European Review of Digital Administration & Law - Erdal
2022, Volume 3, Issue 2, pp. 13-33
ISSN 2724-5969 – ISBN 979-12-218-0798-1 - DOI 10.53136/9791221807981 03

*Data Governance Act and Re-Use of Data in the Public Sector**

Fabio Bravo
(Full Professor of Private Law, University of Bologna, Italy; Director of the Postgraduate Course in Privacy and Data Protection Officer, University of Bologna, Italy)

ABSTRACT This article aims to provide a critical analysis of the legal framework for the re-use of data held by public sector bodies, in the light of both the European Commission's Communication on the European Data Strategy and the new European Data Governance Act. What emerges is a new approach by the European legislator that requires public administration to play a new role, not only as an intermediary and facilitator in the circulation of data, but also as the one who can 'empower' natural and legal persons to exercise their rights over data and information belonging to protected categories. The new protection mechanisms outlined in the Data Governance Act present significant critical aspects from a legal point of view, but also new perspectives, which are discussed in this work.

1. *A new European approach to data*

The European Commission, in its Communication entitled "A European Strategy for Data" [COM(2020) 66 final, 19.2.2020], has adopted a new fortified approach towards a regulation of personal and non-personal data. The starting point can be found in the awareness that "Over the last few years, digital technologies have transformed the economy and society, affecting all sectors of activity and the daily lives of all Europeans (…)."[1] In this scenario it was clearly stated that "(…) Data is at the centre of this transformation and more is to come. Data-driven innovation will bring enormous benefits for citizens, for example through improved personalised medicine, new mobility and through its contribution to the European Green Deal."[2]

On the basis of such premise, the European Commission significantly argued that "In a society where individuals will generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules."[3]

However, this anthropocentric vision also meets the needs of the (European single) market, in a multiple perspective typical of the European approach: together with the celebration of the individual protection of persons' fundamental rights and freedoms, we can find the statements concerning the opportunities of a relevant social and economic development.[4] In this direction, the Commission stated that "Citizens will trust and embrace data-driven innovations only if they are confident that any personal data sharing in the EU will be subject to full compliance with the EU's strict data protection rules. At the same time, the increasing volume of non-personal industrial data and public data in Europe, combined with technological change in how the data is stored and processed, will constitute a potential source of growth and innovation that should be tapped."[5]

The enormous significance attributed to the processing of (personal and non-personal) data can be perfectly understood. Data are openly considered "the new oil",[6] not without some negative implications which need to be addressed, especially in the field of data protection law[7], competition law[8] and AI law.[9] How-

* Article submitted to double-blind peer review.

[1] European Commission, *A European Strategy for Data* [COM(2020) 66 final, 19.2.2020], Brussels, 2020, 1.

[2] European Commission, *A European Strategy for Data*, 1.

[3] European Commission, *A European Strategy for Data*, 1.

[4] See also S. Rodotà, *Tecnologie e diritti*, Bologna, Il Mulino, 1995.

[5] European Commission, *A European Strategy for Data*, 1.

[6] K. Bhageshpur, *Data Is The New Oil - And That's A Good Thing*, in *Forbes*, 15 November 2019, available online at www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/;

[7] D.D. Hirsch, *The Glass House Effect: Big Data, the New Oil, and the Power of Analogy*, in *Maine Law Review*, 2014, available at SSRN: https://ssrn.com/abstract=2393792; L. Scholz, *Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies*, in *Tennessee Law Review*, 2020, Vol. 85, available at SSRN: https://ssrn.com/abstract=3252543.

[8] See European Parliament, *Is data the new oil? Competition issues in the digital economy*, Brussels, 2020, available online at www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)6

ever, the main value of data should not be founded in their direct economic worth, but in the set of capabilities that can be derived from themselves, by means of an accurate analysis.
That is precisely the crux of the matter. The great value of data mainly consists in supporting decision-making. Data and data analysis allow for better decisions, with huge benefits for natural and legal persons, such as citizens, associations, foundations, non-governmental organizations (NGOs), enterprises and companies, and public administrations.
According to the above-mentioned Communication, "Citizens should be empowered to make better decisions based on insights gleaned from non-personal data. And that data should be available to all – whether public or private, big or small, start-up or giant. This will help society to get the most out of innovation and competition and ensure that everyone benefits from a digital dividend. This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident."[10]
The approach adopted by the European Commission seems not to be the one based on the "commodification" of personal and non-personal data, in order to have a monetary gain in the digital market of data, but the one that consider data as means of innovation and development for society, institutions and markets, both in private and public sector, "to enable the EU to become the most attractive, most secure and most dynamic data-agile economy in the world – empowering Europe with data to improve decisions and better the lives of all of its citizens."[11]
In fact, the European Union aims to build a different model, in which data do not consist in "commodities" or "goods", but, first of all, in "a value" available to all, as a key factor of growth, wealth and development, for the entire society, including citizens, public administrations, enterprises and other public and private bodies.
In this direction the European Commission strongly specified – in its Communication on "The European Strategy for Data" – that "The EU can become a leading role model for a society empowered by data to make better decisions – in business and the public sector. To fulfil this ambition, the EU can build on a strong legal framework – in terms of data protection, fundamental rights, safety and cybersecurity – and its internal market with competitive companies of all sizes and varied industrial base. If the EU is to acquire a leading role in the data economy, it has to act now and tackle, in a concerted manner, issues ranging from connectivity to processing and storage of data, computing power and cybersecurity. Moreover, it will have to improve its governance structures for handling data and to increase its pools of quality data available for use and re-use. Ultimately, Europe aims to capture the benefits of better use of data, including greater productivity and competitive markets, but also improvements in health and well-being, environment, transparent governance and convenient public services."[12]
A couple of years later, those considerations have been translated into a new regulation, dedicated to the European Data Governance: the EU Regulation No. 868/2022 ("Data Governance Act"),[13] by means of which the European legislator has intended to facilitate data-sharing in the internal market, by creating a harmonised legal framework for data exchanges, without prejudice to data protection law (Regulation No. 679/2016, General Data Protection Regulation – GDPR).[14]
Regarding that matter, the aim of this essay is to examine the legal framework and analyse the main disruptive legal issues concerning the governance of data held by public bodies under the above-mentioned Data Governance Act, focusing on the re-use of such data for commercial and non-commercial purposes and the new role attributed to the public bodies themselves, taking into account, at the same

46117_EN.pdf.
[9] G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, Mucchi, 2021; B. Custers and E. Fosch-Villaronga (eds.), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice*, Springer, 2023; L. Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities*, Oxford, Oxford University Press, 2023.
[10] European Commission, *A European Strategy for Data*, 1.
[11] European Commission, *A European Strategy for Data*, para. 7.
[12] European Commission, *A European Strategy for Data*, 1.
[13] Regulation (EU) No. 868/2022 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). According to its Art. 38, the DGA is applicable from 24 September 2023.
[14] Regulation (EU) No. 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 (General Data Protection Regulation, GDPR).

time, the interrelations with the data protection law.

2. *Data Governance Act as a major component of the European Strategy for Data and the key role of data intermediaries*

It is perfectly clear, and it can be proved by the opening words used in the first Recital of the Data Governance, that the European legislator has intended to "provides for the establishment of an internal market and the institution of a system ensuring that competition in the internal market is not distorted" and therefore "the development of a framework for data governance should contribute to the achievement of those objectives, while fully respecting fundamental rights."

The re-use of large amounts of personal and non-personal data held by public sector bodies is therefore, according to the European strategy, one of the main key factors in achieving this general objective, which is aimed at the development of a European data market, where competition is ensured, preserved, and facilitated. This approach is clearly outlined in the Data Governance Act, in which the European legislator wished to leverage and strengthen the role of relevant figures, capable of furthering this objective, both in the private and in the public sectors.

The fundamental idea underlying this strategy is to resort to public and private subjects as "intermediaries" of personal and non-personal data, so as to favour the movement and re-use of said data by other subjects, with various purposes, connected to the carrying out of entrepreneurial activities, for altruistic aims and to pursue a public interest.

It should be considered that Chapter III of the Data Governance Act (see Articles 10-15) contains the regulations of the "*Data intermediation services*"[15] provided by "*data intermediation services providers*",[16] which include not only private intermediaries that collect and facilitate the use of personal data belonging to others, but also "*data cooperatives*",[17] who obtain data from their own members and then circulate them in favour of other subjects,[18] and even public bodies: as is clearly noted by Recital No. 27, "Data intermediation services providers, which may include public sector bodies, that offer services that connect the different actors have the potential to contribute to the efficient pooling of data as well as to the facilitation of bilateral data sharing."[19]

Data intermediation, within this framework, concerns commercial relationships, which the intermediary seeks to favour, even if they are a public sector body. Therefore Recital No. 29 DGA specifies, among other things, that "This Regulation should not apply to services of-

[15] In accordance with Art. 2, para. 1, no. 11, DGA, "'data intermediation service' means a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data, excluding at least the following:
(a) services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users;
(b) services that focus on the intermediation of copyright-protected content;
(c) services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things;
(d) data sharing services offered by public sector bodies that do not aim to establish commercial relationships."

[16] F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa,* 2021, 1, 199-256; D. Poletti, *Gli intermediari di dati*, in *European Journal of Privacy Law and Technologies*, 2022, 1, 45-56.

[17] F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, 2023, Vol. 39, Issue No. 3, 757-799; L. Petrone, *Il mercato digitale e le cooperative di dati*, in *Contratto e impresa*, 2023, Vol. 39, Issue 4, 800-817.

[18] The DGA, under Art. 2, para. 1, No. 15, expressly mentions the "services of data cooperatives", defined as "data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data".

[19] The strategic importance of data intermediation services, offered by public and private sector subjects, is clearly highlighted in the rest of Recital No. 27, where it is added that "Data intermediation services are expected to play a key role in the data economy, in particular in supporting and promoting voluntary data sharing practices between undertakings or facilitating data sharing in the context of obligations set by Union or national law. They could become a tool to facilitate the exchange of substantial amounts of relevant data. (…)."

fered by public sector bodies in order to facilitate either the re-use of protected data held by public sector bodies in accordance with this Regulation or the use of any other data, insofar as those services do not aim to establish commercial relationships."

This seems like a way to counter the oligopoly (and in some cases the virtual monopoly) of extra-European "Big Tech" multinational corporations and favour both the rise of new European enterprises in this field, as well as of European data spaces, which are independent from those managed by the afore-mentioned multinational corporations and an alternative to them, with major effects on the market. The above-mentioned Recital No. 27 itself specifies that "(…) Specialised data intermediation services that are independent from data subjects, data holders and data users could have a facilitating role in the emergence of new data-driven ecosystems independent from any player with a significant degree of market power, while allowing non-discriminatory access to the data economy for undertakings of all sizes, in particular SMEs and start-ups with limited financial, legal or administrative means. This will be particularly important in the context of the establishment of common European data spaces, namely purpose- or sector-specific or cross-sectoral interoperable frameworks of common standards and practices to share or jointly process data for, inter alia, the development of new products and services, scientific research or civil society initiatives. Data intermediation services could include bilateral or multilateral sharing of data or the creation of platforms or databases enabling the sharing or joint use of data, as well as the establishment of specific infrastructure for the interconnection of data subjects and data holders with data users."

Furthermore, under the Chapter IV of the Data Governance Act (see Articles 16-25) another kind of data intermediary – in a broad sense – has been regulated: the "recognised data altruism organisations", who have a role in the voluntary sharing of both personal and non-personal data, on the basis of the consent of data subject or permissions of data holders, without seeking or receiving any reward.[20] The Regulation does not use the term "intermediaries" for such entities, but it is perfectly clear that they operate in that very role, albeit in a different context and to meet other needs, other than commercial ones, to which *public administrations* are certainly not unrelated. One must but consider what is specified in Art. 16 DGA, which sets out that "Member States may have in place organisational or technical arrangements, or both, to facilitate data altruism. To that end, Member States may establish national policies for data altruism. Those national policies may, in particular, assist data subjects in making personal data related to them held by public sector bodies available voluntarily for data altruism, and set out the necessary information that is required to be provided to data subjects concerning the re-use of their data in the general interest."

Also to this end the Data Governance Act aims at achieving the EU's ambitious strategies in an innovative manner, by favouring the movement of data not only for market needs, but also for "altruistic" needs related to individual and social welfare, as well as for needs related to the pursuit of the general interest. A relevant element in this respect is the definition of "*data altruism*" contained in Art. 2, para. 1, No. 16, DGA, which states that it "(…) means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest."

What clearly emerges it the link between *data altruism* and *public administration*, whereby the personal data of the data subjects and the non-personal data of the data holders that are

[20] In accordance with Art. 2(16) of the Data Governance Act, "'*data altruism*' means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable, such as healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest."

voluntarily made available for altruistic purposes may be used by public sector bodies in the general interest, to improve the public policies and public services in the various sectors in which public administration operates, ranging from healthcare to mobility, from the environment to energy, as well as the activities aimed at preventing and tackling the consequences of climate change. The purpose of this list is simply to provide some examples and it may be enhanced in relation to every activity aimed at achieving the general interest, whose care is entrusted to the action of public administration.

Within the framework of data altruism, public administrations are not only considered subjects benefiting from the voluntary sharing of data by data subjects and data holders, provided for by Art. 2, para. 1, No. 16, DGA mentioned above. Broadly speaking, they themselves may act as intermediaries in the data altruism sector, by formally regaining the role of recognised *data altruism organisation* under Art. 18 of the Data Governance Act, which determines that "In order to qualify for registration in a public national register of recognised data altruism organisations, an entity shall: (a) carry out data altruism activities; (b) be a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, where applicable; (c) operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis; (d) carry out its data altruism activities through a structure that is functionally separate from its other activities; (e) comply with the rulebook referred to Article 22(1), at the latest 18 months after the date of entry into force of the delegated acts referred to in that paragraph."

Public administrations, owing to their role, are legal persons established under national law to pursue the general interests identified within the framework of the national law of a Member State (see lett. *b*) and, within this context, they operate without pursuing profit-making, independently from bodies seeking to pursue profit-making (see lett. *c*) by adopting an *ad hoc* "structure", tasked with performing these activities, in a manner that is functionally separate from the other institutional activities performed by the body (see lett. *d*), by complying with the "rulebook" adopted by the European Commission for the recognised data altruism organisations pursuant to Art. 22 DGA, through the adoption of delegated acts (see lett. *e*).

Thus public administrations could act more effectively in the field of data altruism, by entering a virtuous cycle functional to the pursuit of the general interest, with great potential in terms of efficiency increase and the good performance of public administration, all in compliance with the independence principle, which in the field under examination is also articulated based on subjects whose action is aimed at the pursuit of commercial and profit-making goals.[21]

Other specific rules concerning *public administrations as data intermediaries*, broadly speaking, are provided in Chapter II of the Data Governance Act (see Articles 3-9), dedicated to the "*Re-use of certain categories of protected data held by public sector bodies*."

The aim of this legal regime is to ensure that data, generated or collected by public administrations or other entities at the expense of public budgets, benefit the whole society, even though data, because of the special category which they pertain to, are out of the application of the EU Directive 2019/1024 on "*Open data and reuse of public-sector information*".

Therefore this aspect is also highlighted for the Data Governance Act, which is crucial to the free movement of data. The data held by public administration cannot be considered data owned by public administration to be used for its own benefit to perform sovereign powers, but rather as data of the community, which the public administration holds on behalf of the citizens, so as to pursue the general interest and as these data are collected and managed with economic resources taken from society, said data must be made available to society and, therefore, also to private citizens intending to pursue commercial and non-commercial purposes, not related to the initial purposes for which the data are acquired and processed by the public administration itself.

In this respect the content of Recital No. 6 DGA is far too clear, where it is clarified that "The idea that data that has been generated or collected by public sector bodies or other entities at the expense of public budgets should benefit society has been part of Union policy

[21] A good performance and impartiality of public administration are principles that in Italy are also set under Art. 97 of the Constitution: "(…) Public offices are organised according to the provisions of law, so as to ensure the efficiency and impartiality of administration (…)."

for a long time (…)", as is the content of Art. 2, para. 1, No. 2, DGA, which provides the definition of "re-use" of data, specifying that "'re-use' means the use by natural or legal persons of data held by public sector bodies, for *commercial or non-commercial purposes* other than the initial purpose within the public task for which the data were produced, except for the exchange of data between public sector bodies purely in pursuit of their public tasks".

As in some sectors of the legal system personal and non-personal data enjoy special protection, the Data Governance Act aims at favouring the re-use of these data too, where possible, without undermining the protection guarantees provided for by the special rules governing these areas.

In this respect Recital No. 6 can be useful, specifically where it specifies that "(…) Directive (EU) 2019/1024 and sector-specific Union law ensure that the public sector bodies make more of the data they produce easily available for use and re-use. However, certain categories of data, such as commercially confidential data, data that are subject to statistical confidentiality and data protected by intellectual property rights of third parties, including trade secrets and personal data, in public databases are often not made available, not even for research or innovative activities in the public interest, despite such availability being possible in accordance with the applicable Union law, in particular Regulation (EU) 2016/679 and Directives 2002/58/EC and (EU) 2016/680. Due to the sensitivity of such data, certain technical and legal procedural requirements must be met before they are made available, not least in order to ensure the respect of rights others have over such data or to limit the negative impact on fundamental rights, the principle of non-discrimination and data protection. The fulfilment of such requirements is usually time- and knowledge-intensive. This has led to the insufficient use of such data. While some Member States are establishing structures, processes or legislation to facilitate that type of re-use, this is not the case across the Union. In order to facilitate the use of data for European research and innovation by private and public entities, clear conditions for access to and use of such data are needed across the Union."

Therefore, the Data Governance Act attempts to introduce legal solutions to make such data, ruled under a restrictive regime, available for a re-use for commercial and non-commercial purposes, preserving at the same time the respect for fundamental rights.

The role of public administration, in this respect, is extremely interesting, because it winds up acting, in the public interest, as an intermediary, in the logics of re-use of data which it holds for its institutional purposes, while preserving the protection of the subjects to whom these data refer to who, thanks to the action of public administration, can enjoy an enhanced system that protects their rights.[22]

While however in the field of the provision of "data intermediation services" referred to in Chapter III and data altruism referred to in Chapter IV the public sector bodies can contribute with those of the private sector to performing an intermediary role aimed at favouring data circulation, in the case of "Re-use" referred to in Chapter II intermediation can occur only through the action of the bodies acting in the public sector, regarding data, falling under certain categories, which they hold to pursue their institutional purposes. The subjects that operate in the private sector can interact with public administration and have access to said data and their re-use, for commercial and non-commercial purposes, within the limits and conditions of the specific legal regulations outlined therein (Articles 3-9 DGA)

3. *Data Governance Act and the re-use of (certain categories of protected) data held by public sector bodies, for commercial and non-commercial purposes*

The issue of the re-use of data held by public sector bodies is of course nothing new: specific regulations were already present in Directive 2019/1024/EU on open data and the re-use of public sector information.[23] For some categories of data, however, the movement follows more restrictive rules, owing to the need to protect trade and professional secrets, statistical confidentiality, intellectual property rights of third parties and fundamental rights connected to personal data.

[22] The mechanism can be partly compared to the services of data cooperatives, within the field of the provision of data intermediation services in the private sector, referred to in Recital No. 31, under Art. 2, para. 1, No. 15 and Articles 10-15 of the Data Governance Act. See F. Bravo, *Le cooperative di dati*, 757-799.

[23] J. Valero Torrijos, *Datos abiertos y reutilización en el contexto de la Estrategia europea de datos*, in *Tábula*, 2021, 201-213; T. Douville, *Open data des décisions de justice, cinq ans après : état des lieux et perspective*, in *Légipresse*, Vol. 65, No. HS1, 2021, 49-61.

Following the new European strategy on data governance, with the Data Governance Act the European legislator chose to favour the re-use of said data in this very field, creating at the same time the prerequisites to preserve a high level of protection to defend the requirements that the sectorial legislation, in the afore-mentioned fields, aimed to safeguard.

Art. 3, para. 1, DGA, therefore identifies the scope of application of the new regulatory provisions on re-use, which apply to "data held by public sector bodies which are protected on grounds of: (a) commercial confidentiality, including business, professional and company secrets; (b) statistical confidentiality; (c) the protection of intellectual property rights of third parties; or (d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024."[24]

The Data Governance Act therefore aims at enhancing the regulations related to the re-use of data held by public sector bodies, already provided for by Directive 2019/1024/EU on open data and the re-use of public sector information, by also applying it to other data, held by public sector bodies, who are under a restrictive data flow regime.

The goal is to build a trustworthy environment to increase the availability of personal and non-personal data for "secondary use" and, therefore, facilitate the re-use of data and the creation of innovative services and products based on data.

It can be considered a major component of the European strategy for data, which aims to bolster both the data economy and the data-driven society.

The introduction of regulations on the re-use of personal and non-personal data held by public administration provides a major role to public administration, which thus becomes a facilitator in the data movement and enhancement processes which it already has at its disposal by virtue of its institutional purposes.

It should be noted, however, that with the Data Governance Act the EU did not seek to require the public administration to make available the data it already holds for re-use: the Member States will decide to what extent public administration will be involved in the national law, with the risk of heterogeneous situations arising from this in the various national legal systems. In particular, Recital No. 11 DGA specifies that, in this respect, "This Regulation should not create an obligation to allow the re-use of data held by public sector bodies. In particular, each Member State should therefore be able to decide whether data is made accessible for re-use, also in terms of the purposes and scope of such access (…)." Moreover, the same Recital also adds that "This Regulation should complement and be without prejudice to more specific obligations on public sector bodies to allow re-use of data laid down in sector-specific Union or national law. Public access to official documents may be considered to be in the public interest. Taking into account the role of public access to official documents and transparency in a democratic society, this Regulation should also be without prejudice to Union or national law on granting access to and disclosing official documents. Access to official documents may in particular be granted in accordance with national law without imposing specific conditions or by imposing specific conditions that are not provided by this Regulation."

Of course, the role of public administration, in making available data and information that can have a strategic importance on the market, must be impartial. Otherwise it would dangerously alter the competition dynamics that the Data Governance Act sought to favour.

Thus, Art. 4 DGA forbids exclusive arrangements that give an advantage to some subjects to the detriment of others, unless the granting of the exclusive rights to the re-use of data constitutes a necessary measure to ensure the provision of a service or product of general interest that would otherwise be impossible to provide. In this case, however, the exclusive rights, which must be agreed on through an administrative act or a contract, are limited in time and are subject to the principle of transparency: they can only last up to twelve

[24] Art. 3, para. 2, DGA, however, clarifies that the provisions concerning the re-use of data foreseen in the Data Governance Act do not apply to the following further data categories: "(a) data held by public undertakings; (b) data held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit; (c) data held by cultural establishments and educational establishments; (d) data held by public sector bodies which are protected for reasons of public security, defence or national security; or (e) data the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State concerned, or, in the absence of such rules, as defined in accordance with common administrative practice in that Member State, provided that the scope of the public tasks is transparent and subject to review."

months and the reasons that made the exclusive rights necessary must be made public online, in a form that complies with the European regulations on the matter of public procurement.[25]

One of the key features of the regulations on the re-use of data covered in the DGA are the terms of the re-use provided by Art. 5.

Firstly, para. 1 determines that "Public sector bodies which are competent under national law to grant or refuse access for the re-use of one or more of the categories of data referred to in Article 3(1) shall make publicly available the conditions for allowing such re-use and the procedure to request the re-use via the single information point referred to in Article 8. Where they grant or refuse access for re-use, they may be assisted by the competent bodies referred to in Article 7(1).

Member States shall ensure that public sector bodies are equipped with the necessary resources to comply with this Article."

The European legislator, with the DGA, could have set the requirement for public sector bodies to make available the data for the re-use, but instead chose to have the Member States work on the more specific regulation. The national law will therefore regulate whether public sector bodies have the right to grant or reject the requests to access the data they themselves hold. The European regulation does not formally introduce an *obligation* of the public sector bodies of providing the data for re-use, but it does not prohibit this obligation from being introduced in the national law. In other words, the national legal systems will introduce criteria, principles, *obligations* and *rights*, by virtue of which the public sector bodies will make available the data to be devoted to re-use, which will consequently lead to a heterogenous situation across Member States, a far cry from the goal of achieving the homogeneity in EU law that a regulation, unlike a directive, is supposed to achieve. This is certainly a critical aspect, which suggests that there will be further regulatory measures implemented by the European legislator to create uniformity between national legal systems, at a later, riper stage.

The discretion of Member States is not boundless, given that, albeit with the criteria that will be set at a national level, they are nevertheless required to allow for the re-use of data belonging to the above-mentioned categories and to provide the public sector bodies with the necessary *resources* to achieve said goal. The discretion of Member States is also limited by the need to meet a set of principles generally applicable to public administrations, which however in Art. 5, para. 3, DGA are further specified with a particular focus on the re-use of data: "Conditions for re-use shall be non-discriminatory, transparent, proportionate and objectively justified with regard to the categories of data and the purposes of re-use and the nature of the data for which re-use is allowed. Those conditions shall not be used to restrict competition."

Apart from the impartiality principle, also in relation to the effects on the competition dynamics, transparency and proportionality, there is also a clear doctrine of necessity, which requires the conditions of re-use to be "objectively justified", not only meaning that they must guarantee a balanced reconciliation of the relevant interests, but also in the sense that they must lead to the achievement of the goal sought by the legislator (re-use of certain categories of protected data held by public sector bodies") with the smallest sacrifice possible of the opposed interest protected by the legal system (protection of the data subject, protection of the intellectual property rights, and so on), without this interest being devalued, undermined or destroyed in its funda-

[25] See Art. 4 (*Prohibition of exclusive arrangements*): "1. Agreements or other practices pertaining to the re-use of data held by public sector bodies containing categories of data referred to in Article 3(1) which grant exclusive rights or which have as their objective or effect to grant such exclusive rights or to restrict the availability of data for re-use by entities other than the parties to such agreements or other practices shall be prohibited.
2. By way of derogation from paragraph 1, an exclusive right to re-use data referred to in that paragraph may be granted to the extent necessary for the provision of a service or the supply of a product in the general interest that would not otherwise be possible.
3. An exclusive right as referred to in paragraph 2 shall be granted through an administrative act or contractual arrangement in accordance with applicable Union or national law and in compliance with the principles of transparency, equal treatment and non-discrimination.
4. The duration of an exclusive right to re-use data shall not exceed 12 months. Where a contract is concluded, the duration of the contract shall be the same as the duration of the exclusive right.
5. The grant of an exclusive right pursuant to paragraphs 2, 3 and 4, including the reasons as to why it is necessary to grant such a right, shall be transparent and be made publicly available online, in a form that complies with relevant Union law on public procurement.
6. Agreements or other practices falling within the scope of the prohibition referred to in paragraph 1 which do not meet the conditions laid down in paragraphs 2 and 3 and which were concluded before 23 June 2022 shall be terminated at the end of the applicable contract and in any event by 24 December 2024."

mental characteristics.
Within this framework, the DGA does not refrain from setting specific conditions for the re-use of data, which emphasise the new role given to public sector bodies within this context: not only of "intermediary" (in a broad sense) in the re-use of the data held by them, which in particular fall under the categories subject to specific protection, but also of active supervisor, facilitator and, above all, "*protector*" and "*enhancer*" of the rights of those who can be damaged by the movement of the data, belonging to specific protected categories, held by public sector bodies.
The latter, upon granting access to the data for re-use, are required to play an *active role*, which goes far beyond making available the data they already hold by virtue of the performance of institutional tasks. They must, in accordance with European and national law, do all that is necessary to "ensure that the protected nature of data is preserved (…)".[26]
The DGA, in particular, requires public sector bodies to "to grant access for the re-use of data only where the public sector body or the competent body, following the request for re-use, has ensured that data has been:
(i) anonymised, in the case of personal data; and
(ii) modified, aggregated or treated by any other method of disclosure control, in the case of commercially confidential information, including trade secrets or content protected by intellectual property rights (…)".[27]
This is a first active measure on data and in terms of control, both with the goal of tackling the risks of infringement of rights otherwise undermined by the movement of the data themselves within the framework of re-use strategies, and to ensure that said rights are preserved and not undermined.
The European legislator has envisaged a second important measure to the same end, by requiring that the access and re-use of said data – anonymised, modified, aggregated or treated, as specified above – occur "remotely within a *secure processing environment* that is provided or controlled by the public sector body"[28] or "within the physical premises in which the *secure processing environment* is located in accordance with high security standards, provided that remote access cannot be allowed without jeopardising the rights and interests of third parties."[29] Thus, in a general way in the field of re-use of data held by public sector bodies a solution that has already been tested at a European level for research on statistical microdata in the basis of Commission Regulation (EU) No. 557/2013 is applied.[30]
Moreover, a third measure required from public sector bodies entails the preservation of the integrity of the systems used to create a treatment environment that is safe for accessing and re-using data, with powers-duties of public administration both in terms of regulations and of control, that extend even to the results of the processing activity carried out by the data re-user, whose use may also be prohibited following the above-mentioned control.[31]
The guarantee and control functions performed by public service bodies when it comes to the re-use of data, together with that of "enhancer" of rights emerge from the further role assigned to them in the stage of information flow: they "(…) shall make the re-use of data (…) conditional on the adherence by the re-user to a confidentiality obligation that prohibits the disclosure of any information that jeopardises the rights and interests of third parties that the re-user may have acquired despite the safeguards put in place"[32]; moreover, the public bodies who perform the re-use of data will receive any notification on the violations of data that may occur among data re-users, who are required to meet certain requirements.[33] For example the GDPR re-

[26] Art. 5, para. 3, DGA.
[27] Art. 5, para. 3, lett. *a),* DGA.
[28] Art. 5, para. 3, lett. *b),* DGA.
[29] Art. 5, para. 3, lett. *c),* DGA.
[30] See Commission Regulation (EU) No. 557/2013 of 17 June 2013 implementing Regulation (EC) No. 223/2009 of the European Parliament of the Council on European Statistics as regards access to confidential data for scientific purposes and repealing Commission Regulation (EC) No. 831/2002.
[31] See Art. 5, para. 4, DGA: "In the case of re-use allowed in accordance with paragraph 3, points (b) and (c), the public sector bodies shall impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body shall reserve the right to verify the process, the means and any results of processing of data undertaken by the re-user to preserve the integrity of the protection of the data and reserve the right to prohibit the use of results that contain information jeopardising the rights and interests of third parties. The decision to prohibit the use of the results shall be comprehensible and transparent to the re-user."
[32] Art. 5, para. 5, DGA.
[33] In accordance with Art. 5, para. 5, DGA it is also set out that "(…) Re-users shall be prohibited from re-identifying any data subject to whom the data relates and shall take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects

quires that the data breach notification by performed by the data controllers to the relevant Data protection Supervisory Authority: this element highlights the special guarantee and control position of the public sector bodies.

The DGA also covers the possibility of the re-use of personal data not being done anonymously, for example if the anonymisation jeoparidises the utility of the data for the user.[34] Under these circumstances the data transfer operations by the public sector body, which holds the personal data, to the subject intending to use the data within the framework of the re-use strategies, may be performed only if there is a legal basis that allows this transfer of data even without the consent of the data subject[35] or if there is a specific consent coming from the data subjects.[36] Here too one can witness the proactive role of the public sector bodies which, based on the DGA's regulations, "shall make best efforts, in accordance with Union and national law, to provide assistance to potential re-users in seeking *consent* of the data subjects or *permission* from the data holders whose rights and interests may be affected by such re-use, where it is feasible without a disproportionate burden on the public sector body (…)".[37]

A similar regime is also applied to (non-personal) data deemed confidential at a commercial or statistical level, before which "(…) the public sector bodies shall ensure that the confidential data is not disclosed as a result of allowing re-use, unless such re-use is allowed in accordance with paragraph 6"[38] (abovementioned), on the basis of the data subjects' consent or the data holders' permission.

Regarding third categories of protected data held by public sector bodies, the DGA merely requires, categorically, that the "re-use of data shall be allowed only in compliance with intellectual property rights (…)"[39]: this requires the authorisation of the holder of intellectual property rights, unless the re-use falls under the scenarios of "fair use" provided for by the sectorial legislation.

There is however the risk that the regulations on the matter of intellectual property winds up hampering the European strategy on the re-use of data if it recognises the intellectual property rights directly in the hands of the public sector bodies. To avert this risk the DGA requires the latter not to exercise these rights in contrast with the purposes of the re-use of data: in particular it is set out that "(…) The right of the maker of a database as provided for in Article 7(1) of Directive 96/9/EC shall not be exercised by public sector bodies in order to prevent the re-use of data or to restrict reuse beyond the limits set by this Regulation."[40]

These are major provisions because they seek to prevent strategies by public administration aimed at not sharing data and even if the public sector bodies held intellectual property rights on the data, they "should, however, exercise their copyright in a way that facilitates

concerned to the public sector body. In the event of the unauthorised re-use of non-personal data, the re-user shall, without delay, where appropriate with the assistance of the public sector body, inform the legal persons whose rights and interests may be affected."

[34] Regarding the re-use of data, the approach of the European legislator, in the DGA, is to set a progressive safeguard, by adopting instruments of maximum protection, which can however by lightened progressively to avoid undermining the re-use strategy. Recital No. 15 DGA is particularly important in this respect, specifically in the part in which it states that "Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a data protection impact assessment and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed. This could be a suitable arrangement for the re-use of pseudonymised data (…)."

[35] For instance, when the processing is necessary: (i) "for compliance with a legal obligation to which the controller is subject" (Art. 6, para. 1, lett. *c*, GDPR); (ii) "in order to protect the vital interests of the data subject or of another natural person" (Art. 6, para. 1, lett. *d*, GDPR); (iii) "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Art. 6, para. 1, lett. *e*, GDPR); (iv) "for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Art. 6, para. 1, lett. *f*, GDPR); (v) "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy" (Art. 9, para. 2, lett. *i*, GDPR); and so on.

[36] See Art. 6, para. 1, lett. *a*, and Art. 9, para. 2, lett. *a*, GDPR.

[37] Art. 5, para. 6, DGA.

[38] Art. 5, para. 8, DGA.

[39] Art. 5, para. 7, DGA.

[40] Art. 5, para. 7, DGA.

re-use".[41]
Specific guarantees are then envisaged in the event that the re-user intends to transfer the data to a third country. In the case of personal data, the special regulations in the GDPR would be applied. In the case of non-personal data, on the other hand, the DGA introduces the requirement, of the re-user, to inform the public body on the intention of the re-user and of the purpose of the transfer, upon requesting the re-use, for the public body to exert further control functions, even to prevent the transfer until "the legal person whose right and interests may be affected of that intention (…) gives permission for the transfer."[42] In the meantime, the re-user must contractually undertake not only to meet, also in the event of transfer of data to a third country, the obligations covered by Art. 5, paragraphs 7 and 8, DGA on the flow across the EU of the data falling under the regulations of confidential information and intellectual property rights, but also to accept "the jurisdiction of the courts or tribunals of the Member State of the transmitting public sector body with regard to any dispute related to compliance with paragraphs 7 and 8."[43] To favour said contractual commitments, similarly to what is already provided for by the GDPR on the transfer of personal data to third countries, the European Commission may introduce, through its implementing acts, specific model contractual clauses to meet the above-mentioned requirements. In the event of a violation of the requirements envisaged for the transfer of data to a third country, the natural or legal person to which the right to re-use non-personal data was granted cannot perform the transfer to said third country.[44]
The push for personal and non-personal data flow is clear. To eliminate the uncertainties on the outcome of the re-use requests, they must be processed within two months since their reception, both in the event of an approval and of a rejection, unless different and shorter deadlines are set in accordance with national law: longer deadlines are not allowed.[45] The only exception provided by the DGA concerns the case of "exceptionally extensive and complex" re-use requests: here the two-month deadline can be prolonged for a maximum of thirty additional days, notifying "the applicant as soon as possible that more time is needed for conducting the procedure, together with the reasons for the delay."[46]
The complexity of the role played by public sector bodies on the re-use of data held by them is clear, so much so that the European legislator had to move in three further directions, so as to put into practice the new European strategy on data governance and make it more effective.
On the one hand there has been the introduction of the possibility, by the public bodies that allow the re-use of data belonging to the specific categories considered by the DGA, to impose fees, which "shall be transparent, non-discriminatory, proportionate and objectively justified and shall not restrict competition."[47]
The non-discrimination principle does not prevent however different fees from being applied, in relation to specific needs, for example to incentivise the re-use of data for non-commercial purposes (as could be the case in the field of scientific research) or the re-use in favour of SMEs and start-ups subject to rules on State aid, or the re-use of data whose request comes from civil society or educational institutions. One may therefore apply reduced fees or reuse data free of charge. These would nevertheless be exceptions compared to the general principle, which envisages the application of a fee system, also for the service to be economically sustainable and efficient, by taking into account both the active role played by public bodies in this specific field (which is added to the normal institutional role they play) and of the costs related to the procedure carried out to meet the re-use requests.[48]
The fee system shall however be established at a national level by the single Member States, also regarding the criteria and methodology to calculate the fees and shall contrib-

[41] Recital No. 17, DGA.
[42] Art. 5, para. 9, DGA.
[43] Art. 5, para. 10, DGA.
[44] Art. 5, para. 14, DGA.
[45] Art. 9, para. 1, DGA.
[46] Art. 9, para. 1, DGA.
[47] Art. 6, para. 2, DGA.
[48] One must note that under Art. 6, para. 5, DGA it is specified that "Any fees shall be derived from the costs related to conducting the procedure for requests for the re-use of the categories of data referred to in Article 3(1) and limited to the necessary costs in relation to: (a) the reproduction, provision and dissemination of data; (b) the clearance of rights; (c) anonymisation or other forms of preparation of personal data and commercially confidential data as provided for in Article 5(3); (d) the maintenance of the secure processing environment; (e) the acquisition of the right to allow re-use in accordance with this Chapter by third parties outside the public sector; and (f) assisting re-users in seeking consent from data subjects and permission from data holders whose rights and interests may be affected by such re-use."

ute, once again, to the spread of heterogeneous choices across the EU.[49] At any rate, each public body is required to meet transparency principles, which in this case is the obligation to "publish a description of the main categories of costs and the rules used for the allocation of costs."[50]

On the other hand the public sector bodies, upon granting or rejecting the re-use of the data belonging to the specific categories covered by the DGA, must be assisted by one or more "competent bodies"[51] equipped with the necessary knowledge and means,[52] designed by each Member State, with the following tasks: (i) "providing technical support by making available a secur processing environment for providing access for the reuse of data";[53] (ii) "providing guidance and technical support on how to best structure and store data to make that data easily accessible";[54] (iii) "providing technical support for pseudonymisation and ensuring data processing in a manner that effectively preserves the privacy, confidentiality, integrity and accessibility of the information contained in the data for which re-use is allowed, including techniques for the anonymisation, generalisation, suppression and randomisation of personal data or other state-of-the-art privacy-preserving methods, and the deletion of commercially confidential information, including trade secrets or content protected by intellectual property rights";[55] (iv) "assisting the public sector bodies, where relevant, to provide support to re-users in requesting consent for re-use from data subjects or permission from data holders in line with their specific decisions, including on the jurisdiction in which the data processing is intended to take place and assisting the public sector bodies in establishing technical mechanisms that allow the transmission of requests for consent or permission from re-users, where practically feasible";[56] (v) "providing public sector bodies with assistance in assessing the adequacy of contractual commitments made by a re-user pursuant to Article 5(10)", [57] in the event of transfers of non-personal data to third countries.

The Member States may assign a key role to the "competent bodies", by enabling them to grant themselves access for the re-use of the data belonging to the categories covered by the DGA, pursuant to European or national law which provides for such access to be granted. In said case all the provisions applicable to the public sector bodies that grant the re-use of data in accordance with the DGA shall be applicable to the "competent bodies", including the provisions on the matter of "Prohibition of exclusive arrangements" (Art. 4), "Conditions for re-use" (Art. 5), "Fees" (Art. 6) and "Procedure for requests for re-use" (Art. 9).

Finally, as a third measure, it has been decided that there will be the establishment by the Member States of "Single information points" with multiple tasks, aimed at making it easier to find the information on the re-use of data and the processing of the requests, with functions that "may be automated provided that the public sector body ensures adequate support."[58]

In particular the Single information points must: (i) make available and easily accessible all the information related to the conditions of re-use of data and the applicable fees;[59] (ii) "transmit them, where possible and appropriate by automated means, to the competent public sector bodies, or the competent bodies (…), where relevant";[60] (iii) "make available by electronic means a searchable asset list containing an overview of all available data resources including, where relevant, those data resources that are available at sectoral, regional or local information points, with relevant information describing the available data,

[49] Art. 6, para. 6, DGA.
[50] Art. 6, para. 6, DGA.
[51] The "competent bodies" established from scratch by the Member States, or the latter may rely on existing public sector bodies or on internal services of public sector bodies that fulfil the conditions laid down in the DGA. See Art. 7, para 1, DGA.
[52] In accordance with Art. 7, para. 3, DGA, "The competent bodies shall have adequate legal, financial, technical and human resources to carry out the tasks assigned to them, including the necessary technical knowledge to be able to comply with relevant Union or national law concerning the access regimes for the categories of data referred to in Article 3(1)."
[53] Art. 7, para. 4, lett. *a*, DGA.
[54] Art. 7, para. 4, lett. *b*, DGA.
[55] Art. 7, para. 4, lett. *c*, DGA.
[56] Art. 7, para. 4, lett. *d*, DGA.
[57] Art. 7, para. 4, lett. *e*, DGA.
[58] Art. 8, para. 1, DGA. The path towards using automated systems has been inaugurated here too, including those based on AI (Artificial Intelligence), which nevertheless require human oversight, as can be witnessed in Recital No. 26, in which it is noted that "Sufficient human oversight should be ensured in the transmission process." See also G. Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Milan, Wolters Kluwer-Cedam, 2023.
[59] Art. 8, para. 1, DGA.
[60] Art. 8, para. 3, DGA.

including at least the data format and size and the conditions for their re-use."[61]
Furthermore, the single information points can "establish a separate, simplified and well-documented information channel for SMEs and start-ups, addressing their needs and capabilities in requesting the re-use of the categories of data referred to in Article 3(1)."[62]
To make the action of the single information points more effective, the decision made was to develop them at various territorial levels. A single information point is established at national level, by each Member State, which may designate, to this end, a new body or an existing body or structure.[63] Along with the "national" single information point, each Member State can then envisage other "sectoral, regional or local information points", connected to the central one, located at a national level. The national single information points, in turn, are connected to a European single access point, established by the European Commission, "offering a searchable electronic register of data available in the national single information points and further information on how to request data via those national single information points."[64]

4. ***Critical aspects***

The critical aspects of the new regulations on the re-use of data by the public sector bodies are certainly numerous and some of them have already been highlighted.
The European legislator chose to use a regulatory source that ultimately leads to an overall uniformity in the Member States' legislation, by resorting to the European "regulation" to regulate European data governance, but, at least regarding the re-use of data, the European legislator wound up delegating many of the identified solutions to the discretional choices of the Member States, thus undermining the goal of regulatory uniformity within the EU: take for example the choice of letting the Member States determine whether the Public sector bodies have the right to decide whether to grant or reject access for the re-use of one or multiple categories of data, as well as determine the applicable fees for the re-use, in accordance with Articles 5 and 6 DGA.
Moreover, apart from the lack of uniformity at European level, the need for regulatory measures at a national level leads to an unavoidable postponement of the regulations' implementation, as one must wait for regulatory acts in the national legal systems, which result in a delayed actual implementation of the regulations in question compared to the deadline envisaged by Art. 38 DGA, in accordance with which the regulation "shall apply from 24 September 2023."
Some critical aspects had been highlighted by the EDPB and the EDPS in the Joint-Opinion No. 3/2021 on the Proposal for a regulation of the European Parliament and of the Council on Euopean data governance (Data Governance Act), v. 1.1, 9 June 2021. These are, however, findings that are not universally deemed valid.
The first of these concerns the ambiguity and uncertainty between the application boundaries of the regulations on the re-use of data in the DGA and the regulations provided for by Directive (EU) 2019/1024 on the matter of open data,[65] which should have been better specified, not only within the Recitals, but also with dedicated articles of the regulation.[66]
In the final text of the DGA, Art. 3, para. 1, lett. d), clarifies that Chapter II, on the "Re-use of certain categories of protected data held by public sector bodies", "(…) applies to data held by public sector bodies which are protected on grounds of: (…) d) the protection of personal data, insofar as such data fall outside the scope of Directive (EU) 2019/1024."
Art. 1 of said Directive sets out that "In order to promote the use of open data and stimulate innovation in products and services, this Directive establishes a set of minimum rules governing the re-use and the practical arrangements for facilitating the re-use of (…) existing documents held by public sector bodies of the Member States (…)" and that, however, it "(...) does not apply to (…) documents, access to which is excluded or restricted by virtue of the access regimes on grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data or as undermining the

[61] Art. 8, para. 3, DGA.
[62] Art. 8, para. 3, DGA.
[63] Art. 8, para. 4, DGA.
[64] Art. 8, para. 4, DGA.
[65] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
[66] See EDPB-EDPS, *Joint Opinion No. 3/2021*, Section 3.3.1.

protection of privacy and the integrity of the individual, in particular in accordance with Union or national law regarding the protection of personal data."[67]

The regulations on the matter of "open data and re-use of public sector information", therefore, do not exclude beforehand the possibility of the re-use of personal data held by public sector bodies: it allows it when it does not violate the regulations on the matter of personal data protection, including the cases in which one resorts to the anonymisation of personal data. In fact, Recital No. 52 of the Open Data Directive expressly states that "This Directive does not affect the protection of individuals with regard to the processing of personal data under Union and national law, particularly Regulation (EU) 2016/679 and Directive 2002/58/EC of the European Parliament and of the Council and including any supplementing provisions of national law. This means, inter alia, that the re-use of personal data is permissible only if the principle of purpose limitation as set out in point (b) of Article 5(1) and Article 6 of Regulation (EU) 2016/679 is met. Anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. Rendering information anonymous is a means of reconciling the interests in making public sector information as re-usable as possible with the obligations under data protection law, but it comes at a cost. It is appropriate to consider that cost to be one of the cost items to be considered to be part of the marginal cost of dissemination as referred to in this Directive."

By taking this into account, however, the new Data Governance Act encourages the application of the regulations on the re-use of data held by public sector bodies contained in the open data directive,[68] while also proposing to extend the scope of data re-usability, if this is not possible in accordance with the regulations contained in the above-mentioned directive. Recital No. 10, DGA, is very clear about this, where it is clarified that "The categories of data held by public sector bodies which should be subject to re-use under this Regulation fall outside the scope of Directive (EU) 2019/1024 that excludes data which is not accessible due to commercial and statistical confidentiality and data that is included in works or other subject matter over which third parties have intellectual property rights. Commercially confidential data includes data protected by trade secrets, protected know-how and any other information the undue disclosure of which would have an impact on the market position or financial health of the undertaking. This Regulation should apply to personal data that fall outside the scope of Directive (EU) 2019/1024 insofar as the access regime excludes or restricts access to such data for reasons of data protection, privacy and the integrity of the individual, in particular in accordance with data protection rules (…)."[69]

Therefore the interpreter, during the implementation, shall determine when the regulations on the re-use of data referred to in Directive (EU) 2019/1024 are applicable and when the regulations referred to in the DGA are. There may be cases of partial overlapping, which should be resolved with the application of the DGA, both because it came after the 2019 Directive (*lex posterior derogat priori*), and because it must be considered a special law compared to the more general law contained in the directive *(lex speciali derogat generali)*. It must be noted, in this respect, that in the DGA the regulations of Chapter II are more limited both from a subjective point of view, in that it only concerns data held by *public sector bodies*, with the exclusion of data held by public undertakings, (included instead in the 2019 Directive), and from an objective point of view, in that it only concerns "*certain categories of protected data*" (while the regulations on the re-use contained in the 2019 Directive covers larger categories of data).

Moreover, the regulations contained in the DGA are immediately applicable in all Member States and would prevail over the rules of the national legislation of the Member States,

[67] Art. 1, para. 2, lett. h, Directive (UE) 2019/2014.

[68] See Recital No. 9, DGA: "(9) In order to facilitate the protection of personal data and confidential data and to speed up the process of making such data available for re-use under this Regulation, Member States should encourage public sector bodies to create and make available data in accordance with the principle of 'open by design and by default' referred to in Article 5(2) of Directive (EU) 2019/1024 and to promote the creation and the procurement of data in formats and structures that facilitate anonymisation in that regard."

[69] See Recital No. 10, DGA, which also adds that "(…) The re-use of data, which may contain trade secrets, should take place without prejudice to Directive (EU) 2016/943, which sets out the framework for the lawful acquisition, use or disclosure of trade secrets."

rendered in implementation of the previous directive, even more so if one considers the fact that the DGA lacks the rules aimed at establishing that Directive 2019/1024 would prevail in the event of contrast with the Regulation, [70] unlike what is provided for in other regulatory fields, including those regulating the protection of personal data and competition law.[71]

A second finding by the EDPB and the EDPS concerns the heterogeneity of the categories of data covered by the regulations on re-use outlined in the DGA, which winds up generating applicational uncertainties: in particular when it brings together under a single "umbrella" the heterogeneous categories of personal and non-personal data (regarding intellectual property rights and confidential information protected for commercial or statistical reasons) and suggests that the regulations on the matter of personal data protection hinders the re-use of data, thereby slowing down the general interest and the economy.[72] The EDPB and the EDPS even describe these aspects as "*regrettable*, since it suggests the idea of data protection regulation as impeding the free movement of personal data, rather than laying down the rules of free flow of personal data while protecting the rights and interests of the persons concerned."[73]

Based on the regulatory framework of the DGA, analysed above, I believe that this judgment is far too harsh and not in line with the approach adopted by the European legislator who, by further incentivising the re-use of certain categories of data held by public sector bodies, has implemented a system that is particularly focused on realising the protection of the rights and freedoms of data subjects and making it effective, also thanks to the new role outlined for public administration and the further adjustments (i.e. secure processing environment; competent bodies).[74]

Other issues emerge regarding the coordination between the DGA and the GDPR.

What is certainly unfortunate is the introduction of subjective categories, such as those of data holder and data user, which are not well coordinated with those used in the GDPR (data controller, data processor, data subject) and can potentially create great uncertainty in the implementation of the regulations on the matter of European data governance.[75] The uncertainty is then exacerbated by the translation choices made in the national legal systems, such as in Italy, where data processor is translated as "titolare del trattamento" and data holder as "titolare dei dati". The interpreter of the regulation once again will be tasked with creating a system of these subjective categories in European and national law, while taking into account the interactions between the regulations on the matter of data protection and those on the matter of data governance.

Then it must be noted that, in general, the DGA does not introduce new legal bases for the lawfulness of processing, therefore the personal data processing performed upon the re-use are only legitimate if the legal basis envisaged by Articles 6-9 of the GDPR are met. In this respect the final text of the DGA, compared to the text of the proposal, is clearer, as is shown by Art. 5, para. 6, DGA and, above all, by Art. 1, para. 3, DGA, where it is expressly specified that "(…) This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations

[70] An implicit reference to the rules of Directive (EU) 2019/1024 can be found in Art. 2 DGA, but its formulation does not allow for the former to prevail on the latter in every situation: on the contrary, the formulation seems to indicate that the rules of the DGA and the further provisions of European and national law are applicable, provided that they guarantee (and do not limit) the re-use and access to data. The above-mentioned Art. 2 DGA in fact clarifies that "(…) This Regulation is without prejudice to: (a) specific provisions in Union or national law regarding the access to or re-use of certain categories of data, in particular with regard to *the granting of access* to and *disclosure* of official documents; (b) the obligations of public sector bodies under Union or national law to *allow* the re-use of data or to requirements related to processing of non-personal data."

[71] In fact, Art. 1, para 3 and 4, DGA sets out that "Union and national law on the protection of personal data shall apply to any personal data processed in connection with this Regulation. In particular, this Regulation is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directives 2002/58/EC and (EU) 2016/680, including with regard to the powers and competences of supervisory authorities. In the event of a conflict between this Regulation and Union law on the protection of personal data or national law adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data shall prevail. This Regulation does not create a legal basis for the processing of personal data, nor does it affect any of the rights and obligations set out in Regulations (EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680" (para 3) and that "This Regulation is without prejudice to the application of competition law" (para 4).

[72] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 66-67.

[73] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 68.

[74] See above, in this work, Section No. 3.

[75] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para. 29-46.

(EU) 2016/679 or (EU) 2018/1725 or Directives 2002/58/EC or (EU) 2016/680."

It must however be noted that the DGA, upon outlining the conditions of re-use of personal data, legitimises it [the re-use] when the data are anonymised by the public sector body holding them. However, the anonymisation process too, mentioned in the DGA, is a processing operation that would require the presence of a legal basis in accordance with the GDPR. It is not certain that the anonymisation is a processing operation covered by the legal basis used to legitimise the original processing activity, while in the DGA it is peacefully covered as a systematic operation, a default operation, to guarantee the flow of data in the perspective of re-use. In this case the DGA seems to introduce a new element compared to the GDPR, as it envisages at a regulatory level an anonymisation obligation, which can easily be traced back to the legal categories of the GDPR. It would therefore be a processing operation whose legal basis was a regulatory requirement in accordance with Art. 6, para. 1, lett. *c*), GDPR,[76] or in the (substantial) public interest pursued by the public sector body to achieve, in accordance with the rights of the data subjects, the re-use purposes of the data sought by the European legislator and the anonymisation operation is therefore based on Art. 6, para. 1, lett. *e*),[77] and Art. 9, para. 2, lett. *g*), GDPR,[78] to connect to the regulatory provision contained in Art. 5, para. 3, lett. a(i), DGA, which requires the anonymisation of personal data the meet the requirements of re-use, while preserving the free flow of data without undermining the rights and freedoms of the data subjects.

From a different perspective, the EDPB and the EDPS highlight the need to nevertheless meet the principles of data protection described in Art. 5, paragraphs 1 and 2, GDPR,[79] including the principle of purpose limitation,[80] which limits the scenario of secondary use of personal data to the boundaries outlined by Art. 6, para. 4, GDPR, whereby "Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law (…), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

The solutions proposed by the DGA move in a "complementary" direction: the regulation of the re-use of certain particular categories of data held by public sector bodies does not affect the secondary use referred to in Art. 6, para. 4, GDPR – which is therefore implicitly confirmed – but rather the concrete and effective possibility of using personal data for further purposes other than those of initial data collection, both through anonymisation (and the envisaging of instruments to make it more concretely possible), and through collection mechanisms of a new consent of the data subjects – where anonymisation is not a viable option – to legitimise the further processing of personal data, for purposes not considered upon the initial collection.

Another issue arises for all the scenarios in

[76] Based on Art. 6, para 1, lett. c), GDPR, "Processing shall be lawful only if and to the extent that at least one of the following applies: (…) processing is necessary for compliance with a legal obligation to which the controller is subject (…)".

[77] According to Art. 6, para 1, lett. e), GDPR, "Processing shall be lawful only if and to the extent that at least one of the following applies: (…) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (…)".

[78] In accordance with Art. 9, para 2, let. e), GDPR, the prohibition of processing data belonging to specific categories of data shall not be applied in the event that "processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

[79] For an analysis of the legal regulations of the "Principles" on the matter of personal data protection see F. Bravo (ed. by), *Dati personali. Protezione, libera circolazione,* governance. – Vol. 1, *Principi*, Pisa, Pacini, 2023.

[80] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 73-75.

which the personal data cannot be anonymised: the subsequent re-use may occur with the consent of the data subject which the public sector body will seek to obtain from the data subject, unless there is another legal basis for the processing of personal data other than consent. The critical aspect however derives from the need to meet both the principle of purpose limitation, which requires the purpose of the processing to be clearly and specifically identified and for the processing not going beyond this purpose,[81] and the principles of precision and granularity of consent which, to be valid, must be given based on a duly specific and limited illustration of the purposes of the processing operation that will be pursued.[82]

Providing general consent to the re-use of data is therefore not sufficient, as the purpose of the processing operation one intends to pursue must be clearly outlined, otherwise the consent would inevitably be null and void. Moreover, natural persons are often required to provide their data to public sector bodies based on the requirements of the law or upon the request of a public service and the absence of clear information regarding the re-use of data and the purposes pursued may violate the principles of transparency and fairness provided for by the GDPR.[83]

From a different perspective, one must also verify the validity of the consent when it comes to freedom: the regulations on the re-use of data in the DGA envisages that the public sector bodies must act to request the consent for the processing of personal data for re-use to the subjects towards whom they play an institutional role, therefore potentially resulting in a clear situation of power imbalance, which undermines the freedom of the consent provided by the data subjects.[84]

The specificity of the subject actually seems to indicate that the public sector bodies involved the citizens by allowing them to participate in a collaborative and open manner in the procedures aimed at allowing the re-use of their personal data.[85] This should also lead to restoring a certain order between public power, in the hands of the body that acts to request the consent for the processing of data for re-use, and the data subject called upon to give their consent, thus giving back validity to the consent, when it comes to the freedom requirement,[86] although it would be far better for the re-use scenarios to be determined directly based on a regulatory measure, either from the EU or national,[87] that is of an administrative

[81] In accordance with Art. 5, para 1, lett. b), GDPR, "Personal data shall be (…) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')".

[82] These elements come from the definition of consent, contained in Art. 2, para 1, No. 11, GDPR ("'consent' of the data subject means any freely given, *specific*, informed and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"). See also F. Bravo, *Le condizioni di liceità del trattamento*, in G. Finocchiaro (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 110; D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza italiana*, 2019, 12, 2783-2789.

[83] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 84.

[84] In this respect it has been noted that "(…) it is unclear the role of the public sector body in supporting re-users in obtaining the consent for the reuse by the data subject. As a further remark on Article 5(6) of the Proposal, the EDPB and the EDPS point out that this provision establishes an obligation for public sector bodies ("shall support"), whose content is not well defined. More to the point, the legal basis under the GDPR for contacting data subjects to collect their consent for the re-use should be specified, as well as the respective responsibility related to obtaining a valid consent under Article 7 of the GDPR. In this regard, it should also be taken into account the clear imbalance of power which is often present in the relationship between the data subject and the public authorities. In this context, in line with the GDPR accountability principle, the EDPB and the EDPS recall that the choice of an appropriate legal basis for the processing of personal data, as well as the demonstration that the chosen legal basis (in this case consent) can be validly applied, lies on the data controller". See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 82.

[85] The EDPB and EDPS recommended "to define in the Proposal [of the DGA] adequate means by which individuals may participate, in an open and collaborative manner, in the process of allowing the re-use of their personal data". See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 85.

[86] In this direction see EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 19 May 2021, 6: "(…) due to the fact that the consent of the data subject might not be considered freely given due to the imbalance of power which is often present in the relationship between the data subject and the public authorities, the Joint Opinion expresses concerns on Article 5(6) of the DGA, and, more broadly, invites the co-legislators to clearly define in the Proposal adequate models of 'civic participation', by which individuals may participate, in an open and collaborative manner, in the process of defining the scenarios allowing the re-use of their personal data, following a bottom-up approach to open data projects (…)."

[87] See, again, EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 6: "The Joint Opinion also recommends amending the

instrument of a general nature, if – as is the case of the Italian legal system – this is allowed by the national legislation.[88]

Another critical aspect concerns the matter of the re-use of personal data regarding above all "sensitive sectors" such as healthcare. According to the EDPB and the EDPS, the DGA was supposed to set, in these sectors, the necessary requirements of the protection of personal data, as well as the related conditions and specific data protection safeguards"[89] to meet for the re-use of data, including the data protection impact assessment (DPIA) pursuant to Art. 35 GDPR, also necessary to found the decision on re-use.[90] The choice of the European legislator, in the DGA, was however different: the obligation to perform the DPIA was already envisaged in the GDPR, and said European Regulation remains applicable to the cases of re-use of personal data held by public sector bodies, and prevails in the event of conflict with the provisions of the DGA. As it is already regulated in the GDPR, there is no need to envisage the DPIA obligation in a systematic way in the DGA too for all the scenarios of re-use of data: the applicational boundaries of this obligation shall nevertheless remain those outlined by the GDPR. The obligation to perform the DPIA, for the re-use of non-anonymised personal data, is in any case mentioned in the Recitals.[91]

A further critical aspect highlighted by the EDPB and the EDPS concerns the role of the competent bodies and the relationship with the role of the national Data Protection Supervisory Authorities envisaged in the GDPR and in Art. 8 of the Charter of Fundamental Rights of the EU (CFREU): the risk is that it may generate a multiplying effect of public subjects with competence in the field of data protection, to leave only to the oversight authorities that have already been established with the GDPR, and an interference between tasks and functions in said matter.[92] In this respect it has been specified, on the one hand, that it is by no means clear whether a Data Protection Supervisory Authority can be identified as a "competent body" under Art. 7 DGA;[93] on the

DGA to clarify that the re-use of personal data held by public sector bodies may only be allowed if it is grounded in Union or Member State law which lays down a list of clear compatible purposes for which the further processing may be lawfully authorised or constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23 of the GDPR."

[88] E.g. Art. 2-b ("Legal basis to process personal data for the performance of a task carried out in the public interest or in the exercise of official authority"), para 1, of the Italian Personal Data Protection Code (D.Lgs. 196/2003), Containing provisions to adapt the national legislation to 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 (As amended by decree-law No 139 of 8 October 2021 subsequently enacted and amended by way of Law No 205 of 3 December 2021). According to the Art. 2-b cited, "The legal basis mentioned in Article 6(3), letter b), of the Regulation shall be a law or a regulation or an *administrative instrument of a general nature*".

[89] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 87.

[90] The EDPB and EDPS highlighted that "according to the GDPR, the data protection impact assessment (DPIA) is a key tool to ensure that data protection requirements are properly taken into account and the rights and interests of individuals are adequately protected, so as to foster their trust in the re-use mechanism. Therefore, the EDPB and EDPS recommend to include in the text of the Proposal that a DPIA must be performed by public sector bodies in case of data processing falling under Article 35 of the GDPR. The DPIA will help to identify the risks and the appropriate data protection safeguards for the re-use addressing those risks, in particular for specific sector routinely with special categories of personal data (…)". See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 88, where it is also specified that "(…) The decision on the re-use, in addition to being grounded on Union or Member State law, especially for some "sensitive sectors" (healh sector, but also transport or energy grid) should be based on this assessment, as well as the specific conditions for the re-users and the concrete safeguards for data subjects (for example, clarifying the risks of re-identification of anonymized data and the safeguards against those risks). Finally, the results of such assessment, whenever possible, should be made public, as a further measure enhancing trust and transparency".

[91] The obligation to carry out the DPIA pursuant to Article 35 GDPR is mentioned in Recital No. 15 of the DGA: "(…) Before transmission, personal data should be anonymised, in order not to allow the identification of the data subjects, and data containing commercially confidential information should be modified in such a way that no confidential information is disclosed. Where the provision of anonymised or modified data would not respond to the needs of the re-user, subject to fulfilling any requirements to carry out a *data protection impact assessment* and consult the supervisory authority pursuant to Articles 35 and 36 of Regulation (EU) 2016/679 and where the risks to the rights and interests of data subjects have been found to be minimal, on-premise or remote re-use of the data within a secure processing environment could be allowed (…)." See also Recital No. 7, DGA.

[92] EDPB-EDPS, *Joint Opinion No. 3/2021*, para 104-106.

[93] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 103, where, regarding the competent bodies referred to in Art. 7 DGA it was specified that "(…) despite those bodies are essentially tasked with support and advisory duties vis-à-vis public sector bodies for data re-use, some of their tasks deal with implementing the safeguards set out in the data protection legislation and fos-

other hand the use of "competent" in "competent bodies" under the above-mentioned Art. 7 was criticised;[94] finally, what was highlighted was the need to establish collaboration mechanisms between competent bodies and the Data Protection Supervisory Authorities, with the guiding role played by the latter, "to ensure a coherent application of these provisions."[95]

A final critical aspect to be considered concerns the fee system envisaged by Art. 6 DGA, which in the DGA would constitute the rule, while in the Open Data Directive it would be the exception before the general principle of gratuity of the re-use of data: this contradiction, however, highlighted once again by the EDPB and the EDPS, is actually just apparent.[96] Directive (EU) 2019/1024, in fact, under Art. 6 ("Principles governing charging") envisages, in para. 1, that "The re-use of documents [and data] shall be free of charge", but it also adds that "However, the recovery of the marginal costs incurred for the reproduction, provision and dissemination of documents as well as for anonymisation of personal data and measures taken to protect commercially confidential information may be allowed."[97] Therefore, gratuity is a principle that can be applied only if the public sector bodies perform the re-use of data that are not under specific protection regimes: otherwise, if these bodies are required to protect personal data or commercially confidential information, the general rule is that it is allowed to apply fees for covering the costs taken on to guarantee the protection requirements. In the DGA the regulations on the re-use of data held by public sector bodies specifically concerns "certain categories of protected data", therefore the solution proposed in the DGA appears completely compliant with the choices also made in the Open Data Directive. The criticism of the EDPB and the EDPS seems to miss the mark.

A different matter is the incentive system. It has been highlighted that the regulations envisaged in the DGA seem "(…) to introduce financial incentives to public sector bodies to allow the re-use of personal data."[98] Moreover, in the same way it has also been noted that Art. 6 para. 4, DGA introduces a system of fee incentives to favour the re-use of data in the non-commercial sector or in the sector of State aid,[99] with possible repercussions on the validity of the consent to the processing of personal data with the purpose of re-use and on the actual exercise of the right to revoke one's consent.[100] Also in this case the concerns seem exaggerated, given that the incen-

tering the protection of the rights and interests of individuals with regards to their personal data. However, Chapter II (…) does not clarify whether data protection supervisory authorities – to which the GDPR also confers, among others, advisory powers – may be designed as the competent body under Article 7 (…)" of the DGA.

[94] See EDPB-EDPS, *Joint Opinion No. 3/2021*, para 105: "Furthermore, should specific bodies be designated to assist public sector bodies and data re-users and be entrusted to grant access for the reuse of data, including personal data, such bodies may not be referred as 'competent' as they would not act s a supervisory authority able to monitor and enforce the provisions related to the processing of personal data. In order to ensure legal certainty and consistency of the application of the EU acquis in the field of personal data protection, the activities and obligations of such designed bodies shall also be subject to the direct competence and supervision of data protection authorities, when personal data is involved."

[95] EDPB-EDPS, *Joint Opinion No. 3/2021*, para 106.

[96] For this criticism see, again, EDPB-EDPS, *Joint Opinion No. 3/2021*, para 96.

[97] Still in accordance with Art. 6 of the Directive (UE) 2019/1024, the principle of gratuity f re-use does not apply in the case of "public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks" e di "public undertakings", for which "the total charges shall be calculated in accordance with objective, transparent and verifiable criteria. Such criteria shall be laid down by Member States. The total income from supplying and allowing the re-use of documents over the appropriate accounting period shall not exceed the cost of their collection, production, reproduction, dissemination and data storage, together with a reasonable return on investment, and — where applicable — the *anonymisation of personal data* and measures taken to protect commercially confidential information. Charges shall be calculated in accordance with the applicable accounting principles."

[98] EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 97.

[99] See EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para 98, where it is specified that "It also has to be noted that Article 6(4) imposes an obligation to public sector bodies to "take measures to incentivize the reuse of the categories of data referred to in Article 3 (1) [which include personal data] for non-commercial purposes and by small and medium-sized enterprises in line with State aid rules."

[100] See, finally, EDPB-EDPS, *Joint Opinion No. 3/2021*, cited, para. 99, where, regarding the system of fee incentives it was noted that "This aspect (…) is problematic from a data protection viewpoint, under both legal and practical implementation's perspective. In particular, the lack of clarity on the type of incentives and addressees thereof may raise additional questions as to whether consent, as one of the legal basis relied upon under Article 5(6) of the Proposal for the re-use personal data, will be the appropriate legal ground, especially with regard to the individuals' freedom of choice to refuse to provide their consent to the re-use of their personal data or to withdraw it."

tives do not operate in favour of the data subjects, for the purposes of providing one's consent to the data processing, but rather towards the data users, who request access or the transfer of the personal data held by public sector bodies, after the consent of the data subjects has already been given. It seems as though the data subjects cannot receive any pressure from the data users, to which the fee incentives are applied, so much so that the interactions for the re-use are intermediated by the public sector bodies, called upon to exercise a guarantee function and to "enhance" the rights of the data subjects themselves.

5. ***New prospects***

The different approach introduced in the Data Governance Act (DGA), compared to the Open Data Directive (ODD), on the re-use of protected categories of data held by public administration, paves the way towards a new role of public sector bodies.

These bodies, apart from using the personal and non-personal data at their disposal for their functions, tied to the achievement of public interest, are called upon to act to ensure the flow of the data belonging to protected categories. They are asked to implement what is necessary to ensure both the fruition of the data for the data users, and an adequate level of protection of the rights and interests that the legal system chose to ensure by regulating certain categories of protected data considered in the DGA.

Within this context, public bodies seem to be called upon to reinterpret their action based on the principle of solidarity, by implementing the sovereign powers (as traditionally understood) and by establishing a new relationship with the citizens, whereby the latter see their ability to dialogue with public administration grow, as well as their areas of "active freedom", which come with greater duties and responsibilities for public administration.[101] The public sector bodies become not only intermediaries of the data they hold and facilitators of the free flow of data for commercial and non-commercial purposes not connected to the exercise of sovereign powers, but also subjects with a guarantee function towards those who, because of the nature of these data, have the right to hold a high level of protection of their rights and interests, connected to these data. The DGA outlines an enhanced protection, as it identifies specific protection measures, which translate into duties for public administration: to guarantee the re-use of data the DGA envisages that public administration must implement or oversee the anonymisation of public data, where possible, as well as the adoption of specific security measures, including the establishment of a secure processing environment. The guarantee and enhancement functions of the rights of the subjects to whom these categories of data refer to are then further enhanced with the action of the competent bodies, which are complemented with the action of the single information points, for the flow of data to be more impactful within a framework of re-use.

The relevant regulations overlook some important aspects, which will have to be addressed by the national legislators and by the relevant legal theory.

One concerns the profiles of responsibility that this new role entails for the public sector bodies and the competent bodies, for example where the anonymisation of data has not been carried out or verified correctly by public administration, or if the secure processing environment has not been correctly set up or managed or, also, if the public sector bodies, after receiving the notification of a violation of the non-personal data subject to protection (for example regarding trade secrets or intellectual property) did not act accordingly to counter the violation and curb the damage endured by those whose rights have been infringed.

Another important aspect, which must be examined, is how the re-use of the data held by public bodies will be contractualised, for commercial and non-commercial purposes. While when it comes to non-personal data one can resort to tried-and-tested concepts within the framework of intellectual property law, through the use of licenses, when it instead comes to personal data one must refrain from opting for easy and hasty solutions that are not compliant with European law. When it comes to personal data one cannot identify an ownership of the public sector bodies or other entities holding personal data,[102] nor can contracts

[101] See A.G. Orofino, *La solidarietà in diritto ammnistrativo: da strumento di protezione dell'individuo a parametro di disciplina del rapporto*, in *Il diritto dell'economia*, 2020, 2, 594; F. Benvenuti, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, Venice, Marsilio, 1994, *passim*.

[102] G. Alpa, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, Zorzi Galgano (ed.), Milan, Wolters Kluwer-Cedam, 2019, 11. See also V. Zeno Zencovich, *Do "data markets" ex-*

on the re-use of personal data have as their object the "sale" of data: when it comes to personal data that are not anonymised, one will have to take into account the specific aspects of the GDPR's regulations, as "one of [its] main purposes (…) is to provide data subjects with control over personal data relating to them",[103] preventing personal data from being deemed "a 'tradeable commodity'. An important consequence of this is that even the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights. As a further consequence, the controller to whom consent has been provided by the data subject to the processing of her or his personal data is not entitled to 'exchange' or 'trade' personal data (as a so-called 'commodity') in a way that would result as not being in accordance with all applicable data protection principles and rules."[104]

This must not lead to the conclusion that personal data cannot be the object of contracts regulating their use, but rather that the adopted contractual solutions must be compliant with the specific nature of the fundamental right attributed to the data subject. Personal data can be the temporarily used for legitimate and specific purposes and in compliance with the principles indicated by the GDPR (including those of lawfulness, transparency and fairness, data minimisation, purpose limitation, storage limitation), which (also) have a limitative scope of contractual autonomy, to safeguard the rights and fundamental freedoms of the data subject.

Another very important aspect concerns civic participation. Where it is not possible to anonymise personal data, the public sector bodies are required to obtain the consent of the data subjects for the re-use of personal data, with the above-mentioned problems regarding the validity of the consent acquired by the public body holding the data, given the imbalance of power between public administrations (or at any rate public sector bodies) and the data subjects. The solution put forward by the EDPB and the EDPS, aimed at emphasising civic participation, is interesting for two reasons:

(i) on the one hand it operates on a legal level and aims at eliminating the imbalance present between public administration and the citizen-data subject, through collective measure mechanisms, based on civic participation models, which can also be implemented through associations of citizens and the data subjects. This paves the way toward new forms of protection and new ways to exercise one's rights,[105] in which the single individual, who is powerless before the power of the data controller, is called upon to join organisations that can more effectively protect their interests;[106]

(ii) on the other hand, the solution is particularly important at an ethical level, because it aims at more concretely implementing the FAIR principles (which were also already mentioned in the ODD as well as in the DGA)[107] and put in place ethical models of data re-use, also if they have commercial purposes, as well as non-commercial ones.

Thus a new data governance is emerging, with the new role of public administration: with the new regulations of the DGA, public administration is tasked with managing personal data not to exercise sovereign powers by supervising the citizens-data subjects, but – also in the governance of the territory (e.g. the Urban Digital Twins) – but both to ensure a greater and more effective flow of data, with an increase in collective, economic and social welfare, and to enhance the individual protection of natural and legal persons.

In other words, the regulations on re-use leverages data governance to maximise the enhancement of data, understood in its broadest sense.

ist?, 2019, 2, 25 ff., para. 3; A. Singh, *Protecting Personal Data as a Property Right*, in *ILI Law Rev.,* 2016, 123; P. Hugenholtz, *Data property: unwelcome guest in the house of IP*, in *Better Regulation for Copyright: Academics meet Policy Makers*, Reda, Brussels, 2017, 65-77.

[103] EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 4.

[104] EDPB, *Statement 05/2021 on the Data Governance Act in light of the legislative developments*, 4.

[105] According to F. Benvenuti, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, *passim*, acknowledging the citizens' right to participation translates into making them a part of a relationship on an equal footing with the public system.

[106] This phenomenon is very reminiscent both of the forms of collective consumer protection, in European and national regulations on the matter of consumer protection (e.g. the role of consumer associations and collective actions) and of the new forms of protecting the interests of the data subjects through data cooperatives, which are also covered in the DGA.

[107] See Recital No. 2, DGA: data should be findable, accessible, interoperable and re-usable (the FAIR data principles). See also Recital No. 27 and Art. 10, ODD (Open Data and Public Sector Information Directive, Directive 2019/1024/UE).