friendly and Trustworthy Technology for Society*, Zagreb 2022, 55.

43 On the marketability of personal data, two doctrinal approaches must be highlighted. One (B. Custers, G. Malgieri, *Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data*, in Computer Law & Security Review*,* 2022, 45; S. Yakovleva, K. Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation,* in American Journal of International Law, X, 2020, 114,) which, by bringing the protection of personal data back to the cases of fundamental human rights referred to in art. 8 of the Charter of Fundamental Rights, denies the availability of the legal positions in question to the interested parties; the other (B. Rossler, *Should personal data be a tradable good? On the moral limits of markets in privacy,* in *Social dimensions of privacy: Interdisciplinary perspectives* (eds.) B. Rossler – D. Mokrosinska, Cambridge, 2015, 141; M. Mursia, C. A. Trovato, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in Media Laws*,* 2, 2021, 165; F. Ferretti, *Directive (EU) 2019/770: personal data as consideration in contracts for the supply of digital content and digital services and the inherent impact on privacy law,* in Actualidad Juridica Iberoamericana*,* XVI, 2022, 1740; D. Poletti, *Le condizioni di liceita del trattamento dei dati personali*, in Giur. It*.,* 2019, 2783; R. Senigaglia, *La dimensione patrimoniale del diritto alla protezione dei dati Personali*, in Contr. impr., II, 2020, 760), denying the absoluteness of the right in question, admits the marketability of the personal data provided that compliance with adequate processing to protect the right to privacy of the data subjects is guaranteed.

re-use of health data seem to conform to that more guaranteeist position that for some time has tended to exclude the possibility of eliminating in an absolute and incontrovertible way the danger of re-identification of the data subject by the data controller or third parties[44].

V. Robust governance tools for electronic health data: the secure processing environment, limits on the misuse of access to data.

Once the phase of "depersonalization" of the data has been overcome, the further steps of the procedure are also surrounded by precautions aimed at protecting the confidentiality of the data subjects. Pursuant to art. 73 of the Regulation, the sharing of data takes place with their entry into a "secure" processing environment, a place where the material access to the data by the applicant is witnessed.
In order to reconcile the implementation of the strategic purposes related to the re-use of data with compliance with the principle of transparency, a public register shall be set up at each body showing both the access requests submitted by users, accompanied by the specific purposes for which access has been granted, and the (descriptions of) the data sets made available to the authorized user. The advertising obligation is of considerable importance as it guarantees control over the consultation of the data provided and the verification of compliance with the rules relating to their processing. For the writer, the publicity of such news could perform an important function on a transnational level, as through the construction of interoperable mechanisms designed *ad hoc* for the exchange of information between the various bodies of access to the data of the EHDS, or through a functional implementation of those already provided for by the regulation, it would be possible for each entity to ascertain whether a user has already obtained the access to the requested data or even whether this access has been denied to him and for what reasons. This would prevent the refusal of a data authorization from being circumvented by making the same request to a body operating in another Member State, or from the user being able to have access to the same data set for a longer period. This is clearly a *de jure condendo* perspective since, to date, Article 59 of the Regulation provides for each body responsible for governance only the obligation to carry out a biennial report on the activity carried out; moreover, the effectiveness of such an instrument presupposes that the individual data access bodies record and communicate not only the authorizations but in particular the measures of refusal to the data and the respective justifications. There is also the question of what the margins of binding nature may be for each body concerning any denials decreed by similar bodies[45]. In this regard, it would be useful to provide for a specific means of appeal against the refusal measure - or even a decision-making body - at "EU" level with binding effects throughout the European health data space, capable of avoiding differences in judgment or unequal treatment between individual member states.

[44] C. Gallese, *The Risks of Health Data Commodification in the EU Digital Market,* in Yearbook of Antitrust and Regulatory Studies, XXIX, 2024, 89.
[45] A more precise indication will certainly be obtained from compliance by 26 March 2027 with the obligation for the European Commission, provided for by art. 70 of the Regulation, to create standardized models for access to electronic health data.

The construction of the secure sharing space of data datasets is the prerogative of the body and is clearly part of the tasks congenial to its nature as a data controller. Art. Article 73 of the Regulation provides for the indefectible characteristics of the environment in question by providing for specific security measures suitable for making it a closed and controlled system. It is therefore required to adopt technical precautions to neutralize abuses such as the use of data for purposes other than those for which one is authorized, or access to data by unauthorized parties.

The security of the processing environment fulfils the "political" purpose of re-use, as it aims to ensure that the use of sensitive data such as health data is effectively intended to achieve altruistic purposes that justify a derogation from the ordinary legal basis for the processing of the data subject's data. In this sense, according to letter d) of the aforementioned Article 73, the environment is secure only if the user is able to access only the requested data, any possibility of abusive use of the shared data is then excluded since it is impossible to take "personal" health data from the environment; In fact, the user is allowed to export to an environment other than that of sharing only non-personal data or those provided in anonymised statistical form, unable to re-identify the data subjects. Of extreme interest is the need for the environment to be structured in such a way as to prevent the user from copying, modifying and deleting the data to which he has access; These prerogatives seem to correspond to the implementation of the principle of privacy protection by design, as they guarantee the adoption of a protective technological structure already in the design phase of the data sharing system. The safety of the environment was provided not only by resorting to privacy by design but also by limiting access to the processing environment in a time. In fact, by setting a maximum duration for users to consult the datasets, the European legislator, in addition to ontologically "filling" the principle of proportionality, has at the same time put a stop to the risk of reprocessing the shared data that a dilated time availability on the part of the same user could have generated.

The security of the environment, as well as teleologically, is also declined on a subjective level as the provision of art. 73 aims to prevent the data shared in the secure environment from being circulated in favor of subjects other than those authorized. In the absence of technical precautions, it would be possible for the user to "cede" access to the secure processing environment - and therefore to the data - to subjects to whom authorization has been denied, has expired, or in any case has been granted for other types of data or to process data in an anonymized rather than pseudonymized form. Already at the time of submission of the request, the user is required to indicate in a precise and detailed manner the identity of the natural persons in charge of processing the data and, once the measure has been obtained, only these subjects will be allowed access to the processing environment. This will take place according to a double track operating *ex ante* through procedures of entry into the environment by means of personal identification keys; and *ex post* through the recording of every single operation carried out by the authenticated and identified subject in the secure processing environment. The history of the activities carried out ends up becoming a deterrent to the improper use of access data to the secure environment, and at the same time constitutes an effective tool for ascertaining any abuses

and responsibilities in the secondary management of the data made accessible, favoring a reasonable application of any sanctions imposed.

VI. THE FIGURE OF THE "RELIABLE OWNER".

In the context of the reuse of health data, a final mention should be made of the figure of the "reliable" data holder, i.e. a data holder who, in the light of certain subjective peculiarities and, as a result of an investiture by the individual Member State, is considered suitable for the autonomous management of access requests concerning the data held by him. Thanks to the absence of intermediation by central bodies, if the user intends to use the data in the possession of these figures, the procedural *process* must be initiated directly against the data subject, with the consequence that the subject in question will also become the data controller for secondary use and the data processor for the data granted for use to the applicant. On an operational level, the simplified procedure for access to data in which the reliable controller is present does not derogate from the precautions provided for by the regulation, which are intended to be fully applicable to that entity as well. However, while the provision of a secure processing environment for data sharing seems to be an essential obligation even for the reliable controller, a different argument should be made with regard to the internal structuring of the same. In the opinion of the writer, in fact, the need to equip oneself with a corporative organization capable of guaranteeing horizontal functional autonomy should not be considered indefectible in the hypothesis *in question*. A careful reading of the data authorization procedure highlights how the request for access to the datasets addressed to the reliable data controller does not end with a properly authorizational measure, but rather takes the form of an opinion accompanied by a proposal for a decision; a proposal that must in any case be passed to the scrutiny of the data access body, which can ratify it or deviate both from it and from the opinion issued by the reliable owner. The decision-making process, while not affecting the legal nature that the reliable data controller assumes in the context of the processing, nevertheless guarantees that the authorization measure is in any case the result of an assessment by the data access body (with mere control functions), thus allowing us to dispel any doubts about the presence of potential conflicting interests. On the contrary, the possibility of issuing a decision that differs from that proposed by the reliable owner could be justified precisely in the possible presence of a conflict of interest that the reliable owner by his nature is unable to overcome. Ultimately, for reliability, in the absence of an express provision of the regulation, it does not seem possible to include among the characteristics of the controller, the adoption of a corporate structure as specified by the regulation for data access bodies.

VII. BRIEF CONCLUDING REMARKS

The framework outlined by the European legislator for the governance of health data for secondary use, as repeatedly emphasized, is the result of a delicate and declared compromise between political objectives driven by the ambition to channel the data market along the lines of altruism and the collective interest, and the need to legally protect

individual subjective interests. Balancing these concerns must take into account a fundamental circumstance: the space of health data created by the new regulation is not conceived as a physical reality, but has a purely digital dimension. It follows that to ensure the efficient development of the EHDS and its governance, it is essential to respect those prerogatives that for twenty years have become axioms of the correct creation and dissemination of digital data. The latter, as is well known, presupposes the essential existence of a medium—the electronic document—capable of maintaining reliability, authenticity, integrity, legibility, and retrievability over time. Well, it is therefore appropriate to highlight how only through an accurate and meticulous respect of these characteristics, the greater the informative potential of the electronic health data will be and the higher the possibilities of implementing the altruistic purposes favored by its secondary use will be.