ISSN 2723-9195

# CERIDAP

## Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
4 / 2023

OTTOBRE - DICEMBRE

# The European Strategy for Data and Trust in EU Governance. The Case of Access to Publicly Held Data

*Jane Reichel*

DOI: 10.13130/2723-9195/2023-4-10

*Nella Strategia Europea per i dati, la Commissione formula le sue proposte su come l'UE possa creare uno «spazio unico europeo dei dati». Il progetto è quello di rendere l'Europa leader di una società "guidata dai dati", creando un mercato unico per questi ultimi, che permetta loro di fluire liberamente all'interno dell'UE, e tra i vari settori: tutto ciò a vantaggio delle imprese, dei ricercatori e delle amministrazioni pubbliche. Un elemento centrale dello «spazio unico europeo dei dati» è la creazione di meccanismi di governance degli stessi, in modo tale che risultino chiari e affidabili. Concentrandosi sui dati pubblici, il contributo analizza le strutture amministrative create dalla Direttiva "Open Data", dal "Data Governance Act (DGA)", e del primo spazio settoriale dei dati proposto dalla Commissione, vale a dire lo "Spazio europeo dei dati sanitari (EHDS)". L'interrogativo che costituisce il focus del contributo è se la struttura amministrativa sviluppata dall'UE negli ultimi decenni, in termini di "amministrazione composita europea", sia in grado di raggiungere l'obiettivo di una governance dei dati chiara e affidabile.*

*In its European Strategy for Data, the Commission presents its ideas on how the EU can create a «single European data space». The plan is to make the EU a leader in a data-driven society. By creating a single market for data, it will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers, and public administrations. One central factor in the European data space is putting in place clear and trustworthy data governance mechanisms. Focusing on publicly held data, the administrative structures in the Open Data Directive, the Data Governance Act (DGA), and the first sectoral data space proposed, the European Health Data Space (EHDS), are analyzed. The question posed in the article is whether the administrative structure that has been developed in the EU for the last decades, the*

*European composite administration, is well placed to fulfil the ideal of clear and trustworthy data governance.*

*Summary: 1. Introduction.- 2. Trust, mutual trust, and sincere cooperation as legal tools for the European composite administration.- 3. The composite European administration and the role of data.- 3.1. The composite European administration and trustworthy information sharing.- 3.2. The European Strategy for Data and its regulatory framework for data and the market.- 4. Access to publicly held data in the European Strategy for Data.- 4.1. Facilitating access to publicly held data – PSI and the Open Data Directive.- 4.2. Facilitating access to protected data – the Data Governance Act.- 4.3. Obligations to give access to protected data – the EHDS proposal.- 5. The construction of «clear and trustworthy data governance» in the Open Data Directive, the DGA, and the EHDS proposal.- 5.1. Introductory remarks.- 5.2. Conditions for balancing free movement and third-party rights in a fragmented legal landscape.- 5.3. Administrative and judicial protection in the European composite administration for data.- 6. The European Strategy for Data and Trust.*

## 1. Introduction[1]

«*Data is the new gold*» – this phrase has been repeated numerous times in the public debate in the last decade. The EU has responded to this data-as-gold paradigm via the regulatory route, enacting legislative acts aiming to ensure a data society and economy that are human-centric, trustworthy and secure[2]. One of the first steps was taken with the General Data Protection Regulation (GDPR), refining already existing data protection law largely by introducing technical and organizational requirements for data processors and an innovative and powerful administrative infrastructure. The GDPR has accordingly become an important part of the *Brussels effect,* the phenomena described by Anu Bradford as the power of EU to influence which products are built and how business is conducted in the world at large, by promulgating regulations on competition law, data privacy, consumer health and safety, and environmental protection[3]. From an administrative law perspective, this infrastructure has become one of the

more innovative parts of what is commonly labeled the European integrated or composite administration, consisting of private actors collaborating closely with both European and national authorities on the implementation of EU law and policies[4].

Following the implementation of the GDPR, the Commission presented the European Strategy for Data, creating a single European data space, a single market for data[5].

On its website, the Commission describes that the aim of the strategy is to «*make the EU a leader in a data-driven society*» and that «*creating a single market for data will allow it to flow freely within the EU and across sectors for the benefit of businesses, researchers and public administrations*»[6].

The data space is based on four pillars: 1) the free flow of data, 2) European rules and values in personal data protection, consumer protection, and competition, 3) rules for access to and use of data that are fair, practical, and clear, with clear and trustworthy data governance mechanisms in place, and 4) an open, but assertive approach to international data flows, based on European values[7].

In this paper, the focus is on the second part of the third pillar: the ideal of clear and trustworthy data governance. The European Strategy for Data is not entirely clear on what is meant by trust in governance. Taking a legal perspective on the question, a trustworthy governance will here be understood as an administration with the ability to uphold the rule of law, as in foreseeability, legal certainty, and consistency in the implementation of the law, and the respect of individual rights and interests[8]. The main object of the article is publicly held data, in the form of official documents or other information held by EU and national authorities. For this purpose, the administrative structures in the Open Data Directive[9], the Data Governance Act (DGA)[10], and the first sectoral data space proposed, the European Health Data Space (EHDS)[11], are analyzed. The two acts and the proposal can be said to make up a three-layer regulatory scheme, where the Open Data Directive lays down rules for the access to data without any legal constraints, the DGA contains procedures for facilitating access to data with legal constraints (data protection, confidentiality, intellectual property), but does not prescribe any enforceable rights to access, and the EHDS contains sector-specific rules with forceful procedures to access protected health data, as well as procedures and safeguards to ensure the rights of third-party right holders (data

subjects, intellectual property owners, businesses with trade secrets). The question posed here is whether the EU can rely on its multifaceted and uncoordinated composite administration to fulfill the ideal of clear and trustworthy data governance.
The article is structured as follows. In the second section, the concepts of trust and mutual trust as tools in the composite administration within the EU are presented. The third section analyses the role of information and data in the European composite administration. The fourth section presents the European Strategy for Data and the Open Data Directive, the DGA, and the EHDS. Section five analyses the governance structure instated through the two acts and the proposal. Section six concludes the study.

## 2. Trust, mutual trust, and sincere cooperation as legal tools for the European composite administration

As seen above, trust is a central concept in the European Strategy for Data, where it is given a operative function to convince public and private organizations and individuals to be confident in allowing their data to be shared in data spaces. Trust as such is not a legal concept, and the European Strategy for Data does not give any definition of what is meant by the concept in relation to the digital market. Neither the Open Data Directive nor the DGA include the term in the legal texts, whereas it is included in one article in the proposed EHDS proposal[12]. However, already in the preamble to the GDPR, the importance of «*creating the trust that will allow the digital economy to develop across the internal market*» was recognized[13]. In the preamble to the DGA, trust is discussed in eleven recitals, in connection to a range of different aspects[14].
This use of the concept of trust can be contrasted with the more traditional EU law concept of mutual trust and its connection to concepts like mutual recognition and sincere cooperation. These concepts have a rather different function, as they can be used as conflict of law tools, to allocate the responsibilities when implementing EU law at the national level[15]. The trust to be gained is related to national legal orders and their capacity to uphold jointly accepted legal standards. A prime example is the *Cassis de Dijon* and the requirement for member states to mutually trust and recognize each other's

marketing regulations. The *Cassis de Dijon* formula for free movement of goods can be set out as[16]:

«*Products sold lawfully in one member state may not be prohibited from sale in another, save for cases where the member state can rely on national rules deemed necessary in order to satisfy mandatory requirements, relating among other things to the effectiveness of fiscal supervision, the protection of public health, the fairness of commercial transactions and the defence of the consumer*».

The institutional and procedural law construct of the European composite administration is built on a different, but comparable basis: the principle of sincere cooperation, currently enshrined in Article 4.3 in the Treaty of the European Union, TEU. As held by the Court of Justice in the seminal *Rewe* and *Comet* cases[17], decided two years before the *Cassis de Dijon* case:

«*Applying the principle of cooperation laid down in Article 5 of the Treaty, it is the national courts which are entrusted with ensuring the legal protection which citizens derive from the direct effect of the provisions of Community law*».

In the absence of common rules, the EU law thus entrusts the responsibility to uphold the legal protection of union citizens (in regard to both substantive and procedural law) to the member states and national courts, *i.e.*, the doctrine of national institutional and procedural autonomy. This conflict of law approach thus bridges the regulatory gap caused by an absence of EU secondary law, resulting either from a lack of political will, as in the *Cassis de Dijon* situation in the 1970s, or a lack of full legislative competence, as in administrative and judicial procedural law[18]. The principle of mutual trust has gradually gained in importance, and can now be seen as a principle with constitutional dimensions[19].

Current EU law includes rather extensive legislation on administrative and judicial matters, not least within the composite administration, including cooperation within criminal matters and border control[20]. Central rules were first developed in the case law of the Court of Justice; these include the obligations to ensure effective, proportionate, and dissuasive sanctions for transgressions of EU law[21] and to apply the principle of duty to care in cross-border administrative proceedings[22]. However, the development has been slow, patchy, and with differing scope for national adaptions, leaving quite some room for improvement as regards foreseeability and legal certainty for the individuals

concerned[23].

It seems that with the European Strategy for Data, a novel approach has been taken, at least at the policy level. Thus, this is no longer a question of having the member states mutually trust each other's regulatory, administrative, and judicial capacity, but having both public and private actors within the EU and beyond trust EU governance as such. EU governance is viewed as a free-standing entity, deserving of trust on its own merits. The question will be analyzed further in section 5.

## 3. The composite European administration and the role of data

### 3.1. The composite European administration and trustworthy information sharing

Due to the EU's limited powers in the fields of tax revenue and economic governance, regulation has evolved into its most important governance instrument[24]. Information sharing constitutes a central factor in the EU regulatory governance, and has been so from start. Within social security law, information exchange has been coordinated via EU secondary law since 1958, under the Administrative Commission[25]. Nowadays, European administrative law consists mainly of legal arrangements for management of information necessary in administrative proceedings[26]. Such arrangements may include rules on information gathering, storage and retention of information, corrections and deletion of information, intra- and inter-administrative information exchange, intra- and inter-administrative evaluation of data, and access by citizens and other private parties to administrative information during procedures or in accordance with general transparency policies and administrative publication of administration[27]. The most relevant rules in the composite European administration are related to the gathering and exchange of information, which Schneider in 2014 divided into four categories: mutual assistance, shared databases, duties to inform European authorities, and structured forms of information exchange upon request[28].

Since then, we have seen swift developments, not least through technical

advancements in interoperability in information sharing, and the ability to connect public and private information platforms, with associated legal challenges[29]. The category shared databases could be updated to include other types of data repositories, such as the distributed data pools as proposed in the EHDS, where data remain with public or private data holders until requested by authorized recipients[30]. Also on the technical and administrative side, the EU has furthered its activities by establishing an agency – eu-LISA, the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice – in charge of managing the Schengen Information System (SIS) and the Visa Information System (VIS), and developing the Entry/Exit System (EES), the European Travel Information Authorisation System (ETIAS), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)[31].

A fair amount of the data shared can be assumed to be personal data, and even privacy-sensitive data, in areas such as social security, taxation, crime prevention and control, migration, and security. Information exchange between jurisdictions with different administrative traditions on information management and the fluidity of data underlines the difficulties that may arise when data are used in connection to the exercise of public power in a composite context[32]. EU law has, following implementation of the 1995 Data Protection Directive, connected the protection of the privacy of a data subject to the free movement of personal data[33]. As stated in the preamble to both the Data Protection Directive and the GDPR, albeit with slightly differing wordings, the processing of personal data should be designed to serve mankind[34]. The enabling of economic and social progress and trade expansion has thus been connected to respect for fundamental rights and freedoms of natural persons, most notably the right to informational integrity. As held by Jan Philipp Albrecht, Member of the European Parliament and one of the architects behind the GDPR, the GDPR is meant to serve as a starting point for international standards and a trustworthy digital market[35].

In order to ensure this legal protection in practice, strong enforcement mechanisms were prioritized in the GDPR[36]. Elaborate schemes for composite administration existed before the GDPR, for example in the areas of pharmaceuticals, genetically modified organisms and chemical[37], but data protection differs in the sense that it is a truly horizontal regulatory regime,

involving both public and private actors in virtually all areas of society. The European Data Protection Board (EDPB) and the national data protection authorities cooperate in a composite structure, involving both guidance and standard-setting activities, as well as effective individual decision-making procedures with consistency and dispute resolution mechanisms[38]. Accordingly, even though the substantive data protection rules do not differ much between the Data Protection Directive and the GDPR, the cooperative approach to enforcement has brought about major changes. From being an area of law struggling with shortcomings in implementation and compliance, the GDPR is now one of the EU's flagship regulatory policies[39]. As will be discussed in the following section, the administrative infrastructure of the GDPR has set the standard for the further development of the «*single market for data*».

## 3.2. The European Strategy for Data and its regulatory framework for data and the market

After the adoption of the GDPR as a framework for digital trust, the focus of the EU legislator has turned more decisively to facilitating data economy and data sharing[40]. As discussed above, the aim of the European Strategy for Data is to «*unleash the potential of data*» for the benefit of relevant actors, so they can develop society in various ways[41].

The strategy builds on the FAIR data principle, *i.e.*, that data should be findable, accessible, interoperable, and re-usable[42]. Already before the European Strategy for Data was adopted in 2020, several legislative acts regulating access to data within the internal market had been enacted, such as the 2018 regulation on a framework for the free flow of non-personal data[43], the 2019 Open Data Directive, recasting the 2003 Public Service Information (PSI) Directive[44] and the 2019 Platform to Business Regulation[45].

In accordance with the strategy, three acts were enacted in 2022: the DGA, the Digital Markets Act (DMA)[46], and the Digital Services Act (DSA)[47].

Further proposals are currently being negotiated, including the Data Act[48] and the first out of nine planned sector-specific data spaces, the European Health Data Space. The proposal for an Artificial Intelligence Act can also be mentioned, as it has a clear connection to the trust in EU governance narrative,

though it is constructed as a market surveillance act, rather than an access to information act[49]. In this case, it is the service providers that are under obligation to provide large quantities of data to the composite European administration[50].
From a governance perspective, it may be noted that the aforementioned legislative acts and proposals include rules on tasks for single points of contact and competent authorities at the national level, and several also require the establishment of new EU agencies[51].
The acts describe rules on sanctions or penalties for failure to comply, either soft rules, such as those in the regulation on a framework for the free flow of non-personal data, which states that member states may enact effective, proportionate, and dissuasive penalties[52], or strong rules on administrative fines, such as those in the DSA and DMA, which mandate the national competent authorities and the Commission, respectively, to enact fines up to 6% or 10%, respectively, of annual worldwide turnover[53]. The two acts and the proposal chosen as the objects for this study, the Open Data Directive, the DGA, and the EHDS, will be presented in the following section.

## 4. Access to publicly held data in the European Strategy for Data

### 4.1. Facilitating access to publicly held data – PSI and the Open Data Directive

As the EU does not have any legislative competence to regulate access to documents within the member states, there is no common EU law regulating access to official documents for the EU and the member states. Thus, in contrast to what we see in the area of data protection, the composite European administration is governed under 28 separate transparency rules – those of the EU and the 27 member states[54]. As information sharing is a core trait of the composite administration, this has caused some difficulties and unclarities in relation to deciding on the law applicable to documents held in multiple jurisdictions, putting quite some pressure on transparency-friendly countries not to release documents that may be sensitive for others[55].
However, the already in the early 2000s, the EU began to enact legislation

designed to make data held by public institutions available to the public[56]. EU has enacted rules on how documents defined as public and legally accessible under national law can be made more accessible in practical, organizational, and economic terms. The aims of the 2004 PSI Directive were to make public information held by public sector bodies more accessible for re-use, and to create a level playing field for relevant actors by enabling sharing of data and information that are not under any legal constraints such as confidentiality or intellectual property. The Directive was revised in 2013, and recast in 2019, under a new name, the Open Data Directive. The directives do not contain any obligation to make documents available[57], but lay down minimum rules governing the re-use of existing documents held by public sector bodies and the practical arrangements for facilitating such re-use[58].

In accordance with the FAIR principle, and the principles on non-discrimination and fair competition, member states are to provide documents in formats that are open, machine-readable, accessible, findable, and re-usable, and in accordance with the principle of «*open by design and by default*»[59]. Documents should generally be available free of charge, but necessary and transparent charges for recovery of marginal costs may be allowed. There are also exceptions for public sector bodies generating revenue, such as libraries and archives[60]. Conditions for the re-use of documents are to be non-discriminatory for comparable categories of re-use, and exclusive arrangements for access are only permissible under certain circumstances[61].

In the Open Data Directive, some new categories of data have been included: documents produced in the performance of services in the general interest by public undertakings, research organizations, and research-funding organizations[62]. Further, a new concept, «*high-value datasets*» is defined, where more access-friendly rules apply[63]. The thematic categories of high-value datasets are: geospatial, earth observation and environment, meteorological, statistics, companies and company ownership, and mobility[64].

## 4.2. Facilitating access to protected data – the Data Governance Act

In a subsequent step to the recasting of the PSI, the DGA was enacted. Like the

Open Data Directive, the DGA does not place any obligations on the member states to make documents, information, and data available. However, it does aim to facilitate access to documents under legal constraints[65]. Public sector bodies are to grant access to protected data defined in Article 3, namely data covered by either commercial or statistical confidentiality, intellectual property, or data protection, under non-discriminatory, transparent, proportionate, and objectively justified conditions set out in Article 5 of the Act. Primarily, the public sector bodies are to ensure that confidential information is not disclosed as a result of re-use, Article 5.8. The DGA thus contains measures to work around legal constraints by ensuring alternative protection. These consist of, among other things, establishing competent authorities that can assist public sector bodies in implementing technical requirements, anonymization, and pseudonymization[66], requiring public sector bodies to assist potential re-users in seeking consent from data subjects or permission from data holders[67], and establishing a single information point to help potential re-users find relevant information[68]. These authorities may also be empowered to grant access for the re-use of data, on behalf of the public sector body holding the data[69]. There are also rules on fees and exclusive arrangements[70].

The DGA includes some minimum requirements on the procedure of requesting data for re-use. A public sector body or the competent bodies, as the case may be, is to make a decision on a request for data for re-use within two months, with a possibility of extension in exceptional cases[71]. All persons directly affected by a decision may further have an effective right of redress before an impartial body with the appropriate expertise, such as the national competition authority, the relevant access-to-documents authority, or the national data protection authority under the GDPR[72].

Two new legal concepts are introduced, which are intended to contribute to ensuring protection without legal constraints hindering re-use: data intermediation services and data altruism. The DGA defines data intermediation services as a new concept, «*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*»[73]. These are private organizations that can be appointed roles in the secure handling of data, following a notification

process[74].

Data altruism entails voluntary sharing of data for the benefit of society, including purposes such as healthcare, combating climate change, improving mobility, facilitating development, etc[75]. The main tool of the DGA in this regard is to regulate the role of data altruism organizations, namely «*legal persons that seek to support objectives of general interest by making available relevant data based on data altruism at scale and that meet the requirements laid down in this Regulation*»[76]. The DGA thus introduces a generic registration scheme for data altruism organizations, containing transparency obligations and specific requirements to safeguard the rights and interests of data subjects as well as a legal basis for a standardized data altruism consent form from the European Commission[77]. Both notified data intermediation services providers and registered data altruism organizations may, under the DGA, use official labels identifying their roles, including a common logo[78].

The DGA further entails a requirement for member states to appoint competent authorities for data intermediation services and for the registration of data altruism organizations.

The competent authorities are suggested to be tasked with monitoring and supervising the compliance of data intermediation services providers and data altruism organizations, respectively[79]. Like the data protection authorities under the GDPR, the competent authorities for data intermediation services are empowered to impose sanctions in case of infringements, including «*dissuasive financial penalties*» and suspension or cessation of data intermediation services[80]. For its part, the competent authority for data altruism organizations can only enact softer measures, such as requiring that a data altruism organization ceases with its infringement, at the risk of losing the right to use the label «*data altruism organization recognized in the Union*»[81].

## 4.3. Obligations to give access to protected data – the EHDS proposal

As seen above, the European Strategy for Data foresees the establishment of nine sectoral data spaces in different strategic fields, with the EHDS being the first to enter the legislative process[82]. As with the Open Data Directive and the DGA,

the main aim of the EHDS proposal is to make data accessible, but there are three important differences. First, the EHDS contains rules only on electronic health data, though they cover data from both public and private entities, as well as rules directed at manufacturers and suppliers of electronic health records systems and wellness apps[83]. Further, access is only to be provided for purposes in the general interest, which are listed in the form of eight categories in Article 34 of the proposed regulation[84]. Second, the EHDS includes rules on both primary and secondary use of data, that is, not merely re-use of data, and on use of data for the benefit of the data subject or patient him- or herself. The rules on primary use of data are a continuation of the legislative initiatives in the Directive regarding the application of patients' rights in cross-border healthcare, where a voluntary eHealth Network was introduced – an EU-wide electronic platform for e-prescriptions and patient summaries[85]. As implementation of the voluntary network has been slow, the EHDS provides for a compulsory scheme, ensuring legal, semantic, and technical interoperability of health data[86]. This will indubitably also facilitate secondary use of the data. Third, and mostly relevant for the purposes of this paper, the EHDS proposal requires that protected data are to be transferred under the conditions described below. However, it must be underlined that only data in anonymized or pseudonymized forms can be accessed under the EHDS[87].

The EDHS sets up a scheme with defined roles and responsibilities for entities holding health data (data holders), actors requesting health data (data users), as well as a supervisory body (the health data access body) in each member state. The definition of data holders in Article 2.1.y of the proposed EHDS Regulation is wide and includes entities or bodies in the health and care sector, research institutes, EU institutions, and bodies with the right or legal obligation to make data available [88]. Micro-enterprises are excluded, due to the administrative burden[89]. The data holders are obligated to provide electronic health data in the fifteen categories listed in Article 33.1 of the proposed EHDS Regulation, including electronic health records, data impacting on health, including social, environmental behavioral determinants of health, health-related administrative, data including claims and reimbursement data, public health registries, and electronic health data from medical devices, such as running apps and other health apps. As mentioned above, the proposal defines eight permissible purposes

for which electronic health data can be processed for secondary use[90], and five prohibited ones[91].

The data user is defined as «*a natural or legal person who has lawful access to personal or non-personal electronic health data for secondary use*»[92]. Electronic health data can be accessed in two ways, via a data access application or a data request – the latter being a simplified version containing only an anonymized statistical format, with no access to the underlying electronic health data. Both data applications and data requests can be submitted to a health data access body, but a data request, *i.e.*, the simplified version of access, may also be submitted directly to a data holder, if the data sought are confined to a single data holder and a single Member State[93].

If a data access application is approved, a data permit is issued by the health data access body[94]. Health data access bodies are to give access to electronic health data without requiring a data permit in cases where public sector bodies and Union institutions, bodies, offices, and agencies seek data for the purpose of «*carrying out the tasks enshrined in their mandate, based on national or Union law*»[95].

Any natural or legal person can apply for access to data – no connection to the EU is needed[96]. The application should include, among other things, a detailed explanation of the intended use of the electronic health data, the type of data requested, and whether the data are requested in anonymized or pseudonymized form, where requests for the latter form should be accompanied by an explanation[97]. A description of the safeguards planned to prevent any other use of the electronic health data and to protect the rights and interests of the data holder and of the natural persons concerned should also be included[98].

Each member state is to establish (at least) one health data access body[99]. The main tasks of the health data access bodies are to assess applications for data permits from data users, as described above, and to decide on data permits, with general and specific conditions[100].

When a data user receives a permit, the data holders must put the electronic health data at the disposal of the health data access body within 2 months[101]. Here, it should be mentioned that the proposal also contains a rule putting pressure on the health data access body to act swiftly. Should the health access body fail to provide a decision within the established time limit, a permit is to be

issued[102]. The health data access bodies are to be joint controllers together with the data users, and must therefore continually monitor the processing conducted by the data users[103].

Natural persons affected by the data permit, either as data subjects or businesses whose protected data are encompassed by a permit, are not considered parties to the decision-making procedure. In Article 38.1, the obligations of health data access bodies towards natural persons are listed. These consists of providing general information concerning relevant legal bases for processing, technical and organizational safeguards, and the applicable rights in relation to secondary use. In Article 38.2, it is clarified that the bodies are exempted from providing more detailed information in accordance with Article 14 GDPR.

The health data access boards will also have some sanctioning tools at their disposal, which can be directed towards both data holders and data users. Data holders that do not respect the deadlines set out in Article 41 can be fined for each day of delay[104]. In case of repeated breaches, a data holder may be banned from participation in the EHDS for a period of up to 5 years[105]. The proposal does not include any right to judicial review or other forms of remedy, in case a data holder finds transfer of the data upon request to be contrary to its legal requirements regarding confidentiality, data protection, etc. Article 43.9 of the proposed EHDS Regulation holds that «*any natural or legal person affected by a decision of a health data access body shall have the right to an effective judicial remedy against such decision*». However, the article deals only with penalties[106].

Data users that do not comply with the regulation and with their data permit may have the permit revoked and can be banned from any access to electronic health data for a period of up to 5 years[107]. Data users that try to re-identify pseudonymized data or do not respect measures taken to ensure pseudonymization are to be subject to appropriate penalties under national law[108].

At the EU level, a European Health Data Space Board (EHDS Board) is to be established to facilitate cooperation and exchange of information between member states[109]. Further, the EHDS Regulation also foresees a role for data altruism organizations, connecting it to the DGA[110].

## 5. The construction of «*clear and trustworthy data governance*» in the Open Data Directive, the DGA, and the EHDS proposal

### 5.1. Introductory remarks

As can be seen from the short presentations above, the three acts – the Open Data Directive, the DGA, and the EHDS proposal – represent a stepwise development towards a new and innovative model for facilitating access to publicly held data, and, in relation to electronic health data, an administrative law regime for accessing privately held data. The question raised here is how the ambition to create clear and trustworthy data governance has been realized. Are the competent public bodies at the national level (the public sector bodies under the Open Data Directive and the DGA, the competent authorities for data intermediation services and for the registration of data altruism organizations under the DGA, the health data access bodies under the EHDS, and the European Data Innovation Board and the EHDS Board at the European level) equipped to realize these ambitions? As mentioned above, it is not entirely clear from the European Strategy for Data what is meant by «*clear and trustworthy governance mechanisms*». The focus here is on two aspects that are central from a legal perspective, in order to live up to ideals related to the rule of law. First, is there a clear understanding in the legislative framework of how rights of third parties are to be upheld, in particular data protection for data subjects whose personal data are processed and protection of intellectual property rights and business secrets for businesses whose data are processed? Secondly, are there mechanisms available for administrative and judicial protection? The first question overlaps with the second pillar of the European Strategy for Data: to ensure European rules and values in personal data protection, consumer protection, and competition. Here, the main question concerns the conditions to ensure foreseeability, coherency, and protection of rights, as rules for defining what organ, in what jurisdiction, is competent to handle (seemingly) contradictory law and balance competing rights within an administrative or judicial frame, rather than the substantive issues connected to the rights and

values.

## 5.2. Conditions for balancing free movement and third-party rights in a fragmented legal landscape

As seen above, the European Strategy for Data aims to create a regulatory framework for the digital economy which can satisfy global competition and protect European rules and values on data protection, consumer rights, and competition. The GDPR constitutes a cornerstone, functioning as a framework for digital trust. The Open Data Directive, the DGA, and the EHDS proposal are thus pieces of a bigger legal puzzle within the European Strategy for Data. In relation to the first question, regarding conditions for protecting third-party rights, it is noteworthy that third-party right holders (data subjects, intellectual property owners, businesses with trade secrets) do not have an independent role in the legal frameworks and no express rules are included on how their rights and interests are to be protected.[111] The main task of the competent authorities under the respective legal frameworks is clearly to facilitate access to public (and, in the case of the EHDS, also private) data, whereas the protection of rights of third parties mainly follows from other legal sources: the GDPR in relation to data protection and mostly national law for intellectual property and confidentiality. All public authorities acting within the sphere of application of EU law must furthermore respect the fundamental rights of individuals, including data protection and the right to conduct businesses, enshrined in Articles 8 and 16 of the EU Charter of Fundamental Rights[112]. For the health data access bodies, their position as joint controllers together with data users creates a specific responsibility to ensure that the rights of the data subject are respected[113].

For the competent authorities under the DGA and the proposed EHDS, which oversee access to data under legal constraints, the conditions for balancing the objective of free movement of data with the protection of rights of third parties are complex. One specific challenge consists of balancing the clearly stated aim to give access to data against the patchwork legislative framework for protection of rights. The GDPR is a common legal framework for all member states. However, in many relevant aspects, the GDPR does not specify the legal requirements for

the processing of personal data in any particular context, simply requiring that safeguards are in place, be they legal, technical, or organizational.[114] When combined with the importance attributed to the principle of proportionality in balancing the interest of protection of the rights of the data subject against the interest of access to information and free movement of data[115], this means that the level of protection is context-dependent[116]. Furthermore, many different types of data are involved, for which national traditions differ. The health data access bodies will face an especially challenging task in assessing the applications for data permits, not least as regards the applicants' descriptions of the safeguards planned to prevent any unauthorized use of electronic health data and to protect the rights and interests of the data holder and the natural persons concerned[117]. Even though the national rules vary, one thing that the applicable national legislations seem to have in common is that re-use of health data is closely regulated[118].

In this context, it may also be conceded that the substantive EU law for the digital market is not always consistent. Lundqvist describes the discrepancies as being so manifest that the EU policy could be said to be at war with itself[119]. All in all, this is a complex legal landscape for the competent authorities to handle. Accordingly, the failure to act-procedure in the EHDS – entailing that a data permit will be issued automatically if the health data access board does not make a decision within the time limits – does not seem to be an appropriate tool to ensure foreseeability and protection of rights[120].

The competent authorities in both the DGA and the EHDS are further to be assisted by two new legal entities in a public law context: data intermediation services and data altruism organizations. At this stage, it remains a bit unclear if the roles and functions of these private actors will have any implications for the public law tasks and responsibilities of the public actors. One version of data altruism is well-known in the bioethical domain, where the concept of data stewardship is understood as an ethical standard for data processors[121].

In the European Strategy for Data, the data altruism organizations have a legally defined position, under supervision of public authorities. However, neither the DGA nor the proposed EHDS defines what role the data altruism organizations are meant to have in the actual handling of the data. In legal doctrine, Kruesz and Zopf have suggested that they will typically operate as controllers or joint

controllers, as they will likely determine the purposes and means of the processing of personal data, and thus will often have to take full responsibility for GDPR compliance[122]. In relation to the EHDS proposal, this would imply triple controllers: the data holder, the health data access board and, where applicable, a data altruism organization[123]. This seems excessive.

## 5.3. Administrative and judicial protection in the European composite administration for data

If the Open Data Directive, the DGA and the EHDS Proposal constitutes pieces of a bigger legal puzzle, it could be deemed unproblematic that the individual legislative acts do not include tools to ensure good administration and effective legal remedies for third parties. Such protection may well be ensured via other routes.

The question is rather how this bigger puzzle for implementation and enforcement of EU law is constructed. As discussed above, the European composite administration consists of private actors and public entities in the form of European and national authorities, collaborating closely on the implementation of EU law and policies. Due to the lack of legislative competence of the EU in the area, as well as the doctrine of institutional and procedural autonomy, each public entity remains embedded in its respective constitutional and administrative order. The composite administration will thus often be bound by common rules only at a minimum level, whereas the main route to good administration and effective legal remedies goes via national law[124]. The jurisdictional limitations of national authorities remain and, accordingly, the EHDS proposal includes conflict of law tools as mutual recognition for cross-border access to electronic heath data for secondary use[125].

As the European Strategy for Data is an illustrative example of, the trend towards administrative cooperation across jurisdictions is strong, as is the ambition to move forward. In a communication on the EHDS proposal, the Commission identifies the administrative unclarities as an obstacle[126]:

«*Fragmented and divergent legal and administrative rules, frameworks, processes, standards and infrastructure for reusing health data restrict researchers and innovators' access to health data. They also limit the availability of innovative*

*health products and service*».

Against this background, it would have been expected that greater efforts had been made to lay down minimum administrative and judicial procedures in the legislative acts under the European Strategy for Data, which could be consistently implemented in each act.

Looking at the three legislative acts in focus here, especially the DGA and the EHDS proposal, the construction of the legal protection for those involved in the procedure of accessing data remain uncordinated. The EHDS proposal does not provide any redress mechanism for either the data holders, the data users, or a concerned third party, in relating to decisions to either grant or deny a request for access to electronic health data[127]. A data holder that finds a data permit for access to its data to be contrary to its legal obligations, for example under the GDPR, could find itself in a particularly precarious situation. Only in the case where the health data access board adopts a decision on penalties, such as a daily fine for delays in making the data available to the data user, does the proposed EHDS Regulation guarantee a right to an effective judicial remedy[128]. Whether such judicial proceedings also include a review of the legality of the underlying decision to issue a data permit for data is a matter for national law, taking into account the EU principles of right to an effective remedy[129]. The data holder could find itself in a position of having to choose between adherence to the GDPR or the EHDS. The DGA, on the other hand, at least provides an effective right of redress before an administrative authority to all persons directly affected by a decision on re-use[130].

Despite the aim to create clear and trustworthy data governance mechanisms, it may be submitted that the legislative framework still entails a lack of clarity on how competing rights are to be balanced in a multi-jurisdictional setting and the lack of clear and consistent mechanism for administrative and judicial protection for natural and legal persons concerned. On the other hand, the Open Data Directive, the DGA, and the EHDS proposal include multiple mechanisms for informal and soft cooperation for the authorities involved. Competent authorities within the different sector-specific data fields are to cooperate and learn from each other, share information, and engage in capacity building (not merely from a technical point of view)[131]. Such informal cooperative implementing mechanisms are standard procedure in the European composite

administration[132]. The focus is to foster a culture of openness and accessibility, which in itself could be seen as commendable. However, when it comes to resolving the hard cases, are there clear and accessible mechanisms for the delicate constitutional task of balancing free movement of data and the rights of affected third parties?

## 6. The European Strategy for Data and Trust

Does the EU governance for data deserve trust? The question could perhaps be partially answered with a counter-question: is there really a comprehensive EU governance structure for data? If we are to look at the question from a legal perspective and define a trustworthy governance structure as an organization with the ability to uphold the rule of law, as in foreseeability, consistency, and protection of rights, it seems that there is still room for improvement. Looked upon as an entity, an administrative organization in its own right, it is questionable if the multifaceted and uncoordinated European composite administration can live up to such ideals. As held by Mendes, from a general EU administrative law perspective, there is only weak integration of constitutional concerns regarding framing and taming the exercise of public authority, on the one hand, and the institutional practices of collaboration and diffusion of public authority in the EU administrative sphere, on the other[133].

The Commission stated in its European Strategy for Data 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*»[134].

With the perspective taken here, this analysis seems to open for a stronger convergence also in law. There are a few, small signs that such a development might be on the way. Going beyond capacity-building for technical development, as in the case of eu-LISA, the Commission in 2021 established an expert group on public administration and governance, which is to advise the Commission on issues related to public administration transformation and reforms.[135] A more concrete sign is the newly presented proposal for common procedural rules for the enforcement of the GDPR[136]. Could these examples perhaps be interpreted as first steps towards laying down common rules and

procedures for a clearer and more trustworthy governance for the composite administration? This would entail something of a paradigm shift, from the EU constitutional concept of mutual trust – where member states trust each other – to a trust in the composite EU information governance system as a separate entity[137]. The matter is sensitive[138]. Administrative law is the tool for the nation state to communicate with natural and legal persons within its jurisdiction, and the handing over of such a tool to an entity outside the state could be viewed as a palpable loss of national sovereignty. The acknowledgement of an indirect EU competence to regulate national administrative law in the sphere of application of EU law would change the EU's nature, giving it federal traits[139].

Data may be the new gold in the data economy, but it must be acknowledged that data are highly valuable assets also from a public law perspective. Data are a core asset in public governance and whoever has power over the data will also have power to influence core public tasks[140]. How publicly held data is used and re-used matters. When the European Strategy for Data has been realized, and eight more sectoral data spaces are up and running, an important shift of power over both public and private data can be foreseen – from the member states to a strong, but uncoordinated European composite administration. Now might be the time to take the ideal of clear and trustworthy governance for data more seriously.

1. A first draft of this article was presented at the Administrative Law Discussion Forum in Paris, France, 12-13 June 2023, organized by Professor Russell L. Weaver, University of Louisville, USA and Duncan Fairgrieve, Université Paris Dauphine-PSL, France. I would like to thank the participants of the Forum for valuable input.
2. For example, Article 3.1(a) Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030; Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe*, COM(2018) 237 final, p. 12; recital 3 of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).
3. A. Bradford, *The Brussels Effect – How the European Union Rules the World*, Oxford University Press, 2020, p. xiv.
4. H.C.H. Hofmann and A. Türk, '*The Development of Integrated Administration in the EU and its Consequences*', European Law Journal, Vol. 13, 2, 2007, pp. 253–271.

5. Communication from the Commission to the European Parliament and the Council, the European Economic and Social Committee and the Committee of the Regions, *A European strategy for data*, COM(2020) 66 final, p. 4.
6. See Commission website, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en, accessed on August 28, 2023.
7. A European strategy for data, op. cite n 4, p. 5.
8. Compare H.D. Kristjánsson, *The Governing Idea of the Rule of Law*, in J. Reichel and M. Zamboni (Eds), *Rule of Law 69 Scandinavian Studies in Law*, Vol. 69, 2023, p. 14 *et seq*.
9. 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 (hereinafter, Open Data Act).
10. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act) (hereinafter, DGA).
11. Commission Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM/2022/197 final (hereinafter, EHDS proposal).
12. In Article 13.1, relating to a «*high level of trust and security*» in services provided via MyHealth@EU.
13. Recital 7 in the preamble 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 (General Data Protection Regulation) (hereinafter GDPR).
14. Recital 3, 5, 23, 24, 32, 33, 38, 43, 46, 47 and 52 of the preamble to the DGA. The preamble of the EHDS proposal refers to trust twice, recitals 37 and 61.
15. H Wenander, *A Toolbox for Administrative Law Cooperation Beyond the State*, in A-S Lind and J. Reichel (Eds), *Administrative Law Beyond the State – a Nordic Perspective*, Liber Martinus Nijhoff Publishers 2013, p. 60 *et seq*.; C. Lebeck, *Konstitutionella gränser för ömsedidigt erkännande i EU-rätten: med särskild hänsyn till straffrättssamabetet*, jure, 2022, p. 72 *et seq*.
16. Compare case 120/78 *Rewe-Zentral v. Bundesmonopolverwaltung*, EU:C:1979:42, para 5.
17. Case 33/76 Rewe-Zentralfinanz eG et Rewe-Zentral AG v. Landwirtschaftskammer für das Saarland, EU:C:1976:18, para 5. Compare case 45/76 Comet BV v. Produktschap voor Siergewassen, EU:C:1976:191, para 13.
18. Compare Article 82 *et seq*., 74, 76 Treaty on the Functioning of the European Union (TFEU) in regards to criminal law, and Article 197 TFEU on administrative cooperation.
19. Case C-399/11, Melloni, EU:C:2013:107, para 63; case C-216/18 PPU LM, EU:C:2018:586, para 36; C. Rizcallah, *The Challenges to Trust-Based Governance in the European Union: Assessing the Use of Mutual Trust as a Driver of EU Integration*, EUR. L.J. 25, 2019, pp. 37-56, 54.
20. See for example O. Sallavaci, *Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange*, Eur J Crim Policy Res 24, 2018, pp. 219–235

https://doi.org/10.1007/s10610-017-9355-0; B. Parusel, *Should They Stay or Should They Go? Frontex's fundamental rights dilemma*, Sieps 2022:22epa.

21. Case 68/88 Commission of the European Communities v. Hellenic Republic, EU:C:1989:339, para 24.
22. Case C-340/89 Vlassopoulou v. Ministerium für Justiz, Bundes-und Europaangelegenheiten Baden-Württemberg, EU:C:1991:193, para 16–18.
23. See generally, F. Britos Bastos, *An Administrative Crack in the EU's Rule of Law*, *E*uropean Constitutional Law Review, 16:63–90, 2020; J Reichel, *Ensuring the Principle of Good Administration in EU Financial Markets Law*, in C.B. Bergström and M. Strand (eds), *Legal Accountability in EU Markets for Financial Instruments*, Oxford University Press 2021, pp. 126-157.
24. Bradford, *The Brussels Effect*, op. cite note 2, p. 16.
25. H. Wenander, *A network of social security bodies – European administrative cooperation under Regulation (EC) No 883/2004*, *REALaw* 2103, Vol. 6, 1, pp. 39–71, 47.
26. D.-U. Galetta, H.G.H Hofmann and J.-P. Schneider, *Information Exchange in the European Administrative Union: An Introduction*, *European Public Law* 20, 1, 2014, pp. 65–70, 66 *et seq*.
27. J.-P. Schneider, *Basic Structures of Information Management in the European Administrative Union, European Public Law* 20, 1, 2014, p. 90.
28. Ibid., 91.
29. D. Curtin and F. Brito Bastos, *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue*, *European Public Law*, Vol. 26, pp. 59–70, 65.
30. See section 4.3 below.
31. See eu-LISA's web page, https://www.eulisa.europa.eu/About-Us/Who-We-Are; Curtin and Brito Bastos, *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance*, op. cite, 27, p. 63.
32. D. Curtin, *Interstitial Data Secrecy in Europe's Security Assemblages*, in A.-S. Lind, J. Reichel, and I. Österdahl (Eds), *Transparency in the Future: Swedish,* Openness 250 Years, Ragulka 2017, p. 91.
33. This follows already from the titles of the two central acts, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 and 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 [2016] OJ L119/1.
34. Recital 4 in the preamble to the GDPR; Recital 2 in the preamble to the Data Protection Directive.
35. J.-P. Albrecht, *How the GDPR Will Change the World*, Eur Data Prot L.Rev 2 2016, 287, p. 289. Compare the role of trustworthy legal frameworks discussed above, and recital 7 in the preamble to the GDPR.
36. H. Hijmans, *The European Union as a Guardian of Internet Privacy*. *The Story of Art 16*

*TEU*, Springer, 2016, pp. 516–17.

37. S. Alonso de León, *Composite Administrative Procedures of the European*, Universidad Carlos III de Madrid, 2017, pp. 221 *et seq.*, 226 *et seq*., 237, *et seq.*
38. Articles 70, 55–70 GDPR; H Hijmans, The DPAs and Their Cooperation: *How Far Are We in Making Enforcement of Data Protection Law More European*, Eur. Data Prot. L. Rev. 2, 2016, pp. 362, 367, 369 *et seq*., A. Giurgiu and T. A. Larsen, *Roles and Powers of National Data Protection Authorities*, 2 Eur. Data Prot. L. Rev. 2, 2016, pp. 342, 349.
39. Bradford, *The Brussels Effect*, op. cite not 2, 7, pp. 132 *et seq*.
40. J. Ruohonen and S. Mickelsson, *Reflections on the Data Governance Act*, *Digital Society* 2:10, 2023, pp. 1–9, 1. See also B. Lundqvist, *Regulating Access and Transfer of Data*, Cambridge University Press, 2023, p. 98 *et seq*.
41. A European strategy for data, op. cite 4, p. 26. See also Communication from the Commission to the European Parliament and the Council, *A European Health Data Space: harnessing the power of health data for people, patients and innovation,* COM(2022) 196 final, pp. 2, 3, 8, 13, and 18.
42. A European strategy for data, op. cite n 4, p. 12.
43. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.
44. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. The directive was further revised through Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013.
45. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
46. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act).
47. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).
48. Commission *Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)* COM(2022)68 final.
49. Commission *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final.
50. J. Chamberlain and J: Reichel, *Supervision of Artificial Intelligence in the EU and the Protection of Privacy*, *FIU Law* 2023, 2, vol. 17, pp. 263–281, 277.
51. The European Data Innovation Board is established in Article 29 DGA, the European Board for Digital Services in Article 61 DSA, a European Artificial Intelligence Board in Article 56 of the proposed AI Act and a European Health Data Space Board in Article 64.1 proposed EHDS Regulation.

52. Article 5.4 Regulation on a framework for the free flow of non-personal data.
53. Article 52.3 DSA and Article 30.1 DMA.
54. T. Streinz, *The Evolution of European Data Law, in The Evolution of EU Law*, in P. Craig and G. de Búrca (Eds), *The Evolution of EU Law*, Oxford University Press, 2021, p. 919.
55. J. Reichel, *Public Access or Data Protection as a Guiding Principle in the EU's Composite Administration? An Analysis of the ReNEUAL Model Code in the Light of Swedish and European Case Law*, in P. Wahlgren (Ed), *50 years of Law and IT*, Scandinavian studies in Law, 65, 2018, pp. 285–308, 289 *et seq*, 303 *et seq*.
56. Streinz, *The Evolution of European Data Law*, op. cite 52, p. 919.
57. Recital 9 of the preamble to the 2003 PSI Directive; Recital 7 of the preamble to the 2013 PSI Directive and recital 26 of the preamble to the Open Data Directive.
58. Recital 4 in the preamble to the Open Data Directive.
59. Article 5.1–2 Open Data Directive.
60. Article. 6.1–2 and 7 Open Data Directive.
61. Articles 13–14 Open Data Directive.
62. Recital 10 of the preamble, Article 1.1 (b) and (c) Open Data Directive.
63. Articles 13–14 Open Data Directive.
64. Annex I to the Open Data Directive.
65. Article 1.1–2 DGA.
66. Article 7.1, 4 DGA.
67. Article 5.6 DGA.
68. Article 8 DGA.
69. Article 7.2 DGA.
70. Articles 4 and 6 DGA.
71. Article 9.1 DGA.
72. Article 9.2 DGA.
73. Article 2 (11) DGA.
74. Article 11 DGA.
75. Article 2 (16) DGA.
76. Recital 3 in the preamble to the DGA.
77. Articles 17–21 Data Governance Act; C. Kruesz and F. Zopf, *The Concept of Data Altruism of the Draft DGA and the GDPR: Inconsistencies and Why a Regulatory Sandbox Model May Facilitate Data Sharing in the EU*, *Eur Data Prot L Rev*, 2021, pp. 7, 569, 569.
78. Article 11.9 DGA.
79. Articles 14.1 and 24 DGA.
80. Article 14.4 DGA.
81. Article 24.4–5 DGA.
82. The other eight are: Common European industrial (manufacturing) data space, Common European Green Deal data space, Common European mobility data space, Common European financial data space, Common European energy data space, Common European

agricultural data space, Common European data spaces for public administrations, and Common European skills data space. There are also plans to develop a European Open Science Cloud, see Appendix to the Communication 'A European strategy for data', Common European data spaces in strategic sectors and domains of public interest, A European strategy for data, op. cite n 4, p. 26 *et seq*. See also EHDS proposal, p. 1.

83. Article 1.4 proposed EHDS Regulation.
84. See also recital 41 in the preamble to the proposed EHDS Regulation.
85. Article 14 Directive 2011/24/EU of the European Parliament and of the Council on the application of patients' rights in cross border healthcare.
86. EHDS proposal, p. 2.
87. Article 44.3 proposed EHDS Regulation. In relation to genetic data, it may be questioned whether they can be rendered entirely anonymous, recitals 34–35 of the preamble to GDPR.
88. According to Recital 40 in the preamble to the proposed EHDS Regulation, a wide group of entities are included, both public, non-for-profit and private health and care providers, public, non-for-profit and private organizations, associations and other entities, and public and private entities that carry out research with regard to the health sector.
89. Ibid. and Article 33(2) of the proposed EHDS Regulation.
90. Article 34.1 proposed EHDS Regulation list the following permitted purposes: «*(a) activities for reasons of public interest in the area of public and occupational health, such as protection against serious cross-border threats to health, public health surveillance or ensuring high levels of quality and safety of healthcare and of medicinal products or medical devices; (b) to support public sector bodies or Union institutions, agencies and bodies including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates; (c) to produce national, multi-national and Union level official statistics related to health or care sectors; (d) education or teaching activities in health or care sectors; (e) scientific research related to health or care sectors; (f) development and innovation activities for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices; (g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices; (h) providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons*».
91. Article 35 proposed EHDS Regulation prohibits the following purposes: «*(a) taking decisions detrimental to a natural person based on their electronic health data; in order to qualify as 'decisions', they must produce legal effects or similarly significantly affect those natural persons; (b) taking decisions in relation to a natural person or groups of natural persons to exclude them from the benefit of an insurance contract or to modify their contributions and insurance premiums; (c) advertising or marketing activities towards health professionals, organisations in health or natural persons; (d) providing access to, or*

*otherwise making available, the electronic health data to third parties not mentioned in the data permit; (e) developing products or services that may harm individuals and societies at large, including, but not limited to illicit drugs, alcoholic beverages, tobacco products, or goods or services which are designed or modified in such a way that they contravene public order or morality*».

92. Article 2.1.z proposed EHDS Regulation.
93. Articles 45, 47, and 49 proposed EHDS Regulation.
94. Article 46 proposed EHDS Regulation.
95. Articles 37(1)(b) or (c) and 48 proposed EHDS Regulation.
96. Article 45.1 proposed EHDS Regulation. However, transfer to third countries may require use of specific protective measures, Article 61 proposed EHDS Regulation.
97. Article 45.2 a–d proposed EHDS Regulation.
98. Article 45.2 e–f proposed EHDS Regulation.
99. Article 36.1 proposed EHDS Regulation.
100. Article 46 proposed EHDS Regulation.
101. Article 41.4 proposed EHDS Regulation.
102. Article 46.3 proposed EHDS Regulation.
103. Article 51 proposed EHDS Regulation. The responsibilities of the controller are laid down in Article 24.1–2 GDPR: «*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller*». According to Article 66 proposed EHDS Regulation, the Commission is suggested to establish «*joint controllership groups*» for cross-border infrastructures of the type provided for in Articles 12 and 52.
104. Article 43.5 proposed EHDS Regulation.
105. Ibid.
106. See also Recital 48 of the preamble to the proposed EHDS Regulation.
107. Article 43.5 proposed EHDS Regulation.
108. Article 44.3 and Article 69 proposed EHDS Regulation.
109. Article 64.1 proposed EHDS Regulation.
110. Article 49 proposed EHDS Regulation.
111. Compare S. Slokenberga, *Scientific Research Regime 2.0? How the proposed EHDS Regulation may change the GDPR*, *Research Regime Technology and Regulation*, 2022, pp. 135–147, 141.
112. Article 51 of the EU Charter of Fundamental Rights; C-617/10 *Åkerberg Fransson,* EU:C:2013:105, para 19-21.
113. Article 51 proposed EHDS Regulation and section 4.3.

114. See for example Articles 6.4 (e), 9.2 (b), (d), (h), 10, 13.1(f), 14.1(f) and 5 (b), 15.2, 23.2 (d), (f), 25.1, 30.1 (e), (c), 35.7 (d), 36.3 (c).
115. Recital 4 in the preamble to the GDPR, Article 6.3 and 4 GDPR.
116. See for example C-439/19 *Latvijas Republikas Saeima*, EU:C:2021:1054, para. 122.
117. Article 45.2 e–f proposed EHDS Regulation.
118. See in regard to biobanking, O Tzortzatou, et al, *Biobanking Across Europe Post-GDPR: A Deliberately Fragmented* Landscape, in S. Slokenberga, O. Tzortzatou, J. Reichel (Eds), *GDPR and Biobanking - Individual Rights, Public Interest and Research Regulation across Europe*, Springer, 2021, pp. 397–419.
119. Lundqvist, Regulating Access and Transfer of Data, op. cite 38, pp. 118, 140, 239. See further Kruesz and Zopf, *The concept of Data Altruism of the Draft DGA and the GDPR*, op. cite 75, p. 571.
120. Article 46.3 proposed EHDS Regulation.
121. S. J. O'Brien, *Stewardship of Human Bio-Specimens, DNA, Genotype, and Clinical Data in the GWAS Era*, *Annu Rev Genomics Hum Genet* 10, 2009, pp. 193–209; Y. R. Rubinstein, et al. *The Case for Open Science: Rare Diseases*, *JAMIA Open*, 3(3), 2020, pp. 472–486; *Participatory Data Stewardship - A Framework for Involving People in the Use of Data, Report from the Ada Lovelace Institute Chief Executive, The British Academy,* 2021.
122. Kruesz and Zopf, *The concept of Data Altruism of the Draft DGA and the GDPR*, op. cite 75, p. 574.
123. Article 51 proposed EHDS Regulation and section 4.3.
124. A. de León, S. (2017) *Composite Administrative Procedures of the European Union*, Universidad Carlos III de Madrid.
125. Article 54 Proposed EHDS Regulation.
126. A European Health Data Space: harnessing the power of health data for people, patients and innovation, op. cite n 38, 1.
127. According to Article 46.5 proposed EHDS Regulation, the health data access body must provide a justification to the applicant when refusing to issue a data permit, but no redress mechanism is provided.
128. Article 43(3), (9) proposed EHDS Regulation.
129. Article 47 EU Charter of Fundamental Rights.
130. Article 9.2 DGA.
131. Article 9.2 Open Data Directive, Article 13(3), 14(7), 23(3), 24(6), 30 (i),(j) DGA, Article 37.2 d, 59, 65 proposed EHDS Regulation.
132. N. Xanthoulis, *Administrative factual conduct: Legal effects and judicial control in EU law*, *REALaw* 12(1), 2019, pp. 39-73, 39.
133. J. Mendes, *The EU Administrative Institutions, Their Law and Legal Scholarship*, in P. Cane, H.G.H. Hofmann, E. Ip and P. Lindseth (Eds), *The Oxford Handbook of Comparative Administrative Law*, Oxford University Press, 2020, p. 542.
134. A European strategy for data, op. cite n 4, p. 1.
135. Commission decision of 17.12.2021 setting up the group of experts on public

administration and governance, C(2021) 9535 final.

136. Commission Proposal for a Regulation of the European Parliament and of the Council *laying down additional procedural rules relating to the enforcement of Regulation* (EU) 2016/679, COM/2023/348 final.
137. Curtin and Brito Bastos, *Interoperable Information Sharing and the Five Novel Frontiers of EU Governance*, op. cite n 27, p. 65.
138. M Ruffert, *An Administrative Constitution for the EU?,* in G. Della Cananea and M. Conticelli (eds), *Rule of Law and Administrative Due Process in Europe. Trends and Challenge*s, Editoriale Scientifica, 2020, p. 91; R. Arnold, *The Relation between Constitution and Global Administrative Law – Some Reflection*s, in M Grahn-Farley, J. Reichel and M. Zamboni (Eds), *Governing with Public Agencies: The Development of a Global Administrative Space and the Creation of a New Role for Public Agencies,* Poseidon förlag, 2022, p. 112.
139. M. Heintzen, *Codification of Administrative Law in Germany and the European Union*, in F. Uhlmann (Ed), *Codification of Administrative Law. A Comparative Study on the Sources of Administrative Law*, Bloomsbury Publishing, 2023, p. 169 *et seq*.
140. J. Reichel and J. Chamberlain*, Public Registries as Tools for Realising the Swedish Welfare State – Can the State still Be Trusted?*, *Public Governance, Administration and Finances Law Review*, Vol. 6, 2, 2021, pp. 35–52, 42 *et seq*.; L. Marelli et al*, The European Health Data Space: Too Big to Succeed?,* Health Policy*,* 135, 104861, 2023*,* p. 3.