The European Health Data Space

Examining A New Era in Data Protection

Edited by Santa Slokenberga, Katharina Ó Cathaoir and Mahsa Shabani

First published 2025

ISBN: 978-1-032-82288-4 (hbk)
ISBN: 978-1-032-89684-7 (pbk)
ISBN: 978-1-003-54411-1 (ebk)

Chapter 10

Administrative tools for balancing societal and individual interests

Data protection safeguards and administrative procedural guarantees in secondary use in the European Health Data Space

Jane Reichel

DOI: 10.4324/9781003544111-13

The funder of the Open Access version of this chapter is Justitierådet Edvard Cassels stiftelse, Stockholm

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

10 Administrative tools for balancing societal and individual interests

Data protection safeguards and administrative procedural guarantees in secondary use in the European Health Data Space

Jane Reichel

10.1 Introduction

In its EU Strategy for Data, the Commission draws up a vision of a European space for free movement of data, where the General Data Protection Regulation (GDPR)[1] serves as a solid framework for digital trust.[2] The European Health Data Space (EHDS) is the first sectoral data space, with the aim of 'unleashing the data' in order to pursue important societal benefits.[3] An obstacle to this aim is the administrative governance systems for health data in the member states. According to the Commission, the differences in the implementation of the GDPR between the member states have resulted in 'fragmented and divergent legal and administrative rules, frameworks, processes, standards and infrastructure for reusing health data'.[4] One aim of the EHDS is therefore to create a legal framework consisting of trusted governance mechanisms within the EU and the member states.[5] The EHDS is thus to provide harmonised and tailored legal and technical solutions for accessing electronic health data for secondary use, taking into account the GDPR categorisation of health data as a special category of data in need of extra layers of safeguards in order to protect individual rights.[6]

The idea of using health data as an asset for society is not new. Health data stored in archives, registries and data pools have long been important assets for building the modern welfare state and improving public health, social infrastructures and health care.[7] In order to protect the individual whose data is stored in the archives, registries and data pools, specific safeguards are introduced to balance the societal interest against the interest of the individuals. This chapter analyses the efficiency of the governance structure for access of data for secondary use in the EHDS regulation[8] from the perspective of protecting rights and interests of the individuals concerned via two sets of administrative tools to balance these competing interests.

The first set of tools consists of sector-specific requirements for legal, technical and organisational safeguards to protect the right to informational privacy under Article 8 of the European Convention on Human Rights, and more specifically

DOI: 10.4324/9781003544111-13

data protection under Article 8 of the EU Charter of Fundamental Rights (the Charter) and the GDPR. These safeguards may consist of technical mechanisms to ensure data minimisation, such as anonymisation or pseudonymisation, or legal mechanisms, such as requirements of approvals or licenses, purpose limitations, secrecy and confidentiality. The aim is accordingly to allow for the processing of health data while minimising the risk of breaches of privacy for the natural persons concerned, i.e., the data subjects, when personal data are processed. The focus will be on the role and function of the safeguards in the assessment of applications for access to electronic health data for secondary use.

The second category consists of general administrative guarantees for protecting individual interests in the handling of their matters before a public administration, i.e., the right to good administration under the general principle of good administration that has also found expression in Article 41 of the Charter. The right to good administration includes a general right to have one's affairs handled impartially, fairly and within a reasonable time, corresponding to the public authorities' duty to care, and the right to be heard, the right of access to files and the right to a reasoned decision. These procedural rights aim to ensure that the interests of the individuals concerned are being handled correctly and to allow individuals to be involved in and have insight into the handling of their matters. In connection with this, the relevant interests can be identified first and foremost as data protection, but also as intellectual property (IP) and trade secrets.[9] Natural and legal persons concerned in a legally relevant manner should for example be able to ensure that all relevant aspects are included in the assessment, and be given opportunities to present their views on a matter before a decision is made. If not, they should be able to initiate a review of the decision before a court, Article 47 of the Charter.

The administrative balancing tools are to be used by the health data access bodies (HDABs) when assessing applications for access to electronic health data. The role and function of these bodies are thus also relevant in an analysis of the context in which the balancing tools are to be applied, as are the relations between the national bodies, the EHDS Board and the Commission. The main question raised in this chapter is the following: has the EHDS managed to define administrative balancing tools for the fragmented legal landscape of secondary use of health data in the EU and its member states, which can overcome the legal uncertainties regarding secondary use of electronic health data and barriers thereto?

The chapter is organised as follows. Section 10.2 deals with the implementation of the basic division of competence of regulating administrative safeguards and guarantees in EU and national law, as well as the general safeguards and procedures related to these matters in the EHDS. Section 10.3 includes an in-depth evaluation of the allocation of regulatory powers for legal safeguards and guarantees for handling individual applications in the EHDS, whereas Section 10.4 discusses the different roles and functions of the HDABs. Section 10.5 includes a summary of the findings in the chapter, including conclusions.

10.2 General administrative safeguards and guarantees in EU law and the EHDS

10.2.1 Points of departure for regulating data protection safeguards and administrative guarantees

According to the doctrine of institutional and procedural autonomy, it is up to the member states to appoint public authorities competent to manage specific policy areas under EU law, and – in the absence of EU regulation – to decide what procedures public authorities and courts are to apply, on the condition that they are effective and applied equivalently.[10] The locution 'in the absence of EU law' includes all relevant EU legal sources, i.e., primary and secondary law and general principles of EU law.[11] The EU does not have any independent legislative competence to regulate the internal administrative organisation or procedures of the member states but may merely support, coordinate or supplement the actions of the member states in the area of administrative cooperation.[12] However, institutional and procedural rules are regularly enacted on a sector-specific legislative basis, with the argument that common rules are needed to achieve the goals set out in sector-specific areas.[13] Already from the very beginning of the establishment of the EU, it was recognised that administrative cooperation between the EU and its member states was necessary, not least in the area of sharing administratively relevant data.[14] In the last decades, the EU has, to an increasing extent, introduced common mechanisms for the enforcement, application and supervision of EU law, for EU and national competent authorities to use in cooperation, in more or less fully developed composite procedures.[15]

A core aspect of the EU administrative rules is focused on the management of information in administrative cooperation and handling of individual matters.[16] There are therefore numerous rules in the European composite administration on the gathering and exchange of information. In the past decade, technical advancements have provided for both new possibilities and challenges.[17] Yet national law remains relevant – at least in relation to data which is protected by data protection legislation, confidentiality rules or as IP. As seen in the introduction, the legal landscape for secondary use of health data, however, is fragmented, which the Commission had identified as an obstacle to the free movement of health data.[18]

In regard to safeguards for data protection, the GDPR is the main EU framework for digital trust,[19] laying down general requirements for the member states to ensure that data subjects' rights are upheld and that personal data are processed in a secure setting.[20] Generally, the GDPR allows member states some room for adapting the safeguards to their national traditions and legal context, meaning that the national solutions may differ here too.[21] Specific requirements for safeguards may also be introduced in sector-specific law, as is seen in the EHDS, discussed in the following section.

In secondary law on administrative procedures, the focus is often directed at the formal steps in the handling of administrative matters. Recurring features

are duties of information-sharing between competent national authorities in general, as well as in individual cases,[22] minimum criteria for what parameters to include in assessments,[23] and timelines for public authorities to handle matters.[24] Because many EU sources on administrative and judicial procedures, as well as data protection safeguards in the GDPR, are drafted in an open manner – leaving quite a lot of room to be filled by national law – the relationship between EU and national data protection safeguards and administrative guarantees is often complex.

In addition, the member states are also required to uphold the general principles of law elaborated by the Court of Justice of the European Union in its case law.[25] Accordingly, under the principles of good administration, member states are obliged to investigate matters carefully under the duty to care,[26] the right to be heard,[27] to provide reasoned decisions,[28] and to uphold other administrative principles, such as the principle of legitimate expectations, even though these are not explicitly mentioned in secondary law.[29] As with requirements in secondary law, the application of these principles does not require that national procedures are abandoned, but rather that they are applied in such a way that the sought-after legal protection is guaranteed in an effective manner.[30] The Court of Justice held in *Åkerberg Fransson*, in regard to the principle of *ne bis in idem*, that national procedures can be applied 'provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European Union law, are not thereby compromised'.[31]

10.2.2 General data protection safeguards in the EHDS

According to the EHDS proposal put forward by the Commission, 'strong safeguards and security measures will be implemented to ensure that the fundamental rights of data protection are fully protected'.[32] The EHDS Regulation accordingly sets out a number of general safeguards, to be built into the relevant legal and technical solutions. The most central of these are data minimisation, technical safeguards for secure processing, purpose limitations and an opt-out mechanism for natural persons from the processing of personal health data.[33]

Data minimisation rules are given a particularly prominent place in the EHDS, meaning that electronic health data are primarily to be processed in an anonymised format. Pseudonymised data are only to be made available if the purpose of the planned processing otherwise cannot be achieved.[34] If pseudonymised data are to be provided, the encryption key is to be available to the HDAB only.[35]

Another central category of safeguards is technical safeguards for secure processing. Access to electronic health data for secondary use should be given through a secure processing environment, which the HDAB is to provide.[36] The HDAB providing the service should remain in control of the access to the electronic health data at all times, and grant relevant access to data users. Only non-personal data which do not contain any electronic health data should be extracted by the data users from that secure processing environment.[37] All

secondary use access to electronic health data should be granted through a secure processing environment, and the principle 'bring questions to data instead of moving data' should be applied whenever possible.[38] For multi-country application, where electronic health data need to be accessed across borders, the Commission is to establish an infrastructure, HealthData@EU, in which the national HDABs and other trusted partners will be authorised participants.[39]

The limitation of permitted purposes in the EHDS is a further safeguard, aiming to ensure that the arrangements for making electronic health data available are only accessible for data users with legitimate purposes benefitting society. It defines eight permissible purposes for which electronic health data can be processed for secondary use. They include public and occupational health interests, policy making and regulatory activities, official statistics and scientific research, including the training, testing and evaluating of algorithms and AI systems.[40] There are five purposes that are explicitly prohibited, including making certain decisions detrimental to a natural person, advertising or marketing activities, developing harmful products or services and activities in conflict with ethical provisions pursuant to national law.[41]

10.2.3 Available and efficient administrative application procedures for secondary data use in the EHDS

One of the most central parts of the EHDS for secondary use is the introduction of an elaborate scheme for providing access to electronic health data at the national level, in order to ensure an efficient governance structure for access to data. The regulation lays down two tracks for accessing health data. The main track is via a data access application for a data permit in accordance with Article 67. A simplified form of access can be given via a data request set out in Article 69, merely providing access to anonymised statistical data, without access to the underlying electronic health data. Both tracks go via the HDAB, where the procedure for assessing the data access application, in order to issue a data permit, requires a more in-depth assessment, as discussed below. By derogation, if data are sought from a single data holder in a single member state, the HDAB can refer the application directly to that data holder, if it has been designated a 'trusted data holder'.[42] The trusted data holders are to apply the same assessment requirements as the HDAB.[43] An accelerated application procedure is also provided for public sector bodies and Union institutions, bodies, offices and agencies with a legal mandate in the field of public health.[44] In this chapter, the focus will be on the main track for the data access application.

The EHDS is in line with the type of procedural rules in secondary EU law described above, laying down formal steps in the handling of an administrative matter. The main steps for the procedure for assessing a data access application, in order to issue a data permit, are set out in Articles 67 and 68. The applicant must submit eight categories of information: the purposes for which the data are requested, a detailed explanation of the intended use and expected benefits, a description of the requested data and whether pseudonymised data

are requested, the safeguards planned to prevent any misuse and to protect the rights and interests of the health data holder and of the natural persons concerned, and, where applicable, information on any assessment of ethical aspects of the processing. The eighth point requires the applicant to demonstrate that 'all other requirements in this Chapter are fulfilled'.[45]

The HDAB is then to assess whether the requirements are met, taking into account the risks to national defence, security, public security and public order, as well as the risk of undermining confidential data in the governmental databases of regulatory authorities.[46] The HDAB will also decide on general and specific conditions for each data permit.[47] The HDAB should issue a decision on a permit within three months of receiving a complete application, with the possibility of an extension of three additional months, depending on the urgency and complexity of the application and the volume of requests.[48] After a data permit has been issued, the data holder must put the electronic health data at the disposal of the HDAB within three months, with a possible extension of another three months,[49] after which the HDAB should make them available to the data user within two months, unless it specifies a longer timeframe.[50]

The EHDS foresees that health data applicants may want to access electronic health data from data holders in more than one member state and has therefore devised a specific procedure for the assessment of such applications, in accordance with the single application principle.[51] With a single application, the applicant can thus be able to obtain authorisation from multiple HDABs in different member states. However, each HDAB will remain responsible for deciding to grant or refuse access to the health data within its remit.[52]

Lastly, it may be noted that the EHDS also includes rules on sanctions and penalties for data holders and data users, in case of breaches of their obligations. Data holders that fail to put the electronic health data at the disposal of the HDAB within the deadline can be fined for each day of delay.[53] In case of repeated breaches, a data holder may be banned from participation in the EHDS for a period of up to five years.[54] Data users that do not comply with the regulation and with the data permit may have their permit revoked and can also be banned from any access to electronic health data for a period of up to five years.[55] Furthermore, and more severely, data holders and data users can be subjected to administrative fines of up to 20,000,000 EUR or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[56] These procedures will be discussed below.

10.3 Allocation of regulatory powers: EU or national rules on administrative safeguards and protective tools?

10.3.1 Exhaustive procedures, minimum rules or national regulatory responsibility?

The question to be discussed in this section is what administrative law tools are available for balancing the general and individual interests under the EHDS,

and where the power to regulate these tools is allocated. As seen above, some of these tools are laid down in the EHDS, whereas others follow from national law.

In relation to the process of assessing applications for data permits, the question may be raised of to what extent the procedure laid down in the EHDS is comprehensively regulated, and if it may be complemented by national law. It seems clear that this question cannot be answered in a definitive manner, as the answer will differ between different steps in the procedure. In regard to the rules on time limits for both the HDAB and the data holders, they must be understood to be exhaustive, with no possibility for deviations in national law. The same applies to the definitions of what data are to be accessible and the aforementioned rules on purpose limitations and conditions for access. Accordingly, it is stated in the preamble that member states may no longer maintain or introduce further conditions, limitations or specific provisions requesting the consent of natural persons in accordance with Article 9(4) GDPR, except those that are explicitly mentioned in Article 51(4) EHDS.[57] However, the assessments of the safeguards planned in the individual applications for data permits will have to be complemented by national law, in accordance with the delegated structure of defining appropriate safeguards in the GDPR. These will be discussed in Section 10.3.2.

Furthermore, the EHDS contains only limited rules on the right to good administration, the duty of care, the participation of the parties concerned, the right to reasoned decisions, and the right of access to an effective legal remedy. It must be presumed that national law on the matter will be applicable, as will be discussed in Section 10.3.3.

10.3.2 Legal, technical and organisational safeguards in the assessments of data access applications

Generally, the GDPR itself does not define the exact requirements for the processing of personal data in a specific context but requires that safeguards are in place, be they legal, technical or organisational.[58] As seen in Section 10.2.2, the EHDS contains several strong data protection safeguards, rules on data minimisation, technical safeguards for secure processing, purpose limitations and an opt-out mechanism for natural persons. As for the exact content of these safeguards, this will vary depending on the sector-specific area, as well as the national law applicable. For example, the research exception in Article 89.1 GDPR requires specific safeguards to be adopted.[59] However, the EHDS regulation sets out certain limitations to what safeguards the member states may require. In a medical research context, two mechanisms are widely used, namely the informed consent of the data subject and an ethical approval from a competent research ethics committee.[60] As the EHDS does not rely on the informed consent of the data subject as a legal basis for processing of data, instead relying on different grounds depending on who is doing the processing,[61] national requirements on informed consent are no

longer to be upheld.[62] As seen above, natural persons are given a right to opt out from the processing of their personal health data for secondary use.[63] As regards ethical approval, the EHDS foresees that this assessment will be aligned with that conducted by the HDAB ahead of granting a data permit.[64]

Processing for other purposes than research, such as innovation, policy-making, patient safety, official statistics or regulatory activities, will be governed under other sets of safeguards.[65] With the importance attributed to the principle of proportionality in balancing the interest of protection of the rights of the data subject and the interest of access to information and free movement of data, the level of protection will be context-dependent.[66]

Secrecy and confidentiality rules are another category of legal safeguards that may be used in order to protect both the privacy of individuals (in medical research and elsewhere) and the rights of IP right holders and businesses. Unlike what is the case for data protection rules, there are no generally applicable EU rules on secrecy, although there are many examples of secondary EU law requiring member states to ensure the confidentiality of information circulated under EU law.[67] The EHDS also sets out a procedure for protecting IP rights and trade secrets.[68] As a first step, the data holder should inform the HDAB of any data in their possession containing content or information protected by IP rights, already when communicating the dataset descriptions pursuant to Article 60(3).[69] The HDAB is to take 'all specific appropriate and proportionate measures, including legal, organisational, and technical ones', to protect the relevant rights, for example via contractual arrangements between health data holders and health data users. If a serious risk of infringement of rights remains, access to the health data may be denied.[70] Here too, national traditions and cultures vary, meaning that the available measures will also be likely to vary.

In summary, the HDABs may face a complex task in assessing the applications for data permits. The HDABs will be tasked with assessing all categories of electronic health data available under the EHDS, which includes a wide variety of data divided into 15 different categories,[71] for any of the eight permitted purposes.[72] Even if all processing of health data were to take place locally, in accordance with local law, the data users could come from all over the world, with different traditions regarding the means of processing and of applying safeguards. This may be especially cumbersome in the assessment of multi-country applications.[73] However, trusted data holders assessing single data applications will only assess applications for health data that they are storing themselves.[74]

10.3.3 Administrative and judicial procedural guarantees in the assessments of data access applications

Turning to the second category of tools to balance general and individual interests under the EHDS, this section will focus on the EU rules and principles available to ensure administrative and judicial procedural guarantees,

the right to good administration and the right to an effective remedy within the handling of a data access application. The question is thus to what extent the EHDS lays down rules on the duty to care for the HDAB or the trusted data holder, the right to be heard, the right of access to files and the right to a reasoned decisions for the parties concerned, as well as the right of access to effective judicial remedies.[75] It should be said that the provisions in the EHDS are limited and not always consistent. Five sections involving sub-principles to the general principle of good administration in individual decision-making procedures have been introduced, as well as a general reference to 'appropriate procedural safeguards, including effective judicial remedies and due process' in relation to administrative fines.

First, the procedure for applying for a data permit contains elements of the principle of the duty of care and the right to timely processing in accordance with the rules on time limits. These limits describe how soon the HDAB must handle a data access application, how soon the data holder must provide the data after a permit has been issued and again, and how soon the HDAB must make the data available to the data user.[76] Furthermore, data applicants are given a right to a reasoned decision, if a data access application is refused. However, there is no explicit right to a reasoned decision if the conditions in the data permit should be considered unreasonably strict.

The procedures for investigating breaches of obligations under the EHDS also include some elements of the principle of a duty of care, as they require the HDAB to take 'appropriate and proportionate' measures aimed at the data users.[77] In regard to measures aimed at the data holder, these must be 'transparent and proportionate'.[78] Both data holders and data users are further to be given a right to be heard before any measures are taken against them.[79] Both data holders and data users are to be provided reasons for the measures imposed.[80] The Commission's proposal included a right to effective judicial remedy, which was not included in the EHDS.[81]

In regard to procedural safeguards applicable when handling matters of administrative fines, the EHDS uses a different regulatory model. It makes a blanket reference to EU and member state law, in order for the exercise of power by the HDAB to be subject to appropriate procedural safeguards, including effective judicial remedies and due process.[82] This regulatory model is in line with the general obligation laid on the member states, to uphold the general principles of EU law even when relevant secondary law does not include corresponding rules.[83] Accordingly, the scant rules on administrative and judicial guarantees in the EHDS could be complemented by national rules. However, the regulatory model becomes especially opaque when parts of the procedure are regulated in the form of minimum rules, as is the case for the application procedure with its elements of the right to good administration, and other parts are to be fully regulated under undefined legal principles. It is not obvious to what extent the application procedure can be regulated by national law, or if it is to be exhaustively regulated through the rules described above.

One aspect that can be seen as particularly relevant in this regard is the scope of application of the procedural rules *ratione personae*. Who may be identified as concerned in such a manner that they can trigger the right to good administration and the right to an effective remedy, and at what point in the procedure does this status arise? It follows from the above that the administrative procedure on a data access application only involves the applicant and the HDAB, whereas the data holder is not involved at all until after the data permit is issued. At this stage, the data holder must put the electronic health data at the disposal of the HDAB within three months, with a possible extension for another three months.[84] If the data holder does not comply, it can be fined for each day of delay.[85] There is accordingly no participatory procedure before a data permit is issued to allow the data holder to present its views on the possibility to give access to the data that it is holding, in regard to legal restriction due to data protection rules, IP rights or confidentiality. However, the preamble does seem to presuppose that the data holder could be involved in the application procedure, as it is stated that 'the HDABs and, where relevant data holders, should assist data users in the selection of the suitable datasets or data sources for the intended purpose of secondary use'.[86] The EHDS accordingly foresees that the data holder could assist in the application procedure, but not that it could be given a possibility to state its views on the outcome. Only when the HDAB is investigating the breach of obligations is a right to be heard provided. Moreover, in the final version of the regulation, no right to an effective remedy is ensured.

The deletion of any explicit right to an effective remedy from the final version of the EHDS may be compared to what is seen with the Data Governance Act, which provides an effective right to redress for any natural or legal person directly affected by a decision on a request for re-use of data under the Act.[87] This review could be performed by an 'impartial body with the appropriate expertise', meaning that there is no right to an effective remedy before a court.[88] The EHDS does not provide the individuals who have an interest in the data, either as data subjects or as holders of data protected by IP rights and trade secrets (which can of course be the data holders themselves), any role in the application procedure, nor any right to redress or effective remedy.

In as far as the procedural rules are not to be seen as exhaustive, the ambiguities in regard to the scope of application of the rights may be resolved in accordance with national laws, providing broader administrative and judicial guarantees than the rules in the EHDS. As with the legal, technical and organisational safeguards, administrative and judicial procedures differ between member states. There is a common understanding on standards, principles and rules at a basic level, but there are important differences in the actual implementation, scope of application and content.[89] Thus, it can be foreseen that the data access applications may be handled rather differently in different member states.

Importantly, the right to good administration is traditionally a right to be exercised in an administrative procedure before a public authority, whereas the EHDS foresees that a data access application may also be submitted to a trusted data holder, which may be a private entity, either commercial or non for profit.[90]

On the one hand, the trusted data holder procedure becomes less complex in this two-party setting, involving only the data holder and the data applicant. On the other hand, the implementation of the administrative guarantees that the EHDS includes – for example the different time limits and penalties for not respecting them – may be more difficult to uphold in a procedure with only private parties. The procedures also differ in the sense that in reality, the trusted data holder will have an independent say in the assessment that it would not have if the HDAB were involved. In these cases, it might be beneficial for data applicants if the EHDS provided for a clear right to an effective remedy if a trusted data holder does not give access to data in accordance with the EHDS.

The important differences in administrative and judicial guarantees that can be foreseen may, in themselves, be seen as contradictory to the ambitions of the Commission to enable swift and efficient access to electronic health data, in order to achieve the aim to 'unleash the data'.[91] In the preamble to the EHDS, it is stated that 'in order to ensure that all HDABs issue permits in a similar way, it is necessary to establish a standard common process for the issuance of data permits, with similar requests in different Member States'.[92] The Commission should therefore support the harmonisation of data applications and requests.[93] This may be especially relevant in multi-country applications, which will be discussed in the following.

10.4 The roles of HDABs – facilitators, collaborators and overseers

10.4.1 The different roles of the health data access bodies

Two sets of administrative balancing tools available to the HDAB were discussed above – data protection safeguards and administrative and judicial guarantees – focusing on the allocation of the regulatory responsibilities between EU law and national law. The question discussed here is how the roles and functions of the HDABs are to be understood.[94]

When analysing the discretion and room for manoeuvre of the HDABs to interpret EU and national law, i.e., the context in which the balancing tools are to be applied, it is relevant to take into account what tasks and functions the bodies are given in the EHDS. First, it may be underlined that one important task for the HDABs is to 'contribute to the consistent application of this Regulation throughout the Union', which is to be done by cooperating with the Commission and the Data Protection Authorities (DPAs) under the GDPR, among others.[95] The EHDS also seems to cast the HDABs as multi-tasking organs, with several distinctive features. They can to some extent be described as facilitators, supporting and increasing access to electronic health data. The facilitator feature is not clearly expressed in the tasks of the HDABs but can to a certain extent be read into their role. It is only expressly recognised in relation to multi-country data applications, where the HDABs are tasked with facilitating cross-border access, in close collaboration with each other and with the Commission.[96] This feature is presented in Section 10.4.2.

The HDABs are also to collaborate closely data users and, when providing a secure processing environment. In the EHDS proposal, the HDABs and data users were to be joint data controllers, requiring active involvement on the part of the HDABs in the actual data processing. This role has been removed in the final text of the EHDS and the functions have been separated. The remaining collaborative functions are discussed in Section 10.4.3.

HDABs also function as overseers, to some extent together with DPAs, ensuring compliance with the EHDS. Here, the competence to decide on penalties and administrative fines for both data holders and data users, described above, is key. These issues are further discussed in Section 10.4.4.

Lastly, it may be mentioned that the HDABs have some, limited obligations vis-à-vis the natural persons whose health data are being processed, regardless of whether they can be considered data subjects under the GDPR. The obligations are mostly of a general nature, directed at the public at large, not individual data subjects. The HDABs are to provide information on the conditions under which electronic health data are made available for secondary use. This shall include information on technical and organisational measures undertaken to protect the rights of natural persons, the applicable rights of natural persons in relation to the secondary use and how rights under the GDPR may be exercised, as well as the results of the outcomes of the projects for which the health data were used.[97] If an HDAB is informed of a significant finding related to the health of a natural person, the HDAB is to inform the data holder about that finding. The data holder, in turn, is to inform the natural person or the relevant health professionals, in accordance with national law.[98]

10.4.2 HDABs as facilitators in multi-country applications

Although the overall aim of the EHDS is to improve access to electronic health data for the benefit of society,[99] it does not expressly state that this is an aim for the HDABs to pursue. Instead, the EHDS defines the role of the HDABs in more neutral terms in Articles 55 and 57, with the granting of access to electronic health data on application as their most prominent task. However, in the preamble, it is noted that the establishment of HDABs is 'an essential component for promoting the secondary use of health-related data'.[100]

As seen above, the EHDS explicitly tasks the HDABs with facilitating access to health data in one situation, namely multi-country applications.[101] The preamble acknowledges that going through the authorisation process in multiple member states can be repetitive and cumbersome, and that the stated purpose of the single application procedure is to reduce the administrative burden and barriers for data users.[102] The data applicant will be able to obtain authorisation from multiple HDABs in different member states with one single application. However, this will not result in just one permit. Each HDAB remains responsible for assessing access to the data held in their member state.[103] The HDABs are to communicate via HealthData@EU, a secure infrastructure for participants authorised under the EHDS.[104] The Commission will operate HealthData@EU and support and facilitate the information exchange necessary.[105]

How the assessment of the different parts of the application is to be carried out is not quite clear, but in order to meet the goal of easing the administrative burden, it must be assumed that the HDABs are to coordinate their work. The EHDS Board is also tasked with facilitating the cooperation and information exchange between member states, for instance in coordinating the practices of HDABs, and to issue written contributions and exchange best practices on matters related to this coordination.[106] The HDABs are to be represented in the EHDS Board and will thus take part in that work.[107] The Commission further has a general role in supporting capacity building in the member states.[108]

However, the procedure for multi-country applications in the EHDS must be described as vague, with no elements of actual composite decision-making. The single application will not result in just one data permit. On the other hand, the EHDS foresees that the coordinated assessment could ease the acceptance of a decision in other member states, as it is held that 'a data permit issued by one concerned HDAB may benefit from mutual recognition by the other concerned HDABs'.[109] For this to work in practice, the HDABs would probably need to actively interpret national laws in the light of the aim of the EHDS, to facilitate access to electronic health data.

10.4.3 HDABs as collaborators with data holders and data users

Although the EHDS – unlike the EHDS proposal – no longer allocates joint controllership to HDABs and data users, it is clear that the parties must cooperate. In order to separate the roles of the HDAB, the data holder and the data user, the EHDS sets out a model for how the roles of controller and processor are to be allocated during the transfer of data, in so far as they constitute personal data according to the GDPR, i.e., are not fully anonymised.[110] The data holder should be deemed to be the controller for the disclosure of the requested data to the HDAB, whereas the HDAB should be deemed to be the controller for the data processing when 'fulfilling its tasks pursuant to this Regulation'.[111] In the preamble, this is described as 'when preparing the data and making them available to the health data user'.[112] After this, it is the data user that is deemed to be the controller for the processing of data in pseudonymised form in the secure processing environment pursuant to its data permit. The HDAB is then deemed to be a processor on behalf of the data user. If data are accessed from a trusted data holder directly, the data holder should be deemed to be acting as a controller and processor under the same terms.[113]

It is expected that the Commission will establish a template for controller–processor agreements for the HDABs and data users.[114]

10.4.4 HDABs as overseers

The third and last role of the HDABs to be analysed here is that as overseers of compliance on the part of data holders and data users. The HDABs are to monitor and supervise the compliance of data users and data holders with the

requirements laid down in the regulation.[115] As presented above, the EHDS includes rules on penalties for both data holders and data users, which the HDABs are responsible for enforcing. In a late stage in the legislative procedures, the HDABs were given a mandate to issue substantial administrative fines against data holders and data users, which must be considered to alter their cooperative relationships to some extent.

If the supervisory functions involve processing of personal health data, the relevant provisions in the GDPR would apply. According to the preamble, the supervisory authorities under the GDPR would then be the only authorities competent to enforce those rules.[116] In such a case, the HDAB is to inform the competent DPA and provide all the relevant information.[117] Furthermore, in regard to the possibility for member states to introduce an opt-out mechanism from the processing of personal health data for secondary use, the EHDS allocates the supervisory responsibilities for this to the DPAs.[118]

10.5 Summary and conclusions: what are the conditions for balancing general and individual interests under the EHDS regulation?

The main aim behind the EHDS is to improve access to health data and to enable their use for the benefit of society.[119] Thus, there is a societal interest in making the data easily accessible, which is to be secured by the introduction of available and efficient administrative procedures for data applicants. The EHDS should also strive to uphold the rights and interests of the natural and legal persons involved, mainly related to data protection, IP rights and trade secrets. This will be another task for the competent public authorities.[120]

In this chapter, the analysis has focused on the tools provided in the EHDS for balancing these two interests. The main question to be answered is if the EHDS regulation has managed to define administrative balancing tools for societal and individual interests within the fragmented legal landscape for secondary use of health data in the EU and its member states, which may overcome the legal uncertainties regarding secondary use of electronic health data and barriers thereto.

The answer to the question could be yes or no, depending on whether you see the EHDS as a half-full or half-empty glass. Important steps have certainly been taken. The EHDS provides for strong general data protection safeguards by only allowing access to electronic health data in anonymised or pseudonymised form in a secure processing environment. For the latter type of data, the aim is that the principle 'bring questions to data instead of moving data' is to be applied, as far as possible. Furthermore, in regard to the main road to access electronic health data – the data access application for a data permit – the EHDS provides for an efficient governance structure by laying down a step-by-step procedure. There is also clear allocation of responsibilities for the different roles, and there are timelines, penalties and administrative fines to ensure compliance.

However, there is a risk that the efficiency of the step-by-step procedure laid down will be efficient only on paper. The actual assessment of the requirements of data protection safeguards for granting a data permit is regulated only at a minimum level, with the gaps to be filled by national law. These rules will accordingly vary between member states. It is for the data user to propose safeguards to be implemented in each individual case and for the HDAB to assess if these fulfil the requirements of national law. The HDABs must accordingly assess the sector-specific rules for all the 15 categories of health data available under the EHDS, in relation to any of eight permitted purposes. This must be described as a complex administrative endeavour. In Finland, where a similar centralised health data access regime has been introduced, there are reports that the procedure is both lengthy and expensive.[121]

The applicable administrative procedures are also regulated at a minimum level. A data user may submit a single application for multi-country access. The HDABs are then supposed to collaborate in their assessment under the lead of the HDAB of the data user's choice. However, there are no actual composite decision-making procedures. The collaboration is only informal and will not lead to only one data permit. Instead, the EHDS recommends member states to apply the principle of mutual recognition in relation to the other HDABs concerned. Whether or not this will work in practice is difficult to say.

Furthermore, the roles of the natural and legal persons involved in the procedure are unclear. As for administrative guarantees for good administration, the EHDS does contain some minimum rules, mainly in regard to procedures on penalties and restrictive measures. In the most important procedures, on administrative fines, the regulation simply refers to "appropriate procedural safeguards" in EU and national law, which casts some doubt over how the other procedural rules are to be interpreted. To what extent are the procedural rules of the EHDS exhaustive and to what extent might they be complemented by other sources? For example, should the HDAB provide a right for the data holder to be heard before a data permit is granted by an HDAB, if this follows from national law? Beyond protecting the rights and interests of the individuals concerned, such procedural guarantees might actually render the assessment more adequate, as it is the data holder that has detailed knowledge of the electronic health data and the legal constraints that may apply. On the other hand, the explicit aim to render the access to health data less fragmented would be challenged.

The EHDS thus seems to leave quite some room for manoeuvre. National legislators can lay down rules for the HDABs or trusted data holders in applying the administrative balancing tools in individual cases. The HDABs may thus have quite a lot of freedom in performing the balancing in individual cases. It is relevant to analyse how the roles and functions of the HDABs have been formulated. Indeed, the roles of the HDABs are diverse. The most prominent task is to neutrally and objectively assess applications for data permits, ensuring that the safeguards planned are adequate to prevent misuse of data and to protect the rights and interests of the data holders and the natural

persons concerned. However, in regard to multi-country applications, the HDABs have been explicitly tasked with facilitating access. Furthermore, the HDABs are to collaborate with data holders and data users when providing a secure processing environment but will at the same time monitor and supervise them and may subject them to substantive fines. In the final version of the EHDS, a specific task was introduced for the member states to ensure that any conflict of interest between the different tasks of HDABs is avoided.[122] This could be interpreted as an admission of the complexity of the roles and functions of the HDABs.

In order for the EHDS to overcome the legal uncertainties regarding secondary use of health data and barriers thereto within the EU, there seems to be a need to streamline how the room for manoeuvre of the HDABs and any discretionary power is to be used. The EHDS envisions that the HDABs will cooperate amongst themselves and with the Commission and the EHDS Board, sharing best practices and developing standards and common processes. This could foster a culture of openness and accessibility, which in itself could be seen as commendable.[123] The cooperation also extends to the DPAs under the GDPR, as well as administrative bodies under the Data Governance Act, the Data Act[124] and the AI Act.[125] All in all, this creates a multifaceted and complex administrative organisational model.

There are signs that the EU is beginning to take some small steps towards filling in some gaps. The Commission has recently proposed harmonised administrative rules to be applied in the one-stop-shop procedure under the GDPR, a composite decision-making procedure for collaboration between DPAs in multi-country enforcement of the GDPR.[126] The proposal focuses on the administrative procedural guarantees for the rights of complainants and for parties under investigation, implementing existing rights under the Charter, as well as streamlining cooperation and procedures.[127] As the EHDS is to be applied in close connection to the GDPR, this may also affect EHDS-related matters, at least indirectly and in certain cases. In a sensitive area like health data, this may be seen as challenging. On the other hand, the uncertainty regarding how assessments are to be regulated is a problem in itself. If the EU legislator is not willing to go down the road of a concretely formalised composite procedure, it would perhaps be better to let the administrative balancing tools remain in the context of national law after all.

Notes

1 European Parliament and of the Council Regulation 2016/679 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) [2016] OJ L 119/1.

2 Commission, 'A European strategy for data' (Communication) (2020) 66 final, hereinafter a European Strategy for Data, 4. See further Commission, 'A European Health Data Space: Harnessing the Power of Health Data for People, Patients and Innovation' (Communication) COM(2022) 196 final, 3.

3 A European strategy for data (n 2) 1; Commission communication COM(2022) 196 final (n 2), 2, 3, 13 and 18; Commission Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, COM(2022) 197 final, Recital 38 in the preamble to the proposed regulation (hereinafter EHDS proposal); Corrigendum to the position of the European Parliament adopted at first reading on 24 April 2024 with a view to the adoption of Regulation (EU) 2024/... of the European Parliament and of the Council on the European Health Data Space', (COM(2022)0197 – C9-0167/2022 – 2022/0140(COD)), 27 November 2024 (hereinafter EHDS).
4 Commission communication COM(2022) 196 final (n 2) 6.
5 EHDS proposal 1–2.
6 EHDS proposal 3–4; GDPR Article 9.1.
7 Jane Reichel and Johanna Chamberlain, 'Public Registries as Tools for Realising the Swedish Welfare State – Can the State Still Be Trusted?' (2021) 6 *Public Governance, Administration and Finances Law Review*, 35, 35–36.
8 See note 3.
9 See Tjaša Petročnik 'Secondary use of health data in the EHDS: public interest and the role of HDABs' in this volume.
10 The principle of the institutional autonomy of the Member States was introduced in case 51-54/71 *International Fruit Company v Produktschap voor groenten en fruit* EU:C:1971:128, 4; The principle of procedural autonomy was introduced in case 33/76 *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland*, EU:C:1976:167, 5.
11 In regard to general principles, see for example C-349/07 *Sopropé – Organizações de Calçado Lda v Fazenda Pública* EU:C:2008:746, para 37 et seq; C-222/86 *Unectef v Heylens* EU:C:1987:442, paras 15–16, discussed below.
12 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, Articles 6 and 197 (hereinafter TFEU).
13 Compare Mariolina Eliantonio, 'Proceduralisation of EU Law Through the Backdoor: Legitimacy, Rationale and Future Prospects' (2015) 8 *Review of European Administrative Law* 177, 178, focusing on procedural rules for national courts.
14 An early example is the Administrative Commission on Social Security for Migrant Workers, established in 1958, see further Henrik Wenander, 'A Network of Social Security Bodies – European Administrative Cooperation under Regulation (EC) No 883/2004' (2013) 6 *Review of European Administrative Law* 39, 47.
15 Jürgen Schwarze, *European Administrative Law* (rev. ed, Sweet and Maxwell, 2006) cxiii; Herwig C H Hofmann and Alex Türk, 'The Development of Integrated Administration in the EU and its Consequences' (2007) 13 *European Law Journal* 253; Craig, P. et al. *ReNEUAL Model Rules on EU Administrative Procedure* (OUP 2017).
16 Diana-Urania Galetta, Herwig G.H. Hofmann and Jens-Peter Schneider, 'Information Exchange in the European Administrative Union: An Introduction' (2014) 20 *European Public Law*, 65, 66 et seq.
17 Jens-Peter Schneider, 'Basic Structures of Information Management in the European Administrative Union' (2014) 1 *European Public Law*, 90 et seq; Deirdre Curtin and Filipe Brito Bastos, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (2020) 26 *European Public Law* 59, 65.
18 Commission communication COM(2022) 196 final (n 2) 6.
19 A European Strategy for Data (n 2) 4.
20 Herwig C.H. Hofmann and Lisette Mustert, 'Data Protection' in M Scholten (ed), *Research Handbook on the Enforcement of EU law* (Edward Elgar Publishing 2023).
21 Jane Reichel, Allocation of Regulatory Responsibilities: Who Will Balance Individual Rights, the Public Interest and Biobank Research Under the GDPR? in S Slokenberga, O Tzortzatou and J Reichel (eds.), *GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe* (Springer 2021), 422 *et seq*.

22 Schneider (n 17) 90 et seq. See, for example, Articles 81 and 87 European Parliament and the Council Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) [2014] OJ L 173/349.
23 See, for example, Article 5.1 European Parliament and the Council Directive 2004/38/EC 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77, stating that 'no entry visa or equivalent formality may be imposed on Union citizens'.
24 European Parliament and the Council Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1, Article 9.1.
25 This follows explicitly from Article 51, Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
26 C-340/89 *Irène Vlassopoulou v Ministerium für Justiz, Bundes-und Europaangelegenheiten Baden-Württemberg* EU:C:1991:193, para 16–18; C-604/12 *H. N. v. Minister for Justice, Equality and Law Reform* EU:C:2014:302, paras 49–50. See, in general, Diana-Urania Galetta, Herwig C.H. Hofmann, Oriol Mir Puigpelat and Jacques Ziller, 'The General Principles of EU Administrative Procedural Law. An In-Depth Analysis' (2015) 5 *Rivista Italiana di diritto pubblico Comunitario* 1420.
27 *Sopropé* (n 11) para 37 et seq.
28 C-222/86 *Unectef v Heylens* EU:C:1987:442, paras 15–16.
29 C-453/00 *Kühne & Heitz NV v Produktschap voor Pluimvee en Eieren* EU:C:2004:17, para 27; C-119/05 *Ministero dell'Industria, del Commercio e dell'Artigianato v Lucchini SpA* EU:C:2007:434 para 59 et seq; C-568/11 *Agroferm A/S v Ministeriet for Fødevarer, Landbrug og Fiskeri* EU:C:2013:407, para 49 et seq.
30 C-46/16 Valsts ieņēmumu dienests v "LS Customs Services", SIA ECLI:EU:C:2017:839, para 46.
31 C-617/10 *Åklagaren v. Åkerberg Fransson* EU:C:2013:105, para 29.
32 EHDS proposal (n 3) 15.
33 See further Eila El Asry, Juli Mansnérus, Sandra Liede 'Striking the Balance: Genomic Data, Consent and Altruism in the European Health Data Space' in this volume.
34 EHDS Articles 66(2)–(3).
35 EHDS Article 66(3).
36 EHDS Article 73(1) and Recital 72.
37 EHDS Articles 73(1)–(2).
38 EHDS Recital 80.
39 EHDS Article 75.
40 EHDS Articles 53(1) a–f.
41 EHDS Article 54.
42 EHDS Articles 72(1)–(2).
43 EHDS Article 72(4).
44 EHDS Article 68(6).
45 EHDS Articles 68(1) a–h.
46 EHDS Articles 68(2) a–b.
47 EHDS Article 68(10).
48 EHDS Article 68(4).
49 EHDS Article 60(2).
50 EHDS Article 68(7).
51 EHDS Article 67(3).
52 EHDS Article 68(5).
53 EHDS Article 63(4).
54 EHDS Article 63(4).

55 EHDS Article 63(3).
56 EHDS Articles 64(4–5).
57 EHDS Recital 52.
58 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) GDPR, among others.
59 See Magdalena Kogut-Czarkowska, Mahsa Shabani 'Federated Networks and Secondary Uses of Health Data – Challenges in Ensuring Appropriate Safeguards for Sharing Health Data Under the GDPR and EHDS' in this volume.
60 Olga Tzortzatou-Nanopoulou, Kaya Akyüz, Melanie Goisauf, Łukasz Kozera, Signe Mežinska, Michaela Th Mayrhofer, Santa Slokenberga, Jane Reichel, Talisiea Croxton, Alexandra Ziaka and Marina Makri, 'Ethical, Legal, and Social Implications in Research Biobanking: A Checklist for Navigating Complexity' (2023) *Dev World Bioeth*. Epub ahead of print. PMID: 37428947, 4.
61 EHDS Recital 52 of the preamble to the EHDS regulation states that one of the legal bases set out in Article 6(1), points (a), (c), (e) or (f), GDPR combined with Article 9(2) GDPR should be required.
62 EHDS Recital 52. On consent in this volume see Patricia Cervera de la Cruz, Mahsa Shabani 'Fair Enough? Exploring the Role of Fairness in Secondary Uses of Health Data in the European Health Data Space in this volume.'
63 Patricia Cervera de la Cruz, Mahsa Shabani 'Fair Enough? Exploring the Role of Fairness in Secondary Uses of Health Data in the European Health Data Space in this volume.'
64 EHDS Article 55(2).
65 GDPR Articles 9(2) (g), (h) and (i).
66 GDPR Recital 4, Articles 6.3-4 GDPR; C-439/19 *B joined parties:Latvijas Republikas Saeima*, EU:2021:1054, para 122.
67 Carl Fredrik Bergström and Mikael Ruotsi, *Grundlag i gungning? En ESO-rapport om EU och den svenska offentlighetsprincipen* (ESO 2018:1), 125 et seq.
68 EHDS Article 52.
69 EHDS Article 52(2).
70 EHDS Articles 52(3–5).
71 EHDS Article 51.
72 EHDS Article 53.
73 Quentin Fontaine and Jan Clinck, 'The European Health Data Space Proposal: A First Look at the Newest Piece of the EU Data Sharing Puzzle' (2022) 6 EHPL 87.
74 EHDS Article 72.
75 For the content of these rules, see Galetta et al. (n 16).
76 EHDS Articles 60(2) and, 46(3–4).
77 EHDS Article 63(3).
78 EHDS Article 63(4).
79 EHDS Article 63(2).
80 EHDS Article 63(5).
81 EHDS proposal Article 43(9).
82 EHDS Article 64(7).
83 Section 10.2.1, *Sopropé* (n 11) para 37 et seq.
84 EHDS Article 60(2).
85 EHDS Article 63(4).
86 EHDS Recital 73.
87 Compare with Article 9(2) Data Governance Act.
88 Article 9(2) Data Governance Act.
89 Paul Craig, *EU Administrative Law* (OUP 2018) 265.
90 EHDS Recital 59.
91 A European strategy for data 1.
92 EHDS Recital 73.
93 EHDS Recitals 73–74.

94 See also Chapter Tjaša Petročnik, 'Secondary use of health data in the EHDS: public interest and the role of HDABs' in this volume.
95 EHDS Article 55(1).
96 EHDS Article 57(1)i.
97 EHDS Article 58(1).
98 EHDS Article 58(3).
99 EHDS Recital 1.
100 EHDS Recital 64.
101 EHDS Article 57(1).
102 EHDS Recital 83.
103 EHDS Article 68(5).
104 EHDS Article 75(7).
105 EHDS Article 75(8).
106 EHDS Articles 94(2) a and b.
107 EHDS Article 92(1).
108 EHDS Article 82.
109 EHDS Article 68(5).
110 EHDS Articles 74(1–2) and Recitals 72 and 79.
111 EHDS Article 74(1).
112 EHDS Recital 79.
113 EHDS Article 74(2).
114 EHDS Article 74(3).
115 EHDS Article 57(1)a(ii).
116 EHDS Recital 65.
117 EHDS Article 63(1).
118 EHDS Article 65.
119 EHDS Recital 1 and the EHDS proposal 2.
120 See especially EHDS proposal 15.
121 Aleksi Reito and others, 'Toisiolaki – lääketieteellisen tutkimuksen mahdollistaja vai tukahduttaja?' (2022) *Suom Lääkäril*, 77, www.laakarilehti.fi/e30589, English summary: Enabler or Suppressor? – Survey on the Effects of the Act on the Secondary Use of Health and Social Data on Medical Research.
122 EHDS Article 55(2).
123 Jane Reichel, 'The European Strategy for Data and Trust in EU Governance – the Case of Access to Publicly held Data' (2023) 4 *CERIDAP* 129.
124 European Parliament and the Council Regulation 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L2854/ 2854.
125 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence; see Tjaša Petročnik 'Secondary use of health data in the EHDS: public interest and the role of HDABs' in this volume.
126 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' (Communication) COM(2023) 348 final.
127 Commission, Proposal for Additional Procedural Rules Relating to the Enforcement of Regulation (n 126), 2, 9.

Bibliography

Legislative acts

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.
Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

Council of Europe, European Convention on Human Rights as amended by Protocols Nos. 11, 14 and 15, supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16, [4 November 1950], CETS 5.
European Parliament and the Council Directive 2004/38/EC 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC [2004] OJ L 158/77.
European Parliament and the Council Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast).
European Parliament and the Council Regulation 2016/679 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) [2016] OJ L 119/1.
European Parliament and the Council Regulation 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L2854/ 2854.
European Parliament and the Council Regulation (EU) 2022/868 of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1.

Official documents

Commission, 'A European strategy for data' (Communication) (2020) 66 final.
Commission, 'A European Health Data Space: Harnessing the Power of Health Data for People, Patients and Innovation' (Communication) COM(2022) 196 final.
Commission, 'Proposal for a Regulation of the European Parliament and of The Council on the European Health Data Space' (EHDS proposal) (Communication) COM(2022) 197 final.
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' (Communication) COM(2023) 348 final.
Council of the European Union, 'Proposal for a Regulation on the European Health Data Space – Analysis of the final compromise text with a view to agreement' 2022/0140(COD) (hereinafter EHDS compromise text).

Literature

Bergström C F and Ruotsi M, Grundlag i gungning? En ESO-rapport om EU och den svenska offentlighetsprincipen (ESO 2018:1).
Craig P, *EU Administrative Law* (OUP 2018) 265.
Craig P, et al. *ReNEUAL Model Rules on EU Administrative Procedure* (OUP 2017).
Curtin D and Bastos P B, 'Interoperable Information Sharing and the Five Novel Frontiers of EU Governance: A Special Issue' (2020) 26 *European Public Law* 59.
Eliantonio M, 'Proceduralisation of EU Law Through the Backdoor: Legitimacy, Rationale and Future Prospects' (2015) 8 *Review of European Administrative Law* 177.
Fontaine Q and Clinck J, 'The European Health Data Space Proposal: A First Look at the Newest Piece of the EU Data Sharing Puzzle' (2022) 6 *EHPL* 87.
Galetta D-U, Hofmann H C H, Puigpelat O M and Ziller J, 'The General Principles of EU Administrative Procedural Law. An In-Depth Analysis' (2015) *Rivista Italiana di diritto pubblico Comunitario* 1420.
Galetta D-U, Hofmann H C H and Schneider J-P, 'Information Exchange in the European Administrative Union: An Introduction' (2014) 20 *European Public Law* 65.

Hofmann H C H and Mustert L, 'Data Protection' in M Scholten (ed), *Research Handbook on the Enforcement of EU law* (Edward Elgar Publishing 2023).
Hofmann H C H and Türk A, 'The Development of Integrated Administration in the EU and its Consequences' (2007) 13 *European Law Journal* 253.
Reichel J, Allocation of Regulatory Responsibilities: *Who Will Balance Individual Rights, the Public Interest and Biobank Research Under the GDPR?* in Slokenberga S, Tzortzatou O and Reichel J (eds.), *GDPR and Biobanking. Individual Rights, Public Interest and Research Regulation across Europe* (Springer 2021). DOI: 10.1007/978-3-030-49388-2_23
Reichel J, 'The European Strategy for Data and Trust in EU Governance – the Case of Access to Publicly held Data' (2023) 4 *CERIDAP* 129.
Reichel J and Chamberlain J, 'Public Registries as Tools for Realising the Swedish Welfare State – Can the State Still Be Trusted?' (2021) 6 *Public Governance, Administration and Finances Law Review* 35, 35–36. DOI: 10.53116/pgaflr.2021.2.4
Reito A and others, 'Toisiolaki – lääketieteellisen tutkimuksen mahdollistaja vai tukahduttaja?' (2022) Suom Lääkäril, 77, www.laakarilehti.fi/e30589
Schneider J-P, 'Basic Structures of Information Management in the European Administrative Union' (2014) 1 *European Public Law* 90.
Schwarze J, *European Administrative Law* (rev. ed, Sweet and Maxwell 2006).
Tzortzatou-Nanopoulou O, Akyüz K, Goisauf M, Kozera Ł, Mežinska S, Mayrhofer M Th, Slokenberga S, Reichel J, Croxton T, Ziaka A and Makri M, 'Ethical, Legal, and Social Implications in Research Biobanking: A Checklist for Navigating Complexity' (2023) *Developing World Bioethics*. DOI: 10.1111/dewb.12411
Wenander H, 'A Network of Social Security Bodies – European Administrative Cooperation under Regulation (EC) No 883/2004' (2013) *Review of European Administrative Law*, 6, 39.

Case law

51-54/71 *International Fruit Company v. Produktschap voor groenten en fruit* EU:C:1971:128.
33/76 *Rewe-Zentralfinanz eG and Rewe-Zentral AG v Landwirtschaftskammer für das Saarland* EU:C:1976:167.
C-222/86 *Unectef v Heylens* EU:C:1987:442.
C-340/89 *Irène Vlassopoulou v Ministerium für Justiz, Bundes- und Europaangelegenheiten Baden-Württemberg* EU:C:1991:193.
C-453/00 *Kühne & Heitz NV v Produktschap voor Pluimvee en Eieren* EU:C:2004:17.
C-119/05 *Ministero dell'Industria, del Commercio e dell'Artigianato v Lucchini SpA* EU:C:2007:434.
C-349/07 *Sopropé – Organizações de Calçado Lda v Fazenda Pública* EU:C:2008:746.
C-617/10 *Åklagaren v. Åkerberg Fransson* EU:C:2013:105.
C-568/11 *Agroferm A/S v Ministeriet for Fødevarer, Landbrug og Fiskeri* EU:C:2013:407.
C-604/12 *H. N. v. Minister for Justice, Equality and Law Reform* EU:C:2014:302.
C-46/16 Valsts ieņēmumu dienests v "LS Customs Services", SIA EU:C:2017:839.
C-439/19 *B other party: Latvijas Republikas Saeima* EU:2021:1054.