Seminars in Cancer Biology 84 (2022) 271–283

Contents lists available at ScienceDirect

Seminars in Cancer Biology

journal homepage: www.elsevier.com/locate/semcancer

Harmonization after the GDPR? Divergences in the rules for genetic and health data sharing in four member states and ways to overcome them by EU measures: Insights from Germany, Greece, Latvia and Sweden

Fruzsina Molnár-Gábor [a,*], Julian Sellner [a], Sophia Pagil [b], Santa Slokenberga [c], Olga Tzortzatou-Nanopoulou [d,e], Katarina Nyström [b]

[a] Heidelberg Academy of Sciences and Humanities, BioQuant Centre (BQ 049), Im Neuenheimer Feld 267, 69120 Heidelberg, Germany
[b] Sahlgrenska University Hospital, 413 45 Göteborg, Sweden
[c] Uppsala University, Faculty of Law, Sweden
[d] BBMRI-ERIC, Graz, Austria
[e] Biomedical Research Foundation of the Academy of Athens, 11527 Athens, Greece

ARTICLE INFO

Keywords:
Health data sharing
Data sharing for scientific research purposes
European Health Data Space
General Data Protection Regulation
Opening clauses

ABSTRACT

The EU member states' healthcare and health-related research sectors are both characterized by an emerging infrastructural coalescence on a national and European level. The culmination of this coalescence is the planned creation of a European Health Data Space, an EU-wide infrastructure for the processing of personal data for healthcare and for secondary uses such as scientific research. In contrast to growing technical interoperability, the legal framework for such integration is not yet defined in detail, particularly with regard to data protection law. Its development is accompanied by discussions about divergent member state implementations of the EU General Data Protection Regulation (GDPR) that affect data sharing between healthcare and scientific research actors and across various sectors driven by divergent processing purposes.

The article presents four member states' main rules on data sharing based on the respective provision of the GDPR in six health-related contexts regarding data sharing across the healthcare and research sector and between the main actors of those sectors. The striking differences are then evaluated from the perspective of their factual effect on European data sharing depending on the legal characteristics of the GDPR provisions they rely on. Against this backdrop, the planned regulatory measures for the setup of the European Health Data Space are introduced and evaluated with regard to further harmonization between member states' laws and possibilities to overcome divergences in data protection rules relevant for European data sharing.

The results of the analysis point to the conclusion that the destructive effect of divergent member state rules depends on the legal qualification of the EU provisions they rely on and that this qualification also determines which further EU regulatory measure would be the most effective to set the framework for the European Health Data Space.

1. Introduction

The EU General Data Protection Regulation (GDPR) [1], which entered into force in May 2016, aims to secure a high level of protection of personal data in all EU member states by defining directly applicable rules for personal data processing thereby harmonizing the legal situation across the EU. Data can cross EU internal borders if the planned processing complies with the general requirements of the GDPR, as such transmission does not count as an international data transfer and is not subject to further admissibility grounds of Chapter V of the GDPR. Both the consistent level of personal data protection and the elimination of obstacles to data flows are intended to foster data sharing within the EU (recital 10 GDPR).

Besides opening up the door for further EU rules to foster harmonization, the Regulation leaves ample latitude in the application of national laws as well. Opening clauses in the GDPR allow member states to

* Corresponding author.
E-mail addresses: fruzsina.molnar-gabor@hadw-bw.de (F. Molnár-Gábor), ju.sellner@hadw-bw.de (J. Sellner), sophia.pagil@vgregion.se (S. Pagil), santa.slokenberga@jur.uu.se (S. Slokenberga), otzortzatou@bioacademy.gr (O. Tzortzatou-Nanopoulou), katarina.nystrom@vgregion.se (K. Nyström).

https://doi.org/10.1016/j.semcancer.2021.12.001
Received 9 September 2021; Received in revised form 30 November 2021; Accepted 2 December 2021
Available online 9 December 2021

go beyond the provisions of the Regulation and define their own rules for specific data processing situations. This corresponds to the shared competence of data protection regulation between the EU and the member states (Art. 16(2) 1st subpara. sentence 1 TFEU). It provides room for decentral amendments and allows for member state autonomy as well as national and regional specificities, rooted amongst others in divergent constitutional law traditions of data protection [2], various approaches to balancing individual rights and the divergent assessment of relevant interests therein, including the public interest. As such, it promotes the key principles of EU law: subsidiarity, proportionality (Art. 5 TFEU) and loyal cooperation (Art. 4(3) sentence 1 TEU), while at the same time fostering implementation of EU law by defining the conditions for divergences and exceptions.

However, the mixture of directly binding EU rules and specific member state regulations makes harmonized substantive data protection rules in the EU in sectors particularly affected by the opening clauses difficult to attain. Health-related data processing is notably affected.

Individual member states have a broad scope for regulations regarding genetic and health data. Art. 9(4) of the GDPR provides that member states may maintain or introduce conditions beyond those defined by the GDPR, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. In addition, based on Art. 9(2) GDPR, various prerequisites for processing special categories of data, including health and genetic data, are applied by implementing national laws. Besides being determined by the GDPR's framework, the design of member-state regulations will vary, depending on what further national rules apply (e.g. regarding professional secrecy in healthcare and on interpretative decisions made by the national legislators, for example, on the necessity and proportionality of data processing for scientific research purposes or the appropriateness of technical and organizational measures to secure the processing of special data categories for research purposes). A further significant possibility for member states to define their own rules concerns the implementation of the rights of the data subject, which may be restricted in the course of scientific data processing on the basis of the law of a member state (Art. 89(2) GDPR). As shown in many studies, national legislators have extensively used these opening clauses to define specific rules for health and genetic data processing for various purposes [3].

The room that the GDPR creates for further regulation at the national level and fragmentation is a widely discussed challenge for EU data sharing with regard to medical care and scientific research [4]. Recently, the European Commission contracted a study to obtain a more nuanced picture of the fragmentation of the rules in member states on health and genetic data processing for scientific research and medical care purposes [5]. While the study maps out the laws of each member state with accurate detail, it fails to take a closer look at what challenges emerge when these differences need to be accounted for in collaborations, how the various means to enact further national rules differentiate from one another and how these differences affect the development of EU data sharing such as within the European Health Data Space (EHDS) [6]. This article seeks to fill this gap.

The authors aim to shed light on the divergences of the rules for health and genomic data sharing for healthcare and scientific research purposes in four member states, Germany, Greece, Latvia and Sweden. The relevant opening clauses will be selected based on their significance for data sharing in healthcare and scientific research contexts. These data processing areas structure the presentation of member state provisions in reaction to the opening clauses. The divergences will be evaluated from two perspectives; firstly, they will be analysed as hurdles for data sharing between EU member states. Secondly, their deharmonizing effect will be examined according to the exact type of opening clause of the GDPR they rely on. Finally, building on both evaluations, the EU regulatory activities planned for the EHDS will be assessed as regards their potential for further harmonization of data protection laws. The EHDS aims to connect different types of health data across the EU member states and to promote access to and exchange of health data for healthcare, research and health policy purposes. As the plurality of member states regulations in the field of data protection impedes the exchange of data, the question of how to best achieve harmonization is of great importance.

Against the backdrop of an emerging EU infrastructure for healthcare and secondary use of healthcare data for scientific research purposes, the effect of divergences and further harmonization potential across member states remains a crucial regulatory subject.

2. Genomic and health data sharing in different countries and settings

2.1. Applicable laws for healthcare and health-related scientific research

The GDPR achieves extensive harmonization within the field of data protection law. However, provisions relevant for data processing in the area of healthcare and scientific research usually require further legislation to enable the processing [7]. Many of the opening clauses regulating this area provide for further EU rules. However, the EU has not yet become active here while, on the contrary, member states have done so. Particularly with regard to lifting the ban for the processing of special categories of personal data under Art. 9 GDPR, the GDPR relies considerably on the laws for medical care and scientific research that are defined by the member states (with only few exceptions, see below). This basic regulatory structure already sets the stage for a complicated interplay of EU and member state regulations that must be applied to health and genetic data processing, considering rules from various areas of regulation which vary in legal nature and force, particularly related to ethical questions and data protection oversight in scientific research.

Accordingly, national data protection laws define general rules for data processing which implement general opening clauses but member states have also adopted sector-specific rules for genomic and health data sharing for healthcare and research purposes, prominently based on Art. 9(2) GDPR. These rules have a *lex specialis-lex generalis* relation, in that the general rules implementing the GDPR will only apply to processing personal data for healthcare and health-related research if there are no more context-specific rules. For healthcare and scientific research data processing, the following details of regulatory structure in the member states are to be highlighted:

In *Germany*, as a main rule, the Federal Data Protection Act (BDSG) applies to the processing of health-related data by federal public bodies and to processing by non-public bodies, e.g. privately-owned hospitals. The BDSG applies to federal states' public bodies only subsidiary [8]. Regardless of the respective ownership structure of the hospital, state law applies to hospitals when processing health-related data [8]. State hospital laws are *leges speciales* compared to state data protection laws in the case of publicly-owned hospitals. With regard to data processing for scientific research purposes, specific provisions in the aforementioned legislation apply, depending on the controller's nature and nature of entity (e.g. public or private entity). For healthcare data and its usage for scientific research, recent rules of the Patient Data Protection Act [9] apply which focus on the electronic patient files and define rules in addition to the civil law provisions applicable to traditional patient files. Provisions on patients' rights are scattered across all the laws mentioned and must be applied according to their relation *lex specialis-lex generalis*. Ultimately, data protection oversight remains the realm of the competent federal and state supervisory authorities. Professional secrecy rules must be applied parallel to data protection rules. Professional standards and rules are decisive for ethics compliance of research, but ethics checks will ultimately remain the responsibility of institutional ethics committees. The Genetic Diagnostics Act (GDA) defines genetic data processing for diagnostic purposes but processing for scientific research purposes lies outside its scope; therefore, the general rules apply [10]. There is no specific law on biobanking.

In *Greece*, the national implementation of the GDPR, the Greek Data

Protection Act (DPA [11]) applies to the processing of healthcare data, with important foundations for the processing of personal data in the context of healthcare and medical research in the Code of Medical Ethics [12]. The Code describes the patients' right to receive all necessary information regarding their health status as well as their right not to know. All patients' personal data are protected under the obligation of medical confidentiality and those which must be processed for health-related purposes such as the age, sex, address and medical history of patients are extensively described in the Code. There is no difference between rules on data processing for public and private entities. Additionally, Law 3418/2005 defines the approval of scientific research with health-related data by the respective scientific council which mainly checks the scientific soundness of the research protocols. More recently, Law 4521/2018 establishes rules for ethics committees in the context of data processing for scientific research purposes. Therefore, since 2018, deontological screening is conducted by the competent ethics committee. This screening includes not only scientific and ethics checks but also data protection law compliance. The national Data Protection Authority may also be consulted by the data controllers for more complicated types of data processing such as large-scale genomic sequencing. The ethics committees of universities, hospitals and research facilities always take the opinion of the aforementioned scientific councils into account if there is one in place. No sector-specific law on health and genomic data exists and there is no specific law on biobanking.

In *Latvia*, general guidance regarding the processing of health and genetic data is set out in the Personal Data Processing Law (PDPL [13]). The Law on the Rights of Patients (LRP) [14a] is a central law regarding both sharing of patient data for medical care and scientific research purposes. The general rules regarding personal data processing apply without distinction to public and private entities. In Latvia, the PDPL refers to the sector-specific areas and purposes mentioned in Art. 6(2) and (3) GDPR. The law also indicates that sector-specific laws can also implement Art. 9(4) GDPR, thereby creating an alternative legal basis to Art. 9(2) GDPR for processing special categories of personal data. The specificity of this regulatory solution is that it explicitly declares that one of the requirements set forth in Art. 6(1) GDPR must be met, in case of sensitive data: one derogation under Art. 9(2) GDPR or a national rule based on Art. 9(4) GDPR (Sec. 25 para. 1 and 2 PDPL). Further specifications regarding particular processing contexts are defined in sector-specific laws. For medical care and access to patient data for healthcare and scientific research purposes, the main statute is the LRP. For the purposes of processing genetic data in scientific research, the central law is the Human Genome Research Law (HGRL) [14b]. There is an ongoing process to modernize the latter regulation through a biobank law and a data secondary use law; however, as of August 2021 only the former has been presented as a bill.

In *Sweden*, the Patient Data Act (PDA) [15] applies to data that is collected and processed by both private and public healthcare providers. The act contains provisions that complement the GDPR's rules on processing of personal data in health care. A further regulation of importance is the Public Access to Information and Secrecy Act (PAISA) [16], which defines rules for the handling of public documents by authorities which is also relevant in sector-specific contexts such as the medical context. The principle of public access to information is a fundamental principle of government in Sweden. One of the fundamental laws, the Freedom of the Press Act (FPA) [17], contains provisions on the right to access official documents, which is a manifestation of the principle of public access to information (Sec. 2 Clause 1 FPA). In principle, everyone is entitled to read the documents held by public authorities. There are,however, provisions on secrecy that restrict the right to access official documents, also in a medical context (Sec. 25 Clause 1 PAISA).

When it comes to research purposes, the Swedish Ethical Review Act (ERA) [18] states that the relevant authority (the Ethics Review Authority) must approve certain research relating to humans and biological material from humans, including research that comprises the treatment of special categories of personal data pursuant to Art. 9(1) GDPR (Sec. 3 ERA). As of now, there is no specific law on genomic data. Sweden does have a biobank law, but data processing related to biobanking falls under the GDPR and involves the Ethical Review Authority as shown above (Act on biobanks in health care) [19].

On the one hand, this short overview of applicable laws already shows that data protection rules related to specific data such as genetic and health-related data and to specific processing circumstances such as healthcare or research settings exist in member states. As will be detailed out in the following subsections, while all four countries have central data protection legislation, modalities for particular processing are detailed elsewhere. Accordingly, finding the relevant specific and general rules requires nuanced navigation through applicable laws. At the same time, some vital biomedical research areas, such as biobanking, are not necessarily specifically managed; the same applies to secondary data processing. One can question whether the member states have utilized their full capacity to create an environment which can foster scientific research.

On the other hand, rules related to the legal regimes of civil and criminal law or to the conduct by public authorities that lie outside the realm of data protection law in member states are also relevant in order to conduct health data processing. This setup of applicable rules creates not only manifold connections between EU and member state data protection rules, but also between applicable provisions in each member state within and beyond data protection law in a strict sense. These provisions also need to be respected according to their scope of application and this broadened network of applicable rules on data processing altogether increases divergence in the substantive rules in member states.

2.2. Conditions for the lawful processing of data for healthcare purposes including transmission of and access to data beyond bilateral doctor-patient relations

In order to lawfully process genomic and health data for healthcare purposes, a legal basis must be invoked pursuant to Art. 6(1) GDPR, as well as a legal ground that justifies the processing of special data categories pursuant to Art. 9(2) GDPR.

While the grounds to process special categories of data are specific to the purpose of the processing, the legal bases do not refer to any purpose. Also, the GDPR does not harmonize the definition of healthcare. Accordingly, member states might understand these purposes differently and can define divergent rules as to whether healthcare also comprises administration or quality purposes or only immediate patient care, with any other health-care related purposes constituting further processing. Member state definitions immediately influence transmission of and access to data outside the narrow and often bilateral medical care relationship for these purposes.

Additionally, when lifting the ban on the processing of special categories of personal data in Art. 9(1), the GDPR is only directly applicable in a very limited way: if processing is of vital interest to the data subject pursuant to Art. 9(2)(c) and, if not excluded by member state law, based on the exception of explicit consent pursuant to Art. 9(2)(a).

In *Germany*, as a main rule, health-related data may be processed for patient care in accordance with Art. 9(2)(h), (3) in conjunction with Art. 6(1)(b) GDPR. In this context, the treatment contract serves as the legal basis. Furthermore, there is no provision in federal or state law that excludes the lifting of the processing ban for sensitive data in Art. 9(1) GDPR by explicit consent of the data subject, so that Art. 9(2)(a) can be applied directly. Sector-specific requirements for the processing of health-related data are based on Art. 9(4) GDPR, e.g. regarding genetic examinations and analyses for medical purposes, mandating written informed consent (§ 8 GDA). This consent functions both as a consent to the medical intervention as well as to the related data processing. In the state hospital laws, processing of patient data for the purpose of patient care is permitted, some explicitly standardize processing based on consent. The transmission of patient data from one service provider to

another for the purpose of care is likely to take place on the same legal basis as for the initial processing for the purpose of medical care, although some regulations prioritize patients' consent. Some federal state hospital laws establish an authorization for further data processing for healthcare purposes. The BDSG states the parallel and independent application of professional secrecy rules for data processing (§ 1(2) sentence 3 BDSG). Many federal state hospital laws regulate that patient data can only be processed if processing does not constitute an unlawful disclosure within the meaning of § 203 of the Criminal Code. Beyond rules explicitly mandating disclosure of personal data that falls into the scope of professional secrecy, it is disputed if and which further data protection provisions might constitute a disclosure competence [20].

In *Greece*, the DPA allows processing of special categories of personal data if it is necessary to provide health or social care or for the management of health or social care systems and services or pursuant to contract with a healthcare professional or other person bound by professional secrecy or with a person under his supervision (Art. 9(2)(h) GDPR) [21]. There is no provision in the law that excludes the lifting of the processing ban for sensitive data pursuant to Art. 9(1) GDPR by explicit consent of the data subject. The legal bases for processing health data for normal healthcare provision purposes within the context of a patient - healthcare professional relationship are Art. 6(1)(c) (legal obligation) and Art. 6(1)(e) GDPR (public interest). Health data processed within medical services is subject to medical confidentiality that can only be lifted with data subject's consent. All data transmission between different healthcare providers within Greece is regulated by law 4600/2019, Article 84(4)(2). Its rules state that the Individual Electronic Health Record (IEHR) contains the individual health history of the health services recipient as well as data, assessments and information of all kinds about the condition and clinical development of this person as a patient throughout the treatment process. The content of the IEHR is maintained for life and is undivided and mandatory at national level.

In *Latvia*, the question of legal basis is not comprehensively regulated at the national level. However, various combinations of legal basis and exception grounds for special data categories could be drawn on, including a legal obligation (Art. 6(1)(c) GDPR) combined with public interest in the area of public health (Art. 9(2)(i) GDPR or combined with a provision of health or social care (Art. 9(2)(h) GDPR) as well as public interest (Art. 6(1)(e) GDPR) in connection with Art. 9(2)(h) or (i) GDPR. Hereby, the distinction between Art. 6(1)(c) and Art. 6 (1)(e) GDPR depends on various factors, including the status of the healthcare provider in question. Additionally, as it is not expressly regulated, healthcare providers may mandate consent or, as discussed below, might be required to mandate consent and therefore Art. 6(1)(a) GDPR and Art. 9 (2)(a) GDPR apply. There is no provision in the law that excludes the lifting of the processing ban for sensitive data pursuant to Art. 9(1) GDPR by explicit consent of the data subject. Furthermore, privately funded healthcare maybe based on Art. 6(1)(b) and Art. 9(2)(h) GDPR, with contracts falling under civil law rules.

Generally, rules pertaining to the processing of patient data in different contexts are set out in the LRP. This law enables patient data sharing for different purposes, including medical care of the patient and healthcare administration. As regards sharing patient information for the purposes of medical care, upon a written request and receipt of a written permission given by the head of the medical treatment institution, information shall be provided to persons and institutions listed by the law within five working days for the purpose of achieving the objectives of the medical treatment (Sec. 10 § 5 Clause 1 LRP). The LRP does not further regulate whether the medical treatment purposes refer to the patient or to others. This would need to be addressed on case-by-case basis through purpose specification of a particular processing activity, and further modalities specified in law, e.g. the mentioned regulation or Article 9(2)(c) GDPR. The Law also allows Patient e-Health records to be processed (Sec. 10 § 52 Clause 1 LRP) as specified by the Cabinet in Regulation No 134 of 22 March 2014 Regulations Regarding the Unified Electronic Information System of the Health Sector (e-Health Regulation). Despite the fact that the said regulation enables processing of previously collected patient data in different specified situations, there are occasions when a patient's consent is required instead. One example is processing of previously collected data when the patient is attending another GP than that where the patient is listed (Para. 23 e-Health Regulation).

In *Sweden*, the PDA defines an exhaustive list of processing purposes for healthcare providers (Sec. 2, Clause 4 PDA), such as care and treatment, development, and assurance of quality of the healthcare provider, based on Art. 9(2)(h) GDPR. Data processing for purposes of healthcare and medical treatment requires a professional healthcare-relationship between doctors and patients which allows the doctor to process data and thereby take part in the patients' medical journey.

Under certain conditions, the bilateral confidentiality obligation can be lifted and different healthcare providers can process data as part of the same medical record ("coherent medical record"). The main provisions for a coherent medical record are:

1 the data relates to a patient with whom there is a current patient relationship;
2 the data can be assumed to be important for the prevention, investigation or treatment of diseases and injuries of the patient in the healthcare system; and
3 the patient agrees to it.

The legal bases for healthcare data processing according to Art. 6 GDPR are (c) compliance with a legal obligation and (e) performance of a task carried out in the public interest.

Altogether, consent and the vital interest of patients are the only legal grounds based on which special categories of personal data can be processed without member states' further regulation, providing for harmonization in the healthcare setting. However, the GDPR provides the possibility to draw on other legal grounds, foremost Art. 9(2)(h), processing for healthcare purposes, which is subject to member states' implementation, and offers a variety of legal bases independent of the legal grounds and without mandating their explicit hierarchy. Accordingly, member states can specify legal grounds and mandate their application as well as the particular legal basis with which they should be paired, including in combination with informed consent in particular settings. This leads to divergent justifications for the processing of the same data categories in the member states and will lead to a divergent scope of possible processing for healthcare purposes. Altogether, there is an increased level of legal complexity that needs to be communicated to patients and which per se poses a challenge to transparency.

2.3. Conditions for the use of healthcare data for scientific research purposes

Scientific research is another term that is not defined by the GDPR. Recital 159 only states that it must be understood broadly, including any type of research. This leaves room for member states' interpretations of whether data processing for scientific research purposes must additionally comply with rules determining the public interest vested in those purposes or with rules related to the public or private character of the entity conducting research. Additionally, Art. 9(2)(j) GDPR establishes a legal ground for data processing for scientific research subject to necessity and proportionality. Even though there is extensive non-binding guidance on the necessity and proportionality test by the European Data Protection Supervisor [22], the test remains subject to national practice, as its application must also be measured against national fundamental rights in the context of the opening clauses. The coherence of European and national fundamental rights protection must be maintained. However, this doubling of the fundamental rights protection will influence the interpretation and application of Art. 9(2)(j) GDPR, because the article prescribes a weighing of the competing fundamental

rights of data protection and scientific research freedom [23].

According to the GDPR, the further processing of personal data for scientific research purposes can be based on a new legal basis and derogation from the general ban on processing sensitive data, if the further processing is considered justified. Additionally, it can be considered factually compatible with the original processing purpose and the original legal basis for processing can be applied based on Art. 5 (1)(b) GDPR. However, across many EU member states, this easing of the purpose limitation for scientific research data processing has until now only been applied in a reserved manner, as its interpretation is disputed [24]. It is more common that a new legal basis is sought to further process health data for research.

In *Germany*, health-related data can be used for scientific research purposes on the legal basis of consent. It should be noted that, according to the Conference of Data Protection Supervisors (DAK), broad consent can only be used if the concrete design of the research project does not foreseeably permit a complete purpose definition at the time of data collection and if additional measures that enhance transparency, data security and trust-building purposes are installed [25]. Beyond consent, Art. 9(2)(j) GDPR is implemented in the Federal Data Protection Law (§ 27 BDSG). Accordingly, data processing is lawful if processing for scientific research purposes is necessary in the public interest and the controllers' interest in processing data *significantly* outweighs the interests of the data subject and additional technical and organizational measures are implemented that are further defined by a non-exhaustive list in national law (§ 27(1) BDSG in conjunction with § 22(2) BDSG). The federal states have directly implemented Art. 9(2)(j) GDPR in conjunction with Art. 89(1) GDPR in their state data protection laws. With regard to further processing for research purposes, the applicable regulations of the state hospital laws usually differentiate between internal and external hospital research when transmitting the data, in addition to further requirements.

In *Greece*, processing health-related data for scientific research purposes is permitted under the condition of existing safeguards, including DPO appointment, encryption of data and restriction on data by data controllers and processors (Art. 89 GDPR) and requires the data subject's explicit consent. As an exemption to the general rule of informed consent, Art. 9(1) GDPR, the data controller may further process health data for research purposes if it can be proven that the controller's interest in processing such data outweighs the interest of the data subjects in not having their data processed. In the latter case, the data controller must take appropriate and specific measures (Art. 30(1) Law 4624/2019). This last option is the only possibility for an exemption to process special data categories based on other legal grounds than consent for scientific research purposes. There is no regulation or administrative practice covering broad consent. Along the same lines, e.g. ad-hoc legislation on COVID-19 registries allows further use of health data only if data subjects have given their informed consent. In all cases, the research project must be approved by the competent scientific council and the bioethics committee (Art. 24(2)(d) Law 3418/2005 and Art. 23 Law 4521/2018).

In Latvia, patient data that are part of medical records may be used in scientific research (Sec. 10, paras. 7-9 LRP). Further requirements apply depending on the context. Such data processing is lawful if the patient cannot be directly or indirectly identified through the information in question (Sec. 10 § 7 Clause 1 LRP), thereby implementing the relative or context-based approach to anonymity, or if the patient has consented in written form (Sec. 10 § 7 Clause 2 LRP). It can also be deemed lawful if research is performed in the public interest, the competent authorizing body has allowed the use of patient data for specific research, the patient has not previously prohibited in written form the sharing of their personal data, or it is not possible to acquire patient's consent by proportionate means and the research's benefit for the public health is proportionate to the infringement on the right of private life (Sec. 10 § 8 LRP). The law, however, does not further specify the proportionality assessment.

In *Sweden*, the legal basis for research carried out by authorities, such as universities and health care providers, is public interest, cf. Art. 6(1)(e) GDPR (Prop. 2017/18:105, p. 189–190). The disclosure of patient data in the sense of further processing for research must be preceded by an ethical review and a confidentiality assessment. The ERA contains provisions on the ethical review of research relating to humans and human biological material and defines what kind of scientific research must be preceded by an ethical review, including the use of personal data in the sense of Art. 9(1) GDPR (cf. Clauses 3–6 §§ ERA). A concrete approval from the Ethics Review Authority constitutes the legal basis for scientific research in the public interest. The Authority also has provisions on consent for such research, cf. clauses 17–22 §§ ERA. The Ethics Review Authority may decide that research may be carried out without consent according to clause 20–22 §§ ERA. However, this only applies if illness, mental disorder, impaired health or any other similar condition of the research participant prevents their consent from being obtained.

In summary, it can be seen that member states mandate both consent as a legal justification for data processing for scientific research purposes as well as use the privilege of scientific research to create an exception for data processing. Furthermore, it is questionable whether consent is the appropriate justification to process data due to the frequent power imbalance affecting the data subject. Regarding the latter, the analysis of member states' rules related to the investigation of necessity and proportionality are only partially detailed in the individual provisions. The concretization of the application of these principles is ultimately left to the application of law in the context of single-case decision making. Additionally, the connection between scientific research and the public interest is further detailed in member state laws according to the status and assignment of the legal concept of public interest by their national regulations, leading to further differences in which laws, e.g. those assigning public tasks, are applicable to personal data processing for scientific research purposes.

2.4. Rights of data subjects by data processing for scientific research purposes

According to Art. 89(2) GDPR, the data subjects' rights of access, rectification, restriction and to object can be limited in the interest of scientific research data processing under the conditions and safeguards defined in Art. 89(1) GDPR in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. The national approaches regarding to the balancing between the affected fundamental rights as defined under sec. 2.3 above, may become relevant when this rule is applied. In *Germany*, *Greece*, *Latvia* and *Sweden*, the national laws implementing the GDPR enable extensive use of the exceptions of Art. 89(2) GDPR and restrict the rights of data subjects under Art. 15, 16, 18 and 21 GDPR for the purposes of scientific research, subject to the condition defined by Art. 89(1) GDPR. Besides defining particular conditions for this legal ground in member state law, countries have also defined factors that should guide the accompanying weighing of competing legal positions.

In *Germany*, the right of access under Art. 15 GDPR is excluded for scientific research if, inter alia, providing the information would require disproportionate effort (§ 27(2) BDSG). However, it is disputed whether there is any basis for this exception in Art. 89(2) GDPR [26]. The state data protection laws in Bavaria, Baden-Württemberg and Berlin (e.g.) implement comparable solutions. In *Greece*, the right of access also does not apply when personal data are necessary for the fulfilment of the scientific research purposes and providing information to the data subject would require disproportionate effort. In *Latvia*, the law emphasizes the necessity of the limitation of data subjects' rights for the achievement of research purposes following the wording of the GDPR (Sec. 31 PDPL). In *Sweden*, according to the FPA, data subjects' rights do not apply if the processing is necessary to satisfy other important rights, e.g.

to fulfil a legal obligation or to perform a task of general interest. According to the Archives Act, the data subject rights can also be restricted if there is a legal obligation to archive personal data. Both in *Sweden* and *Germany*, limitations on the right to be forgotten as defined by Art. 17(3)(d) GDPR are also regulated together with the limitations of further rights based on Art. 89(2) GDPR. However, it can be questioned, whether Art. 17 GDPR includes an opening clause for member states at all as the prevailing opinion defines its rules as directly applicable.

In *Sweden*, additionally, when research is approved to be done without collecting informed consent, the rights of data subjects (Arts. 14, 15, 16, 17 and 21 GDPR) do not apply. This can only be done upon permission of the Swedish Ethical Review Authority (Clause 20 ERA). This is the case when the Swedish Ethical Review Authority assesses that the research will cause less harm without collecting consent. Research can also be carried out after receiving permission of the Authority if illness, mental disorder, weakened state of health or any other similar condition of the research person prevents their opinion from being obtained. However, the research may only be carried out in this situation if:

1 the research can be expected to provide knowledge that cannot be obtained through research with consent, and
2 the research can be expected to lead to direct benefit for the research participant. Even if these conditions are not met, the research may be carried out if:
3 the purpose is to contribute to a result which may be of benefit to the research participant or to another person suffering from the same or similar disease or disorder, and
4 the research entails an insignificant risk of injury and an insignificant discomfort for the research participant.

In summary, member states rules overlap in that they all make use of limiting data subjects' rights for the purposes of scientific research. In particular, Germany, Greece and Latvia have all defined rules in a way oriented strongly towards the wording of Art. 89(2) GDPR. However, the extent of limitations and the legislative guidance for the balancing between data subjects' and data processors' interests differ. In consequence, this can lead to divergent interpretations of the appropriateness of safeguards that constitute the result of these weighing exercises, having the function of both protecting data subjects and allowing data processing. Additionally, some rights underlie specific limitations in individual member states, such as the right to access or the right to be forgotten. Altogether, the legal position of data subjects differs across member states when it comes to data processing for scientific research purposes, because the interpretation of the dimensions to operationalize their fundamental right to data protection varies.

2.5. Publishing data for scientific research purposes

Publishing research results is inherently part of the scientific research process and can be considered as one of its central elements. As such, scientific publication in the sense of communication of research results is protected by the freedom of expression, which is covered by the broad opening clause of Art. 85 GDPR [27]. Publication is regularly understood as a communication that is addressed to the public, i.e. to a group of persons that is not delimited from the outset. Normally, it is irrelevant whether the publication is of interim or final results. The type of publication or medium is normally also irrelevant; it may include publications in professional journals as well as in the daily press. It may also include repositories for general use or the research institute's own website or other database [28]. In relation to freedom of expression, the term publication is to be interpreted broadly, cf. recital 153 GDPR. However, the balancing of freedom of expression as a competing fundamental right to data protection is subject to member state rules pursuant to Art. 85 GDPR. Public interest in various research results is a guiding principle of such balancing, however, explicated differently in member states' laws.

In *Germany*, publication of research results is dependent on the informed consent of the data subject as defined by the BDSG (§ 27(4) BDSG) and many of the state data protection laws. Publication in a health-related context may be a special case of data transmission. The provisions would then apply together. In principle, however, publication can be distinguished from transmission in that transmission is directed to specific persons, entities or bodies, whereas publication is directed to a possibly identifiable but not closed circle, e.g. all readers of a scientific journal [29].

In *Greece*, the DPA mandates compliance with specific conditions. Data can be published if the data controller has obtained the data subject's prior explicit and written informed consent or if the publication is absolutely necessary to present the results of the research. In latter case, all personal data must be pseudonymized before being published. Pseudonymized data are considered to be anonymised in the context of the publication. This demonstrates the application of a relative understanding of anonymity [30].

In *Latvia*, a person has the right to process data for the purposes of academic expression in accordance with applicable laws and regulations (Sec. 32 para. 1 PDPL). When processing data for the purposes of academic expression, GDPR provisions (except for Article 5, i.e. data protection principles) shall not be applied if the following conditions are present: 1. data processing is conducted while respecting the right of a person to private life and does not affect interests of a data subject that require protection and override the public interest; 2. compliance with the provisions of the GDPR is incompatible with or prevents the exercise of the rights to freedom of expression and information (Sec. 32 para. 3 PDPL).

In *Sweden*, data must be aggregated before being published, which means that it no longer constitutes personal data. The data controller (usually the hospital or university that has been collecting and processing the data before aggregating it) will take responsibility for all risks that are attached to the publication and is thus subject to the relevant provisions of data protection law, e.g. subject to a risk assessment.

In summary, the publication of health-related data underlies stricter conditions in member states. With the exception of Sweden, the main condition is the explicit consent of the data subject that might be subject to further conditions imposed on its form. However, other solutions have also been developed to justify publication, often subject to a specific necessity and proportionality test or to appropriate technological safeguards. This indicates the member states' differences in weighing the freedom of scientific expression against the right to data protection. Altogether, these solutions leave less room for further configuration in the application of law and seem to be better detailed on the legislative level than other data processing rules related to a necessity and proportionality test or the interpretation of the appropriateness of technical safeguards. Nevertheless, these divergent rules themselves can lead to divergent publication conditions and possibilities between member states.

2.6. Data sharing with public authorities

Data sharing with public authorities within the member states is regularly defined in the national data protection laws. This can include specific purposes such as pharmacovigilance and healthcare administration. When related to the health context, many purposes will be defined as an important objective of general public interest and based on the opening clause defined by Art. 23(1)(e) GDPR.

On the federal level in *Germany*, derogating from Art. 9(1) GDPR, both public and private bodies are permitted to process special categories of personal data if processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices (§ 22

(1)(c) BDSG). Obligations to take measures for quality assurance in the healthcare sector arise from various provisions of the Social Code (SGB V), whereby the Joint Federal Committee bears crucial responsibilities. Permission to use secondary data for the improvement of inpatient care is further defined in state hospital laws. For the purposes of pharmacovigilance, professional codes define obligations for physicians and pharmacists to report adverse drug reactions and findings related to the recording, assessment and prevention of risks associated with medicinal products. The Federal Medical Devices Act (MPG) regulates personal data processing for the purposes of evaluation and assessment of risks arising from the application or use of medical devices by the competent higher federal authority (§ 29 MPG). Related to pharmacovigilance, the ordinance on the database-supported information system on medicinal products of the German Institute for Medical Documentation and Information (§ 1(3)(3) DIMDI-Arzneimittelverordnung (DIMDI-AMV)) leaves the application of data protection rules unaffected.

In *Greece*, the law states that the IDIKA SA, as the processor of the archiving system of the IEHR, is allowed to provide anonymous data to the Ministry of Health in order to carry out epidemiological, statistical, financial, administrative and management analyses for improving the health and quality indicators of the services provided (Art. 84(4)(10) Law 2600/2019). In addition, more specific technical issues for the operation of the national Patient Registry for COVID-19 are described in the Joint Ministerial Decision which regulates the measures dealing with the Covid-19 pandemic and other urgent provisions (Art. 83 Law 4600/2019 and Art. 29 Law 2650/2020). Overall, it is the National Organization of Public Health (EODY) which has access to all the information of the COVID-19 Patient Registry and to the searching possibilities within the relevant platform in the context of the epidemiological investigation carried out by the Directorate of Epidemiological Surveillance and Intervention for Patients. EODY also has access to data from hospitals, primary health care facilities, laboratories, the Health Operations Center of the National Emergency Center and the General Secretariat for Civil Protection, with the aim of completing the Covid-19 Patient Registry and implementing corrections in various sections of the platform, e.g. of residence data (Art. 12 paras. 1 and 2 Law 4722/2020).

In *Latvia*, the law lists those actors who are authorized to receive patient data in accordance with the procedures laid down in the laws and regulations regulating the field of health care (Sec. 10 para. 51 LRP). This provision also lists those actors who are allowed to process information accumulated in the health information system regarding a patient in accordance with the procedures and to the extent defined by law. For example it can be noted that the law enables the National Health Service to receive data for the administration of health care services paid by the state budget, as well as for the processing of personal data with the purpose of transferring information to a statistical body (Clause 2 s. 10 para. 51 LRP). The law also enables the State Agency of Medicines to process data for the ensuring of pharmacovigilance functions (Clause 3 s. 10 para. 51 LRP).

In *Sweden*, the PAISA contains provisions on the handling of public documents by authorities and certain other bodies regarding registration, disclosure, and other handling. Before any kind of patient data may be disclosed by the care provider, they must execute a confidentiality assessment. The examination normally consists of two stages. Firstly, the public authority must examine whether there is any secrecy provision that pertains to the information in question. If not, the information is public domain in any case and must be disclosed. If there is a secrecy provision that applies either directly to the public authority or due to a provision on attaching secrecy provisions to the data when transmitted to entities who regularly do not fall under secrecy provisions, the authority must, in the second stage, conduct the required risk assessment. This means that the authority must determine whether the information can be disclosed in the specific situation (Sec. 25 Clause 1 PAISA). Such an assessment may result in either patient data being disclosed for the research study or in a refusal to process the information.

The GDPR leaves it to the member states to define rules for data processing that are related to their particular public interests; these are often condensed in codified public tasks such as those related to public health matters. In contrast, monitoring public health threats, rules on pharmacovigilance and medical devices regulation, as well as provisions on data processing for quality assurance and health management are fields regulated by all member states. They are related to data processing designed as tasks of relevant public authorities in the member states and are currently focused on a scope of application of those laws related to particular situations.

2.7. Further processing of health-related data

As genomic medicine is advancing, genomic databases and linking genomic data with health data gains significance. The distinctiveness and diversity of many diseases that are driven by genomics such as rare diseases and different types of cancer, combined with the small number of patients for many disorders mandates cross-matching data between centres to increase cohort size, enable discoveries and replication of findings, and interlinkage of health data to foster translation of findings into therapies [31]. For this reason, creating health data bases that are both open for the integration of genetic data and research results and are accessible for research purposes can enhance care offered to patients. In the EU member states, there exist different rules related to the possible collection and linkage of genomic data by, for example, adding it to specific registries, biobanks or certain research databanks with divergent access rules. These rules implement the GDPR conditions for further data processing or are defined as new processing and rely on one of the legal grounds pursuant to Art. 9(2) GDPR and a legal basis pursuant to Art. 6(1) GDPR.

2.7.1. Integration of genetic analysis executed in the course of medical care and research into databanks

In *Germany*, there are no specific federal or state level genetic databanks. Currently, the National Research Data Infrastructure is being built. Within this infrastructure, the German Human Genome-Phenome Archive (GHGA) [32] will provide the infrastructure to meet both the desire to handle omics data in an open and FAIR manner and the need to keep personal data safe. It will provide the long-term archive of human omics data federated with the European Genome-Phenome Archive (EGA), streamline data deposition by direct data and metadata transfer from major national omics centres and provide central infrastructure for distributed data access committees, thereby facilitating data access and reuse for research. Furthermore, a national model sequencing initiative has been set up and lately guided by a new law according to which whole genomes that are sequenced in the course of healthcare, will be made available for scientific research based on informed consent through a central databank. The data infrastructure provider and the data trustee are legally subordinate to the Federal Ministry of Health [33].

Greek privacy law contains an ad hoc legislation on health registries which states that during their establishment and operation, the Ministry of Health, which acts as the data controller, should always ensure the protection of human rights, privacy and the protection of personal data in accordance with Art. 9A of the Constitution, the national DPA and the GDPR. However, as indicated above, there is no specific regulation for biobanks which regulates the genetic analysis conducted within the framework of research.

Currently, the legal framework regulating specifically biobanks and databanks is rather vague. For example, in *Latvia*, results of genetic analysis that are carried out in the course of medical care are not included in the national biobank, the genome database of the Latvian population (Genome). These results, however, are retained as part of a patient's medical records. Results of genetic analysis that are carried out in the course of scientific research are generally included in the Genome (Sec. 8 para. 2 HGRL). However, if genetic analysis in the course of scientific research is carried out independently of the Genome, the information regarding the state of health of the person, tissue samples and

descriptions of the DNA shall be included in the Genome only with the gene donor's written consent (Sec. 8 para. 3 HGRL). Data protection modalities regarding research when research is carried out unrelated to the Genome is rather vaguely regulated and will often fall under the generic provisions regulating data protection.

In *Sweden*, results of genetic analysis executed in the course of medical care can only be available for the healthcare providers' employees with a professional healthcare-relationship with the affected patients (Sec. 2 Clause 4 PDA). Genomic databases and linking genomic data with health data could play an important role if the laws permit the use of technical possibilities for data linkage. However, the Swedish legislation does not permit sharing of collected data between different healthcare providers. Only medical staff with a care-relationship to the patient whose data is processed in the database can access patients' health data and it is not permitted to share such data. Results of genetic analysis that are carried out in the course of research can be registered in a database, where the participating parties in the specific research project have access (Sec. 24 Clause 1 PAISA).

2.7.2. Sharing data from electronic health records / e-Health systems for research purposes

In *Germany*, the electronic patient record (ePA) is being introduced to give patients full control over their health-related data. The legal basis for this processing is consent. Use of the ePA is voluntary for patients. The patient decides what data is stored in or deleted from the ePA. They determine who may access the ePA and can also delete the ePA altogether. Insured persons will be able to use their smart devices to determine who can access which document stored in the ePA. They can also release the data for research purposes, including particular research projects. This is made possible by the Research Data Centre that acts as an anonymisation and pseudonymisation centre as well as a trustee to make data available. However, it is not clear from the regulation, whether only scientific institutions in Germany can file access requests to conduct research with the data.

In *Greece*, all medical records can be accessed by the patient according to the Code of Medical Ethics and this right could be exercised after death by the individuals' heirs, as long as they are relatives up to the fourth degree. After the activation of their IEHR, data subjects can exercise their right to access the information contained in it in accordance with the provisions of Art. 15 GDPR. Patient data from e-health records can be used for research purposes according to Art. 84(4) of Law 4600/2019, provided that appropriate and specific measures to safeguard the fundamental rights and interests of the data subject are respected. The procedure of processing is not further regulated. Therefore, it will highly depend on the competent oversight bodies of the healthcare providers to authorize such access, once electronic health records are requested.

In *Latvia*, patient data that are stored in the e-Health system may be used for scientific research purposes (Para. 4 Clause 2 e-Health Regulation). However, the e-Health Regulation does not further specify modalities of that processing. Thus, the question of data access could be led back to the general rules on the processing of patient data in the e-Health system that are set out in Sec. 10 para. 52 LRP. Although this provision sets out several institutions as beneficiaries and purposes for the data processing in the e-Health system, it does not *expressis verbis* specify access to patient data for scientific research. This risks leading to practical difficulties accessing patient data in the e-Health system for scientific research purposes.

In *Sweden* patient data that are stored in the electronic health records may be used for scientific research purposes after permission has been granted by the Swedish Ethical Review Authority (see further elaboration in sec. 2.3. above). With this approval, the researcher may request the data needed for the specific study from the healthcare provider. The healthcare provider that is responsible for the medical record then must conduct the required risk assessment. This means that the authority must determine whether the information can be disclosed in the specific situation in question (Sec. 25 Clause 1 PAISA).

Currently, all four member states are in the process of establishing regulations for genomic databases and linking access rules to such databases to established data protection regulations. In the near future, specific rules for genomic data usage and for linkages of genomic data with other data can be expected. The further processing of data from e-health records is already regulated in the member states in a more detailed manner, either by defining specific rules, including opening up a balancing act to decide on access possibilities in a particular setting, or by referring back to the conditions defined by data protection law. However, these detailed rules regularly fail to clarify what central principles should guide their application in practice and the associated use of discretion. Accordingly, the divergences are also similar. Some models, nevertheless, might open up possibilities for better inter-European data sharing, such as data trustee models.

3. The disrupting and harmonizing effect of different opening clauses from a practical and legal perspective

The GDPR opening clauses are widely used, and the comparative insight shows clear lack of uniformity for health and genetic data sharing among different actors for purposes of healthcare and research. All four member states have general implementations of the GDPR as well as sector-specific rules that apply to healthcare and scientific research data processing and to data sharing within and between those areas. Taken together with the directly binding parts of the GDPR, it remains cumbersome to define the applicable law in individual member states. The legal techniques of implementation are similar in that they integrate different legal areas, for example, in Germany and Latvia, civil law rules related to the doctor-patient relationship, in Greece, ethics assessments, and they take the criminal law perspective on professional secrecy into account in all four countries. Because the affected areas and the regulatory structure are individual to member states, comparison of applicable laws relevant for data protection remains an exhausting legal task and requires extensive knowledge of the national legal framework.

The processing of special categories of data requires an exemption from the general processing ban. Therefore, the implementation of Art. 9 (2) and Art. 9(4) GDPR plays a crucial role for any data sharing. All analysed countries have a specific law or particular rules for at least one of the data types listed under Art. 9(4) GDPR, including health and genetic data, and in relation to one or more purposes listed under Art. 9(2) GDPR, including processing for healthcare or research purposes. The regulatory background has been described under section 2.1.

Typically, these laws regulate the processing of health and genetic data by various actors within the healthcare system, processing between healthcare and research, and various means of sharing data; e.g. by publication, upload in data banks or through different tools developed in the realm of emerging e-health systems as well as by sharing data with public actors. At the same time, they will regularly not have any particular provisions on cross-border sharing of these data types. Accordingly, the data concerned will regularly be subject to circumstances resulting from the exact justification drawn on based on member state law. If these rules leave room for weighing or interpretative decision-making, they might bring about different results with regard to the circumstances of data processing, leading to variation in the technical and organizational measures as well as safeguards guiding data processing. If partners from different countries act as joint controllers, this might lead to divergent obligations on how to process data possibly serving a shared purpose. Depending on the data protection roles assigned to partners involved in cross-country data sharing within the EU, one country's rules for a controller might even guide data in a way that they create obligations for data processors in another country. Applicable law might also be conveyed by access rules related to certain data that directly narrows down the circle of researchers and entities with access rights, or indirectly, by navigating access requesters through obligations defined by the respective national law.

In addition, the complex interplay of different laws as described in section 2.1. culminates in cross-border data exchange, where data processors have to consider the legal specificities of (at least) two countries. Taking the example of jointly conducted research projects, the mere complexity of the legal situation itself already poses a barrier for engaging in such projects, considering the liability for violations of the law and the effort involved in identifying the relevant legal norms. This might also be a result of the lack of legal norms that address cross-border data sharing.

Furthermore, specific data sharing rules are less common regarding genetic data. Often, such laws have not been made, as in Greece, or specific rules on genetic data processing date back to pre-GDPR times, as in Germany. These rules were not specifically mandated or could be upheld during the implementation of the GDPR because Art. 9(4) GDPR provides extensive room and full flexibility to member states to define their own rules for such data and already existing rules could be integrated into the data processing regulatory framework post-GDPR. At the time when these laws emerged, genetic data sharing was not the prominent issue it is today, which could explain why no special provisions were made in case such data should leave a country or be accessed from abroad.

In any case, the divergent conditions for various data processing as defined by the member states must be respected whether in sector-specific or general implementation laws [34].

With Art. 9(4), the GDPR contains an opening clause under which member states can positively derogate from the level of protection intended by the GDPR by imposing additional or stricter requirements. This clause is based on the fact that special public interests in the member states or legal positions of citizens that are worthy of protection can justify stricter data protection provisions within the scope of the GDPR in order to establish or maintain a higher sector- specific level of data protection [35]. If member states use this clause to create specific rules, they can strengthen the protection provided by the GDPR. Recital 53 of the GDPR states that Art. 9(4) GDPR rules imposed by member states should not hamper the free flow of personal data within the EU when those conditions apply to cross-border processing of such data. Already different national regulations require foreign controllers to adapt and thus negatively influence cross-border data sharing. Therefore, some support the idea that rules adopted pursuant to Art. 9(4) GDPR should only be applicable for domestic controllers [36].

Without any explicit mandate but by creating the possibility to derogate by directly addressing the member states, Art. 9(2) GDPR has a similar effect and allows member states to actively deviate from the provisions of the GDPR and adopt or maintain specific conditions under national law for the processing of special categories of personal data based on different exceptions listed by the GDPR.

Examples cover data processing elaborated for healthcare (2.2.) or scientific research purposes (2.3.), as well as the further processing of data from healthcare settings for research, including from e-health records (2.7.).

It is not always clear, whether sector-specific rules in member states implement Art. 9(2) provisions or Art. 9(4) GDPR. Because member states are free to use Art. 9(4) GDPR, the harmonizing effect of the standards defined by GDPR under Art. 9(2) GDPR to allow special data categories' processing and the framework of main conditions defined become insofar meaningless as health and genetic data within the meaning of Art. 9(4) GDPR are concerned. Factually, this reduces the harmonizing effect of Art. 9(2) and altogether hinders more than it promotes cross-border data sharing.

Besides the exception for processing special categories of data, a legal basis is needed. Using Art. 6(2) and (3), member states are free to define specific provisions to adapt the application of the GDPR rules regarding processing for compliance with controllers' legal obligations and for tasks carried out in the public interest by determining specific requirements for processing and other measures to ensure lawful and fair processing. Art. 6(3) sentence 3 of the GDPR contains a list of examples that might fall under such rules including the types of data which are subject to the processing, the data subjects concerned and limitations on disclosure and storage periods. Based on the opening clauses of Art. 6(2) and (3) GDPR, the member states may enact specific data protection provisions for each public task defined. By only looking at the list, any sharing of data in the public domain could be severely affected by these rules. Section 2.6. lists the main fields of data processing that fall under public interest and are manifested in a public task defined by national laws. The scope of this norm is enormous beyond these exemplary areas because it potentially covers all area-specific data protection law in the public sector and thus, potentially, all data processing activities by public entities in the health sector. The scope of application might be even wider in member states where public and private healthcare providers are interwoven, such as in Sweden. Also, by strengthening research within the realm of public interest, rules on the legal basis of data processing for this purpose might be widened.

In addition, according to Art. 85(1) GDPR, there is a mandate for member-state regulation to ensure a balance between the conflicting right to protection of personal data with the freedom of press, freedom of expression and freedom of information, which in most member states covers the publication of scientific research results. These rules have been elaborated under section 2.5. While member states have very broad room to implement such rules, their basic understanding of privacy will apply to limiting publication of personal data. Those countries demonstrating acceptance of relative anonymity (Latvia, Greece) might have different publication rules than countries mostly adhering to a concept of factual anonymisation (Germany). Again, in the case of cross-border research, research results containing personal data that was shared across different member states might only be published in some member states but not in others due to different concepts of anonymity.

Additionally, either as explicit room for deviation from a minimum standard (Art. 9(2)(h), (i), (j) GDPR) or as an explicit mandate to create rules at all (Art. 85 GDPR), scientific research data processing will be subject to a weighing of competing rights and interests conducted by the member states. This has been elaborated in detail under section 2.3. Such balancing and the necessity test will be guided by the weighing practice of member states. The same goes for the limitations of data subjects' rights where guidance on the balancing that must be done between the competing fundamental rights in the context of scientific research is subject to member state specificities, creating divergent operationalization of the fundamental right to data protection in the end. Altogether, opening clauses allow member states to provide for derogations by national law that strengthen protection or to allow derogations that reduce protection under the strict conditions of an interest-based solution for conflicting fundamental rights positions. They are the result of the subsidiarity and proportionality principles of EU law, and will continue to lead to divergence in the standard of data protection law between the member states even if it does not impair the general harmonising effect of the GDPR as framed by its Art. 5.

Such regulatory mandates are further extended by clauses that, firstly, explicitly refer to already existing member state rules such as those related to professional confidentiality. Such an example is the exception of data processing for healthcare purposes under Art. 9(2)(h) GDPR, described in section 2.2. This rule mandates processing by or under the responsibility of a professional subject to the obligation of professional secrecy. Secondly, an extension is achieved by clauses that explicitly mandate the non-applicability of the provisions of the Regulation in case of specific existing EU or member state law. Such provisions serve a uniform regulatory structure in that they hinder derogations from principles communicated by opening clauses by other restrictions and obligations of the GDPR. A prominent example of such a rule is Art. 14(5)(c) GDPR, which limits information obligations towards data subjects if data has not directly been obtained from them. This opening clause provides room for a severe limitation of data subject rights', as limiting transparency will limit the exercise of individual rights such as the right to erasure or the right to restrict processing.

Based on this rule, standardized transparency provisions in the context of cross-border data sharing are going to be difficult to achieve.

Altogether, further harmonization for the processing of genomic and health data will depend on the exact regulatory area in question and which opening clauses these are related to according to the GDPR, as well as whether member states are mandated to deviate, are allowed to deviate or data protection rules relate to areas, where member state rules should be respected. One example for the last type of opening clause are criminal codifications of professional secrecy rules that can have various effects on member state's data protection rules, e.g. blocking data sharing, mandating consent for data disclosure or by simply remaining attached as a limitation to the data as it is shared among public actors.

4. EU regulatory activities for the European Health Data Space

4.1. The European Health Data Space

As illustrated above, the national rules on the processing and exchange of health and genomic data of the four EU member states subject to this analysis differ from each other in multiple aspects. As this plurality of rules may impair the access to and exchange of such data in the EU, the questions arise, which paths to harmonization are viable/open and which means might have promising effects. Accordingly, a regulation planned as the framework legislative act for the EHDS could be based on Art. 114 TFEU, promoting the functioning of the internal market [37].

The European Health Data Space (EHDS), anchored in the European Data Strategy, aims to enable an efficient exchange of and direct access to different health data across the Union in compliance with data protection regulations, in particular the GDPR [38]. It is intended to benefit patients and healthcare providers on the one hand, and researchers and policy makers on the other [39]. Thus, the use of health data is to be enabled for three purposes: health care (so-called primary use), health research and health policy (so-called secondary uses). The EHDS is to be built on three pillars: the creation of a unified governance system for the Health Data Space and clear rules for data exchange (pillar 1), the guarantee of high data quality and technical as well as semantic interoperability between infrastructures (pillar 2), and the development of digital infrastructures (pillar 3). As for the regulatory subject matter, the design of the rules for data exchange is of particular relevance.

4.2. Planned governance and regulatory action

Within the EHDS, different data governance systems are envisaged for health data processing for healthcare purposes on the one hand and for secondary use of health data on the other. The data governance for the primary use of health data (healthcare) is to be taken over by the existing eHealth Network [40]. The eHealth Network is a voluntary network of Member State authorities responsible for eHealth and was created by the Patients' Rights Directive [41]. Together with the European Commission, the eHealth Network has set up a digital infrastructure for the cross-border exchange of health data for certain eHealth services (eHDSI) [42], in which so-called national contact points act as communication interfaces between national eHealth systems and thus as mediators for data exchange [43]. In the context of the creation of the EHDS, the European Commission is considering building on this infrastructure [44] and extending existing (or evolving) cross-border health services (e.g. the transmission of medical images, lab results and hospital discharge reports) [45]. The introduction of national contact points has so far been voluntary, but could become mandatory in the course of the establishment of the EHDS [46].

National and European governance mechanisms are envisaged within the framework of a governance system for the secondary use of data [47]. The structure of data governance is to be based on the future Data Governance Act, which is to be supplemented by sector-specific law [48]. So-called EHDS nodes are to be established and interconnected as access points to the EHDS [49]. They are intended to intertwine national and EU governance mechanisms by representing the entry points to the EHDS and via which national and EU bodies communicate on a cross-border level [50]. Other institutions, e.g. research infrastructures or health authorities could also be connected via these [51].

In order to create clear rules for the processing of health data in such a network, the European Commission plans to develop a Code of Conduct for the secondary use of health-related data [52], which can be declared generally binding throughout the Union by the Commission in accordance with Art. 40(9) GDPR. This could be used to establish uniform interpretation guidelines and rules on central data protection concepts of the GDPR on a sector-specific basis, e.g. on the technical standards for anonymization and pseudonymization of health data, the nature and form of consent (especially in processing for scientific research with regard to recital 33 of the GDPR), or the implementation of joint responsibility (Art. 26 GDPR). At the same time, the Code of Conduct is intended to provide clarity to patients about the consequences of consenting to the use of their health data and what this means in practice [53].

In addition, the Commission is considering establishing uniform data governance principles and health data accessibility through specific EU legislation [54]. However, it is not clear from the documents available in what form the requirements for access to data in the EHDS will be defined. It is also still unclear to what extent the regulations on the (further) processing of health data, which differ at national level, are to be harmonized by secondary legislation. In view of the Union's regulatory competence under data protection law, Art. 16(2) TFEU, this would only be possible for data processing that falls within the scope of Union law, but not for data processing by public authorities of the member states without any reference to Union law. It is also not yet known to what extent the member states themselves can decide which data they make available for secondary use across borders within the framework of the EHDS. The regulation on data governance, which sets the framework for all European data spaces, leaves the right to legislate on access to public sector information with the member states [55]. The same is likely to be expected for the proposed regulation on EHDS.

4.3. Conclusions for the planned regulatory action from the perspective of opening clauses

The described regulatory diversity is detrimental to the availability and Union-wide exchange of health and genetic data – a prerequisite for the promotion of digital technologies in healthcare and building European infrastructures including on a federated level. In this respect, there is a need for harmonization, and with Article 16(2) TFEU, there is also a basic competence to proceed.

4.3.1. Further EU harmonization by new secondary acts

One might ask to what extent the Union is authorized to harmonize within the framework of shared competence if it has previously expressly allowed the member states to introduce of their own rules by means of opening clauses. Art. 2 TFEU makes no explicit provision for this case. In the area of shared competence, the member states can only act insofar as the Union has not exercised its competence. If the Union decides to no longer exercise its competence (Art. 2(2) 3 TFEU), member state competence is revived. According to Declaration No. 18 on the delimitation of competences, this is the case when the Union repeals a legislative act [56]. However, this does not mean that future action by the Union in the area of shared competence is excluded if such action satisfies the principles of subsidiarity and proportionality [57]. Even regulations adopted in the meantime by the member states in the area of the repealed legislative act cannot change this. Yet if existing national regulations cannot stand in the way of the Union exercising its competence, it must also be possible for the Union to harmonize in areas of shared competence where national regulations already exist on the basis

of an opening clause. The regulatory competence under data protection law, which is limited to the scope of application of Union law, is predominantly understood in a broad sense. In the context of the EHDS, data processing should regularly take place across borders and data is to be exchanged, among other things, for the purpose of cross-border healthcare and scientific research as well as the development of a competitive internal market for digital healthcare services, so that these fall within the scope of Union law. If the Union intends to establish uniform data processing rules for the EHDS, it could close the existing opening clauses by secondary law in this respect. However, such secondary legislation cannot be adopted without the Council and thus the consent of the member states (cf. Arts. 289(1), 294 TFEU).

4.3.2. *The possibility of overcoming divergences through a Code of Conduct*

Within the framework of the EHDS, the development of a Code of Conduct as described in Art. 40 GDPR for the primary and secondary use of health data is currently being considered. This is intended to give data processors in the healthcare sector more clarity and guidance in the application of the EU data protection rules. A Code of Conduct can be declared generally applicable by the Commission in the form of an implementing act as tertiary legislation, Article 40(9) GDPR. Although controversial [58], it is convincingly considered to have normative effect [59], so that data controllers who fall within the scope of a Code of Conduct, as well as courts and authorities, are bound by it [60]. However, the harmonization potential of a Code of Conduct is limited; the legal provisions enacted by the member states in fulfilment of the opening clauses cannot be changed or replaced by a Code [61]. Codes of Conduct are primarily an instrument to enable associations or other federations to specify the GDPR for the area the respective data controllers are active in. On the one hand, these clarifications must be compatible with the GDPR (cf. Art. 40(5) sentence 2 GDPR), but on the other hand, they must also be compatible with the relevant national laws [62]. This conformity requirement precludes harmonization of national regulations. It would otherwise be possible to amend the data protection laws of the member states without involving a national or Union legislative body, as the Commission is responsible for declaring the general bindingness of the Code of Conduct (cf. Art. 40(6-10) GDPR on the procedure for declaring a Code of Conduct generally binding). Such far-reaching legislative powers of the Commission were precisely excluded in the legislative procedure for the adoption of the GDPR [63]. Harmonization of national regulations on the (secondary) use of health data for data processing in the EHDS cannot take place in this way [64]. Nevertheless, the Commission considers a Code of Conduct to be a useful instrument to specify essential terms of European data protection law, e.g. anonymization and pseudonymization, type and form of consent in a binding manner [65], and to this extent to enable a uniform application of the rules of the GDPR. A lack of harmonization can thus be partially compensated [66].

Indeed, missing harmonization is partially due to the unclear and vague terms of the GDPR, such as anonymization, of which conceptually different interpretations prevail in the member states, cf. relative anonymity mentioned in sections 2.3. and 2.5. related to Greece and Latvia, as opposed to a more absolute concept, prevailing in Germany, cf. 2.7. Additionally, in some cases, pseudonymization is considered in its legal effect as anonymization, cf. 2.5. related to publications in Greece. The process and design of consent to the processing of genomic and health data also seems a good target for further harmonization, as it is the legal ground for exception for the processing of special data categories that can be applied directly based on the GDPR. These targets for their specific regulation seem appropriate based on the potential for harmonization through a Code of Conduct elaborated above.

However, setting up the drafting team and clarifying the drafting processes of such a Code would have to be guided by exceptional care in order to set the frame for its material appropriateness and substantive success, as there exists no specific example for a successful Code for the healthcare sector yet.

4.3.3. *Potential for further harmonization?*

Opening clauses can have different harmonising effects. Art. 9(4) and Art. 85 GDPR represent specific clauses that provide member states full flexibility to deviate from the GDPR standard and create own rules. These are different in their influence on harmonization than most of the possibilities for explicit derogations from main rules, e.g. regarding data subjects' rights, or clauses that allow member states to design general rules in more detail, such as in relation to Art. 9(2) GDPR. The application of latter clauses is already subject to standardised conditions of the GDPR. However, the regularly required weighing of competing rights and interests in the realm of their application can attract regulatory attention from member states that are guided by their national approaches within the context of fundamental rights protection. Where the application of the regulation is limited in that it refers to member-state rules, regularly those fields are affected which lie within the regulatory competence of member states. Their inclusion through references in opening clauses of the GDPR are of particular relevance to foster coherence with neighbouring regulatory fields that might be subject to pure member state competence.

While a regulatory act creating new secondary law might be inevitable to provide for the functioning of the EHDS, particularly due to Art. 9(2) and Art. 85 GDPR, a Code of Conduct could have more benefits towards a gentle approximation of member states approaches. Besides defining undefined, crucial terms within the GDPR, such as healthcare, a Code's greatest achievement could be to further specify the application conditions of those opening clauses of the GDPR that allow member states to define more detailed or derogative rules. This way, the context-specific minimal standard for building the EHDS and bringing it to life by data sharing could be realized. Along those lines, the effect of regulations on data sharing that fall within the sole competence of member states could be more clearly identified and dealt with in the context of European data sharing. In this way, possible sector-specific harmonization through a Code would lead to better communication among member states' regulatory solutions that cannot be harmonized through a Code, in that the provisions they define for data processing could be understood in the same way across borders, even if they in themselves impose different conditions and obligations.

Such an approximation might be enough to maintain member states' specificities in health and genetic data regulation which are strongly rooted in their constitutional law traditions, and allow them to continue to be respected in a federated European health data infrastructure while providing a continuously high-level and transparent protection of data subjects' rights, enabling up-to-date cross-border digital healthcare and the reuse of health and genetic data for various purposes – with particular emphasis on scientific research – all in a common, European interest, motivated by all-inclusive fundamental rights protection.

Data availability

Data will be made available on request.

Authors' contributions

FMG and JS drafted the manuscript. Information on the regulations in the member states have been provided by FMG for Germany, by SP and KN for Sweden, by SS for Latvia and by OT for Greece. All authors providing information on member states' regulation have carefully reviewed the drafting of their presentation. SS has commented on several draft versions of the text. All authors have commented on the final and the revised draft and have approved the final manuscript prior to submission.

Transparency document

The Transparency document associated with this article can be found in the online version.

Declaration of Competing Interest

The authors declare that they have no competing interests.

Acknowledgments

SP and KN acknowledge Genomic Medicine Sweden (GMS) support provided by the Swedish Innovation Agency Vinnova, participating University Hospitals and Medical Faculties of the GMS seven nodes, and strategic innovation agency SweLife (part of Vinnova). FMG acknowledges funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 825835, EUCANCan: a federated network of aligned and interoperable infrastructures for the homogeneous analysis, management and sharing of genomic oncology data for Personalised Medicine. FMG & JS are funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – NFDI 1/1 "GHGA – German Human Genome-Phenome Archive".

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
[2] F. Molnár-Gábor, Data protection, in: R. Grote, F. Lachenmann, R. Wolfrum (Eds.), Max Planck Encyclopedia for Comparative Constitutional Law, Oxford University Press, Oxford, 2017.
[3] DG Food and Health Safety, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.
[4] (a)Cf., for example: D. Peloquin, M. DiMaio, B. Bierer, M. Barnes, Disruptive and avoidable: GDPR challenges to secondary research uses of data, Eur. J. Hum. Genet. 28 (June (6)) (2020) 697–705, https://doi.org/10.1038/s41431-020-0596-x. (b) S. Bensemmane, R. Baeten, Cross-Border Telemedicine: Practices and Challenges, OSE Working Paper Series, Research Paper No. 44, European Social Observatory, Brussels, 2019, 63p.
[5] DG Food and Health Safety, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.
[6] European Commission, European Health Data Space, European Commission. https://ec.europa.eu/health/ehealth/dataspace_en.
[7] O. Tzortztaou, S. Slokenberga, J. Reichel, A. da Costa Andrade, C. Barbosa, S. Bekaert, et al., Biobanking across Europe post-GDPR: a deliberately fragmented landscape, in: O. Tzortztaou, S. Slokenberga, J. Reichel (Eds.), GDPR and Biobanking Individual Rights, Public Interest and Research Regulations across Europe, Law, Governance and Technology Series, vol. 43, Springer, Berlin, 2021, pp. 397–420.
[8] (a)Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 12 of the Act of 20 November 2019 (Federal Law Gazette I, p. 1626).
(b)For further nuances, cf. § 1 BDSG; BT-Drs. 18/11325, p. 79 et seq.
(c)The prevailing opinion refers to: S. Sosna, Daten- und Geheimnisschutz bei Outsourcing-Projekten im Krankenhausbereich, Nomos, Baden-Baden, 2015 p. 45 et seq., with further references.
(d)With regard to specific sector-related law, cf. B. Buchner, M.-Th. Tinnefeld, § 27 BDSG, in: J. Kühling, B. Buchner (Eds.), BDSG, 3rd ed., C.H. Beck, München, 2020 recital 26.
[9] Patient Data Protection Act of 14 October 2020 (Federal Law Gazette I p 2115).
[10] Genetic Diagnostics Act of 31 July 2009 (Federal Law Gazette I p. 2529, 3672), as last amended by Article 15 (4) of the Act of 4 May 2021 (Federal Law Gazette I p. 882).
[11] Hellenic Data Protection Authority (HDPA), measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions, Law 4624/2019 (Government Gazette, Series A, Issue N 137, p. 3379).
[12] Code of Medical Deontology, Law 3418/2005 (Government Gazette, Series A, Issue N. 287, p. 5391).
[13] Personal Data Processing Law (Fizisko personu datu apstrādes likums – in Latvian) Latvijas Vēstnesis, 132, 04.07.2018.
[14] (a)Law on the Rights of Patients (Pacientu tiesību likums) Latvijas Vēstnesis, 205, 30.12.2009.
(b)Human Genome Research Law (Cilvēka genoma izpētes likums) Latvijas Vēstnesis, 99, 03.07.2002.
[15] Patient Data Act (2008:355).
[16] Public Access to Information and Secrecy Act (2009:400).
[17] Freedom of the Press Act (1949:105).
[18] Ethical Review Act (2003:460).
[19] Act on biobanks in health care (2002:297).
[20] F. Molnár-Gábor, Medical data protection. Nomos Commentary on Medical Criminal Law, Nomos, Baden-Baden, 2022 forthcoming.
[21] O. Tzortztaou, A. Siapka, Mapping the biobank landscape in Greece, in: O. Tzortztaou, S. Slokenberga, J. Reichel (Eds.), GDPR and Biobanking Individual Rights, Public Interest and Research Regulations across Europe, Law, Governance and Technology Series, vol. 43, Springer, Berlin, 2021, pp. 291–308.
[22] European Data Protection Supervisor, EDPS Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to Protection of Personal Data, 2019. https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.
[23] S. Slokenberga, Setting the foundations: individual rights, public interest, scientific research and biobanking, in: O. Tzortztaou, S. Slokenberga, J. Reichel (Eds.), GDPR and Biobanking Individual Rights, Public Interest and Research Regulations across Europe, Law, Governance and Technology Series, vol. 43, Springer, Berlin, 2021, pp. 11–30.
[24] Cf, P. Schantz, H.A. Wolff, Das neue Datenschutzrecht, C.H. Beck, München, 2017, p. 135.
[25] Datenschutzkonferenz, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs "bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO; 3. April 2019.
[26] Cf. only P. Schantz, H.A. Wolff, Das neue Datenschutzrecht, C.H. Beck, München, 2017, p. 364 et seq.
[27] S. Slokenberga, You can't put the genie back in the bottle: on the legal and conceptual understanding of genetic privacy in the era of personal data protection in Europe, BioLaw Journal – Rivista di BioDiritto 1 (2021) 223–250. Special Issue.
[28] S. Simitis, § 40 BDSG, in: S. Simitis (Ed.), BDSG, 7th ed., Nomos, Baden-Baden, 2011 recital 79.
[29] P.C. Johannes, Art. 25 BayDSG, in: M. Schröder (Ed.), Bayerisches Datenschutzgesetz, Nomos, Baden-Baden, 2021 recital 39.
[30] N. Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, Law Innov. Technol. 10 (2018) 40–81, https://doi.org/10.1080/17579961.2018.1452176.
[31] F. Molnár-Gábor, J. Korbel, Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall? EMBO Mol. Med. 12 (2020), e11421.
[32] German Human-Genome Phenome Archive, https://ghga.dkfz.de/.
[33] Gesetz zur Weiterentwicklung der Gesundheitsversorgung (Gesundheitsweiterentwicklungsversorgungsgesetz) v. 11. Juli 2021, BGBl. 2021 I p. 2754 (Art. 1 Nr. 18 b, introducing § 64e para. 9 into SGB V).
[34] In the meantime, there exist extensive typologies of the opening clauses. Here, the differentiation is made re: facultative and non-facultative clauses as well as re: member states' margin of manoeuvre by the implementation.
[35] M. Müller, Die Öffnungsklauseln der Datenschutzgrundverordnung, readbox unipress in der readbox publishing GmbH, 2018, p. 98.
[36] P. Schantz, H.A. Wolff, Das neue Datenschutzrecht, C.H. Beck, München, 2017, p. 226.
[37] D.G. Santé, Combined Evaluation Roadmap/Impact Assessment European Health Data Space, Ares, 2020, 7907993, 23.12.2020, p. 1.
[38] European Commission, Communication 19.2.2020, COM(2020) 66 final, A European Data Strategy, p. 5.
[39] DG Santé, 3.1 European Health Data Space, Presentation 18th eHealth Network, 12-13 November 2020, https://ec.europa.eu/health/ehealth/events/ev_20201112_en (Meeting Documents/Presentations).
[40] eHealth Network, Summary Report of the 18th eHealth Network Meeting, p. 3, https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20201112_sr_en.pdf.
[41] European Data Protection Supervisor. Preliminary Opinion 8/20 on the European Health Data Space, p. 7.
[42] European Data Protection Supervisor. Preliminary Opinion 8/20 on the European Health Data Space, p. 7.
[43] eHealth Network, 9. https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20160607_co05_03_en.pdf.
[44] D.G. Santé, Combined Evaluation Roadmap/Impact Assessment European Health Data Space, Ares, 2020, 7907993, 23.12.2020, p. 5.
[45] European Commission, https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.
[46] DG Food and Health Safety, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.
[47] D.G. Santé, 1.1 European Health Data Space, Presentation 19th eHealth Network, 3-4 June 2021, https://ec.europa.eu/health/ehealth/events/ev_20210603_en (Meeting Documents/Presentations).
[48] European Commission, COM(2020) 767 final, 25.11.2020, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 2, p. 11.
[49] D.G. Santé, 3.1 European Health Data Space, Presentation 18th eHealth Network, 12–13 November 2020, https://ec.europa.eu/health/ehealth/events/ev_20201112_en (Meeting Documents/Presentations).
[50] D.G. Santé, 1.1 European Health Data Space, Presentation 19th eHealth Network, 3–4 June 2021, https://ec.europa.eu/health/ehealth/events/ev_20210603_en (Meeting Documents/Presentations).
[51] Id.
[52] (a) DG Food and Health Safety, Assessment of the EU Member States' rules on health data in the light of GDPR, 2021, p. 131, https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf;
(b) European Data Protection Supervisor, Preliminary Opinion 8/2020 on the European Health Data Space, 2020, p. 8 et seq., recital 17.

[53] DG Health and Food Safety, id., p. 132 et seq.
[54] DG Health and Food Safety, id., p. 133 et seq.
[55] European Commission, COM(2020) 767 final, 25.11.2020, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), p. 3.
[56] Declarations annexed to the final Act of the Intergovernmental Conference, 26.10.2012, OJ C 326/337, 18. Declaration.
[57] Ch. Calliess, Kompetenzen der Europäischen Union und ihre Ausübung im Lichte des Subsidiaritätsprinzips, in: P. Beckert, B. Lippert (Eds.), Handbuch Europäische Union, Springer, Berlin, 2020, pp. 567–596 (573).
[58] V. Jungkind, Art. 40 DS-GVO, in: S. Brink, H.A. Wolff (Eds.), BeckOK Datenschutzrecht, 25th ed., C.H. Beck, München, 2018 recital 32 et seq.
[59] N. Reifert, Codes of Conduct nach der DS-GVO. Ein Mittel für mehr Rechtssicherheit auf europäischer Ebene? ZD 9 (2019) 305–310 (309).
[60] B. Paal, L.K. Kumkar, Art. 40 DS-GVO, in: B. Paal, D.A. Pauly (Eds.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 3rd ed., C.H. Beck, München, 2021 recital 28a.
[61] DG Food and Health Safety, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.
[62] European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0, 2019, p. 15 recital 29.
[63] M. Müller, Die Öffnungsklauseln der Datenschutzgrundverordnung, readbox unipress in der readbox publishing GmbH, 2018, p. 173 et seq.
[64] F. Molnár-Gábor, J. Korbel, Genomic data sharing in Europe is stumbling—Could a code of conduct prevent its fall? EMBO Mol. Med. 12 (2020), e11421.
[65] DG Food and Health Safety, Assessment of the EU Member States' Rules on Health Data in the Light of GDPR, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf.
[66] European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0, 2019, p. 5 recital 1.