BRILL | NIJHOFF

EUROPEAN JOURNAL OF HEALTH LAW (2025) 1–32

European Journal of Health Law

brill.com/ejhl

Mass-Scale G2B Data Sharing in an Emergency: between the GDPR, Data Governance Act, and European Health Data Space

Andrea Parziale | ORCID: 0000-0002-3091-0705
Institute of Law, Politics and Development (Dirpolis), Sant'Anna School of Advanced Studies, Piazza Martiri della Libertà 33, 56127 Pisa, Italy
Corresponding author
andrea.parziale@santannapisa.it

Elisabetta Pulice | ORCID: 0000-0002-2423-8908
Faculty of Law, University of Trento, Via Verdi 53, 3812 Trento, Italy
elisabetta.pulice@unitn.it

Deborah Mascalzoni | ORCID: 0000-0003-4156-1464
Eurac Research, Viale Druso/Drususallee 1, 39100 Bolzano/Bozen, Italy
Centre for Research Ethics and Bioethics (CRB), Uppsala University, Husargatan 3, Uppsala, Sweden
deborah.mascalzoni@eurac.edu

Received 28 February 2025 | Accepted 12 October 2025 | Published online 19 November 2025

Abstract

During the COVID-19 pandemic, government-to-business (G2B) data sharing became a vital practice, exemplified by the 2021 Israeli Ministry of Health-Pfizer agreement. This established a large-scale data sharing operation outside of research and data protection regulations and oversight. This paper explores two related questions: (i) whether an EU Member State could replicate this scenario, and (ii) whether EU data legislation provides sufficient protection against excessive G2B data sharing. The analysis of the General Data Protection Regulation, Data Governance Act, and European Health Data Space shows that (i) despite the uncertain definitions of research and personal data, it would be difficult for an EU Member State to replicate this scenario; and (ii) despite its many grey areas and flexibilities, EU data legislation offers protection against excessive

Published with license by Koninklijke Brill BV | DOI:10.1163/15718093-BJA10158
 | ISSN: 0929-0273 (print) 1571-8093 (online)

G2B data sharing. This highlights the need to explore alternative strategies to facilitate data sharing that can address public health emergencies promptly while safeguarding fundamental rights.

Keywords

Data Governance Act – data protection – European Health Data Space – G2B data sharing – GDPR – health data – public health emergencies – regulatory oversight

1 Introduction

During the COVID-19 emergency, numerous data-sharing collaborations between public and private entities were set up to fight the pandemic,[1] including government-to-business (G2B) data transfers.[2] This is well illustrated by the agreement made in January 2021 between the Israeli Ministry of Health (MoH) and Pfizer, whereby the former agreed to share epidemiological data on the vaccination campaign with the latter, in exchange for prioritised access to Covid-19 vaccine doses.[3] As will be seen in more detail below, the Israeli government managed to keep this agreement out of the scope of national research and personal data protection regulations alike. This means that the data was shared without individuals' consent or independent review by ethics committees or data protection authorities.

The Israel–Pfizer agreement received mixed reactions. Some commentators noted that prioritised access to COVID-19 vaccines likely contributed to the rapid success of the Israeli vaccination campaign, thus contributing to the achievement of an important public health benefit for the Israeli population.[4]

1 F. Gao, L. Tao, Y. Huang and Z. Shu, 'Management and Data Sharing of COVID-19 Pandemic Information', *Biopreservation and Biobanking* (2020) 570–580; R.A. Romero and S.D. Young, 'Ethical perspectives in sharing digital data for public health surveillance before and shortly after the onset of the Covid-19 pandemic', *Ethics & Behavior* 32(1) (2021) 22–31.

2 S. Aidinlis, 'Government-to-business (G2B) research data sharing and the GDPR: Reconciling the 'public' with the 'private'?', in: E. Kosta, R. Leenes and I. Kamara (eds.), Research Handbook on EU Data Protection Law (Cheltenham: Edward Elgar, 2022) pp. 115–142.

3 *Real-world epidemiological evidence collaboration agreement*, available online at www.gov.il/BlobFolder/news/17012021-02/he/files_publications_corona_pfizer_agreement.pdf (accessed 12 September 2025).

4 D. Estrin, 'Vaccines For Data: Israel's Pfizer Deal Drives Quick Rollout — And Privacy Worries', *National Public Radio* (31 January 2021) available online at, https://text.npr.org/960819083 (accessed 12 September 2025).

On the other hand, advocacy groups, along with sympathetic media outlets, expressed concerns over the potential risks of mass-scale sharing of data by a government to a multinational corporation.[5]

This article uses the Israel–Pfizer agreement as a case study to investigate, from a European perspective: (i) whether the government of an EU Member State willing to follow the example of Israel could effectively circumvent personal data protection and research regulations and avoid independent scrutiny; and, if the answer to the first question is negative, (ii) whether the evolving EU legal framework for G2B data sharing provides adequate protection against excessive mass-scale data sharing operations. Conversely, the present article does not intend to assess the legality of the specific Israel–Pfizer agreement under Israeli law. It should be noted that analysing a third-country agreement through the lens of EU law may have interpretive constraints that affect the generalisability of the conclusions, as different legal frameworks and definitions may apply in the jurisdiction where the original agreement was concluded.

To answer these questions, the role of Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR), Regulation (EU) 2022/868 (Data Governance Act, DGA), and Regulation (EU) 2025/327 establishing the European Health Data Space (EHDS Regulation) in the sharing of data is discussed extensively, particularly in connection to the processing of data for scientific research, in the public interest, and for public health.

2 The Israel–Pfizer Agreement: Contents and Concerns

In essence, under the agreement concluded between the Israeli MoH and Pfizer in January 2021 (the Israel–Pfizer agreement), the former committed to sharing data on the national vaccination campaign against Covid-19 to the latter, in exchange for prioritised access to vaccine doses. Initially kept confidential, a partially redacted version was eventually published following calls for transparency from advocacy groups.[6]

In particular, under this agreement, the MoH committed to transmitting 'aggregate epidemiological data' to Pfizer (Section 2.4 and Exhibit B). As per

5 M. Birnhack, 'Who Controls Covid-Related Medical Data? Copyright and Personal Data', *International Review of Intellectual Property and Competition Law* 52 (2021) 821–824.

6 I. ben Zion, 'Israel's data-for-vaccines deal with Pfizer raises privacy concerns', *Times of Israel* (18 January 2021), available online at www.timesofisrael.com/israels-data-for-vaccines-deal-with-pfizer-raises-privacy-concerns/ (accessed 12 September 2025).

the exhibits A and B attached to the agreement, the transferred data include, 'at a minimum', weekly counts of confirmed COVID-19 cases (by age groups, and other demographic factors), hospitalisations, severe or critical cases, ventilator use, deaths, symptomatic cases, vaccines, as total and by age and 'other demographic subgroups'. The aim is to 'measure and analyse epidemiological data arising from [the vaccination campaign], to determine whether herd immunity is achieved, reaching a certain percentage of vaccination coverage in Israel' (Section 2.1). The MoH and Pfizer will analyse the data jointly (Section 3).

MoH 'anonymises' the data, and identifiable information shall not be disclosed (Section 5.2). If identifiable data is, in fact, disclosed, Pfizer committed to immediately returning such data for the MoH to destroy it (Section 5.2).

At the same time, Pfizer is excluded from using the data provided by the MoH in a way that does not improve healthcare and public health or that has any inappropriate social purpose, such as insurance or employment discrimination (Section 7.8). Pfizer also committed to refraining from any activities that might expose individuals' identity or identifying data, e.g., by de-anonymising or re-identifying the data (Section 7.8).

In exchange for the data transferred to Pfizer, Israel obtained prioritised access to Pfizer's COVID-19 vaccines. This was, however, without a direct economic return. In fact, Israel reportedly paid more for the vaccines than other high-income countries.[7]

This agreement sparked quite a debate in Israel. The Israeli Supreme Helsinki Committee for Clinical Trials in Humans (the Israeli committee for clinical trials) claimed that the data-sharing project involving Pfizer was subject to the committee's approval under Israeli research regulations and thus required prior ethics review.[8] The MoH disagreed, arguing that its real-world epidemiological evidence collaboration with Pfizer did not set up any 'clinical trial' over which the ethics committee have jurisdiction.[9] Also, privacy and data protection concerns were dismissed as only statistical data were to be shared.[10]

7 O. Dyer, 'Covid-19: Countries are learning what others paid for vaccines', *British Medical Journal* 372 (2021) n281.

8 H. Ravia, D. Hammer and A. Shoval, 'Israel Discloses its Agreement with Pfizer for De-identified COVID-19 Vaccine-related Health Data', *Lexology* (31 January 2021), www.lexology.com/library/detail.aspx?g=646of968-2862-4e0e-8b89-a52299cdf0a6 (accessed 12 September 2025).

9 *Ibid.*

10 D. Estrin, 'Vaccines For Data: Israel's Pfizer Deal Drives Quick Rollout — And Privacy Worries', *NPR* (31 January 2021), available online at https://www.npr.org/2021/01/31

That being said, these two arguments in defence of the agreement seem, at least, debatable. Regarding the argument that the data sharing operation set up by the agreement is not a clinical trial, it can be argued that the operation in question may still qualify as a kind of non-interventionist, observational research, which would be subject to research regulation and independent review.

Regarding the argument that only statistical data is shared, it can be argued that even the sharing of aggregated data may lead to the (re-)identification of individuals if a sufficient number of segmentation criteria are used.[11] Research on re-identification attempts with health data has demonstrated that seemingly anonymous datasets can be re-identified through various techniques, including differential attacks, auxiliary information correlation, and statistical inference methods.[12] In this respect, two reasons make the risk of (re-)identification more than mere speculation in the case of the Israel–Pfizer agreement.

First, it is unclear what data is actually shared. The exhibits list the categories of data that, 'at a minimum', will be transferred. The expression 'at a minimum' suggests that further, unspecified data might be shared with the recipient company.

Secondly, the agreement states that the data to be shared is indicated as totals and divided by age and other unspecified demographic subgroups. While it may be impossible to identify an individual through segmentation by age or gender alone, segmentation by age, gender, place of residence, and underlying diseases, for example, could potentially reveal the identity of the vaccinated individual. Indeed, several provisions of the agreement assume that the data provided might, in fact, be re-identified. For example, as noted above, section 5.2 of the Israel–Pfizer agreement states that, if identified data is shared, Pfizer must immediately return it to the MoH for destruction.

/9608190 83/vaccines-for-data-israels-pfizer-deal-drives-quick-rollout-and-privacy-worries (accessed 12 September 2025).

11 P. Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 57 (2010) 1701–1777; L. Rocher, J.M. Hendrickx and Y.-A. de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications* 10 (2019) 3069.

12 N. Homer, S. Szelinger, M. Redman, D. Duggan, W. Tembe, J. Muehling, J.V. Pearson, D.A. Stephan, S.F. Nelson and D.W. Craig , 'Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays', *PLoS Genetics* 4(8) (2008) e1000167; A. Narayanan and V. Shmatikov, 'Robust de-anonymization of large sparse datasets', *2008 IEEE Symposium on Security and Privacy* (2008) 111–125.

Both counterarguments will be expanded below, in paragraph 3, in connection with the relevant EU legal framework. Relatedly, there is a lack of clarity on what the recipient company will do with the provided data, how long it will be retained, and the security measures to be implemented to prevent unauthorised access and data breaches. In addition, it is unclear in what country the data may eventually be transferred and processed. The recipient company may indeed be located in a country where data protection laws are less demanding for controllers.

Naturally, the position of the Israeli government is understandable. It served the political purpose of getting research ethics committees and data protection authorities out of the way, to bolster access to as many doses of much-needed COVID-19 vaccines as possible, as quickly as possible. The view advanced in this article is that, in an emergency, it is indeed desirable that exceptions and flexibilities are available to decision makers to address the emergency effectively. However, the fundamental rights of individuals should not be forfeited entirely in the process. Exceptions and restrictions to fundamental rights should be proportionate and respectful of the essence of such rights, as required by Article 52(1) of the Charter of Fundamental Rights of the European Union.

From this principled point of view, agreements creating the conditions (i) for States to share unspecified, sensitive personal data of their citizens with commercial entities, and (ii) for these latter to make use of such data for unspecified purposes, seem questionable, even in times of emergency. Such agreements may feature, like the Israel–Pfizer one, general prohibitions to use the data 'inappropriately', such as to re-identify or discriminate against individuals. This, however, runs the risk of remaining little more than a dead letter in the lack of significant, actionable control by the data subjects or review by an independent body. The distinction between general prohibitions to use data 'inappropriately' and specific, enforceable safeguards implemented through independent review mechanisms lies in the level of accountability and enforceability. While general prohibitions may provide broad guidance, they risk remaining ineffective without specific oversight mechanisms, transparent complaint procedures, and enforceable sanctions for violations. Independent review bodies can provide monitoring, specific guidance on borderline cases, and mechanisms for data subjects to seek redress when their rights are violated.

The relevance of the agreement between the Israeli MoH and Pfizer, and its related concerns, goes well beyond the Israeli borders. In the context of the COVID-19 pandemic, attempts emerged to normalise this kind of arrangement in negotiations for COVID-19 vaccine procurement across the globe. For

instance, in the talks between Taiwan and Pfizer's Chinese sales agent (Fosun) for access to BioNTech Covid-19 vaccines, Fosun agents put forward a template contract seeking access to Taiwanese medical records.[13] In particular, such a template provided that Fosun or its 'authorised representatives' have the right to audit the vaccination process, including checking facilities and reviewing documentation.[14] The template is also entitled Fosun to collect data and interview vaccinees. Taiwanese authorities eventually opposed the move by Fosun, which in turn dismissed the template as a mere 'starting point for negotiations'.[15] Likewise, the Government of the Hong Kong Special Administrative Region felt it necessary to reassure the public that the agreement it concluded with Fosun to buy BioNTech COVID-19 vaccines did not include clauses that 'enable Fosun or any third party to collect, access, or via any means to obtain or use the personal information of vaccinated individuals'.[16]

Despite this backlash in East Asia, it cannot be excluded that pharmaceutical companies will rely on the precedent of the Israel–Pfizer agreement to push for similar arrangements across the globe. In subsequent waves of the epidemic, governments may eventually accept such proposals to obtain prioritised access to COVID-19 vaccines. This is because the coverage ensured by currently available products is limited in time. Therefore, governments will need to find ways to ensure continued access to vaccines. Including data in the negotiation process may help governments secure a competitive advantage in the race to secure as many vaccine doses as possible. This may also apply to future pandemics.

This is not mere speculation. There are signs that similar agreements may take root also in the European context. For instance, the memorandum between the Italian Spallanzani Institute, the Lazio Region, and the Russian Gamaleya Institute[17] went in a similar direction. Published in the Official

13 'Taiwan says COVID vaccine talks held up on China sales deal', *Reuters* (18 April 2022), available online at www.reuters.com/business/healthcare-pharmaceuticals/taiwan-says-covid-vaccine-talks-held-up-china-sales-deal-2022-04-18/ (accessed 12 September 2025).

14 *Ibid.*

15 *Ibid.*

16 'Hong Kong says no personal data shared in vaccine deal with Fosun', *Reuters* (14 July 2021), available online at www.reuters.com/world/asia-pacific/hong-kong-says-no-personal-data-shared-vaccine-deal-with-fosun-2021-07-14/ (accessed 12 September 2025).

17 Lazio Region, decision 8 April 2021, n 184 (Approvazione dello schema di Memorandum d'Intesa per la collaborazione scientifica tra l'Istituto Nazionale per le Malattie Infettive Lazzaro Spallanzani IRCCS — Regione Lazio e il Centro Nazionale di Ricerca Epidemiologica e Microbiologica N.F. Gamaleya -- Fondo Russo degli Investimenti Diretti, 13/04/2021I), *Bollettino Ufficiale della Regione Lazio* n 37.

Journal of the Lazio Region in April 2021, the memorandum set up a framework agreement between the two Institutes.

In particular, the memorandum specifically outlined the exchange of biological materials and associated data. Under the agreement, the Spallanzani Institute committed to sharing 120 SARS-CoV-2 viral strains from its biobank, including variants of concern such as B.1.1.7 (UK variant) and P1 (Brazil variant). In exchange, the Gamaleya Centre agreed to provide human serum samples from subjects vaccinated with Sputnik V in Russia, particularly serial samples from clinical trial volunteers.

The memorandum also established a framework for three categories of clinical studies that would involve Italian citizens' health-related personal data: first, proof-of-concept studies involving 50–100 selected volunteers to test Sputnik V safety and efficacy in special populations; secondly, comparative immunological studies involving 2000–3000 volunteers to compare vaccine effectiveness; thirdly, phase 4 post-marketing surveillance studies on potentially large, non-randomized populations to monitor real-world effectiveness.

The agreement's data protection provisions were notably general, stating only that research would be conducted 'in compliance with territorially applicable laws, norms and regulations' without specifying concrete privacy safeguards or anonymisation protocols. Notably absent from the approval documentation is any evidence of involvement by the Italian Data Protection Authority, despite the agreement's provisions for extensive data and biological material exchanges.

Unlike the Israel–Pfizer agreement, the Spallanzani-Gamaleya memorandum was only a preliminary arrangement towards future protocols, to be submitted to the competent 'regulatory authority' and independent ethics committee. These protocols never followed suit, as the memorandum was suspended following the Russian invasion of Ukraine in February 2022.[18] However, similarly to the Israel–Pfizer agreement, the memorandum established a concerning precedent for potential exchanges of data for vaccines outside data protection oversight.

18 L. De Cicco, 'Stop al vaccino russo Sputnik: il Lazio interrompe i test con Gamaleya. Assessore Sanità: "Scienza al servizio della pace non della guerra"', *La Repubblica* (25 February 2022), available online at https://roma.repubblica.it/cronaca/2022/02/25/news/stop_a_sputnik_il_lazio_interrompe_i_test_con_gamaleya-339134191/ (accessed 12 September 2025).

3 The Role of Research and Personal Data Protection Regulations

Considering the above, it cannot be excluded that agreements along the lines of the one concluded by Israel and Pfizer, and their related concerns, might find their way in the European context. This raises the following question: if the government of an EU Member State were to follow the example of Israel, would the EU legal framework for G2B data sharing allow for this? The answer to this question is not obvious. As will be shown in more detail in the following paragraphs, EU data laws, including the GDPR, are filled with grey areas and flexibilities that might be exploited for more or less opportunistic strategies.

3.1 *Personal Vs Anonymous Data*

At the outset, suppose that the government of an EU Member State concluded a data-sharing agreement with a multinational corporation along the lines of the Israel–Pfizer agreement.[19] Suppose as well that such a government argued, like the Israeli MoH, that data protection regulations do not apply since aggregate, anonymous data will be processed rather than personal data.

Under the GDPR, it would be difficult for any government to support this claim. Indeed, data is anonymous if it cannot be referred to a specific individual anymore (Recital 26 GDPR). Mere de-identification of the data is, however, insufficient to ensure real anonymisation. The re-identifiability test outlined by Recital 26 of the GDPR is, in fact, a dynamic one.[20] The European Data Protection Board (EDPB) noted that it is difficult to achieve and uphold proper anonymisation of personal data, especially 'due to ongoing advancements in available technological means and progress made in the field of re-identification'.[21] In particular, the EDPB warns that anonymisation should be approached with 'caution' in the context of scientific research.[22] Indeed, when health-related data is shared on a mass scale, and a sufficient number of segmentation criteria are used, the re-identifiability of the individuals may, in fact, be 'reasonably likely' within the meaning of Recital 26 GDPR. This means that the shared data, albeit de-identified, are likely to qualify as personal data under Article 4(1) GDPR and, thus, be subject to the GDPR.

19 In the remainder of the article, this is referred to as the 'scenario under consideration'.

20 Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' 0829/14/EN WP216.

21 EDPB, 'Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research' (2 February 2021), available online at https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf (accessed 12 September 2025).

22 EDPB, *supra* note 21, para. 47.

The Court of Justice has further clarified this interpretation in its recent judgment in *EDPS v SRB*.[23] The Court confirmed that pseudonymised data must not be regarded as constituting personal data in all cases and for every person, acknowledging that pseudonymisation may, depending on the circumstances, effectively prevent identification by third parties. However, the Court also emphasised that the assessment of whether data subjects are identifiable depends essentially on the circumstances of processing in each case. Importantly for our analysis, this judgment does not alter the conclusions regarding the boundaries between personal and anonymous data in the context of large-scale epidemiological data sharing. The Court's emphasis on case-by-case assessment and the context-dependent nature of identifiability actually reinforces the position that aggregated health data, particularly when segmented by multiple demographic criteria and shared with entities possessing additional datasets, would likely qualify as personal data under the GDPR's dynamic re-identifiability test.

3.2 *Research Vs Non-Research*

Suppose now that this same government equally claimed that the agreement does not constitute research, arguing, like the Israeli MoH, that the agreement does not set up any clinical trial. Thus, research regulations would not apply. Would this position be tenable under the relevant EU legal framework?

Despite definitional uncertainties, the answer to this question is likely to be negative. The distinction between research and practice is widely debated in the literature,[24] and proposed definitions have proven unsatisfactory so far.[25] Definitional approaches tend to refer to the purpose of the activity at hand; accordingly, research is variably defined as being intended or designed to create generalisable knowledge.[26] These definitions, which historically served the (political) purpose of excluding medical practice from the ethical oversight that is mandated for biomedical research,[27] raise practical questions of how

23 Case C-413/23 P, EDPS v SRB, ECLI:EU:C:2025:645.

24 M.J. Selgelid, 'Public health: VII. Health surveillance', in: B. Jennings (ed.), *Bioethics* (London: Macmillan Reference, 2014).

25 A. Rubel, 'Justifying public health surveillance: basic interests, unreasonable exercise, and privacy', *Kennedy Institute of Ethics Journal* 22(1) (2012) 1–33, 4–9; A.L. Fairchild, 'Dealing with Humpty Dumpty: research, practice, and the ethics of public health surveillance', *Journal of Law and Medical Ethics* 31(4) (2003) 615–623, 618–620.

26 Fairchild, *supra* note 26, 617–618.

27 As '[c]lassification of practice as research […] could impede rapid and effective responses to community health threats' (Rubel, *supra* note 26; 5. *see also* Fairchild, *supra* note 26, 617).

primary or intended purposes can be measured and what should amount to generalizable knowledge.[28] As a consequence, the choice over whether an activity should be classified as research or surveillance can be quite arbitrary and ultimately porous to political pressures.[29] These aporias may give the impression that determining whether an activity is research or not is ultimately an arbitrary exercise, where a government can circumvent research regulations, including ethical oversight, simply by stating that a specific activity is not research.

Nevertheless, the case can be made that, in the EU, it would be hard for a government to do so in the scenario under consideration. In particular, a project aiming to generate real-world evidence on the effectiveness of a vaccine from medical records fits the definition of non-interventional research quite well. In the language of Regulation (EU) No 536/2014 (Clinical Trial Regulation, CTR), non-interventional studies are contrasted with clinical trials. Both are instances of clinical studies, as they investigate the effects of medicinal products; however, they approach such an investigation differently (Article 2(2)(1) CTR). In clinical trials, participants are assigned in advance to a specific treatment. The decision to prescribe an investigational product is taken together with the decision to include the participant in the study, or diagnostic or monitoring procedures in addition to normal clinical practice are applied to the subjects (Article 2(2)(2) CTR). Conversely, non-interventional studies are clinical studies that do not qualify as clinical trials (Article 2(2)(4) CTR). Thus, such studies are limited to collecting data from individuals' files, without intervening directly with the person or changing their usual care. These studies focus on gathering real-world data to understand better the effects of medicinal products, as well as to identify adverse reactions. This is why they are also known as observational studies.[30]

In the EU, the regulation of observational studies is not harmonised, and different legal frameworks apply.[31] In particular, informed consent processes for observational studies are said to be 'less robust' than in clinical trials.[32] However, the involvement of an ethics committee or another

28 Rubel, *supra* note 26, 6; Fairchild, *supra* note 26, 620.

29 Fairchild, *supra* note 26, 620.

30 P. Aurucci, 'Legal Issues in Regulating Observational Studies', *European Data Protection Law Review* 5(2) (2019) 197–208.

31 I. Ramirez, 'Navigating the Maze of Requirements for Obtaining Approval of Non-Interventional Studies (NIS) in the European Union', *German Medical Science: GMS e-Journal* 13 (2015) Doc21, doi: 10.3205/000225.

32 E.E. Ricotta, A. Rid, I.G. Cohen et al., 'Observational studies must be reformed before the next pandemic', *Nature Medicine* 29 (2023) 1903–1905, doi: 10.1038/s41591-023-02375-8.

independent organ is a recurring feature in national frameworks for observational research.[33]

A consequence of this is that, in the scenario under consideration, ethics committees could rely on the (binding) definition of clinical studies under the CTR to argue that the data sharing operation constitutes, in fact, (observational) scientific research and is, therefore, subject to research regulations, as well as to their oversight.

The GDPR also offers support to this argument, even though the GDPR is not a research regulation. Recital 159 of the GDPR states that:

The term processing of personal data for scientific research purposes should be interpreted in a broad manner, including, for example, technological development and demonstration, fundamental research, applied research, and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health.

While Recital 159 fails to provide a clear definition of what research is, it does offer an important indication to navigate the research-practice divide in epidemiological studies. In particular, Recital 159 clarifies that studies conducted in the public interest in the area of public health constitute scientific research for the purposes of the GDPR (importantly, without necessarily implying that all such studies involve the processing of personal data).

The recital establishes a broad interpretation of scientific research that encompasses various types of activities, including those conducted for public health purposes. While the GDPR does not clearly define what the public interest or public health are either, leaving the ultimate decision to the EU Member States, it is reasonable to argue that a joint data-sharing project between a State and a pharmaceutical company to 'generate and analyse' real-world evidence on the effectiveness of a vaccine — with a view to informing a national vaccination campaign (and obtaining prioritised access to vaccines) in a pandemic — would likely be in the public interest and in the area of public health within the meaning of Article 9(2)(i) GDPR. Recital 46 of the GDPR expressly states that processing for the monitoring of epidemics may serve important grounds of public interest, and the EDPB confirmed that the fight against COVID-19 is an important public interest for the purposes of the GDPR.[34] Thus, such a

33 Ramirez, *supra* note 31.

34 EDPB, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* (21 April 2020), available online

study would likely fall under the remit of scientific research for the purposes of Article 89(1) GDPR.

4 The GDPR Research Exemptions and Safeguards

Considering the above, it would be hard for the government of an EU Member State to follow the steps of the Israeli MoH. A data sharing operation along the lines of the Israel–Pfizer agreement would likely fall under both data protection and (observational) research regulations.

However, when personal data is processed for research, the GDPR allows for several exceptions, provided that appropriate safeguards for the fundamental rights of the data subjects are implemented under Article 89(1) GDPR. Subject to this same requirement, the GDPR also foresees potential derogations from the data subjects' rights under Article 89(2) if the data is processed for research. This raises the question of whether the GDPR provides adequate protection against excessive data sharing operations when such exemptions apply.

To answer this question, it is first necessary to recap the GDPR regime for the processing of personal data for scientific research. The GDPR research exemptions warrant derogations from several GDPR principles, starting with the principle of lawfulness under Article 6. Regarding the lawfulness of the processing of personal data, besides the consent of the data subject and compliance with a legal obligation in EU or domestic law (Articles 6(1)(a) and 6(1)(c) GDPR), controllers may rely, as a legal basis, on the performance of a task in the public interest or in the exercise of official authority (Article 6(1)(e) GDPR). This is provided that the purpose of the processing is necessary for the performance of the task and that the legal basis contains specific provisions on the processing, such as the general conditions, the types of data that are processed, the data subjects concerned, the recipients of the data, the purpose limitation, the storage periods, as well as the processing operations and procedures, including measures to ensure lawful and fair processing (Article 6(3) GDPR).

Both legal bases must be based on EU or national legislation, which must pursue an objective of public interest and be proportionate to the objective pursued, as required by Article 6(3) GDPR. Recital 41 specifies that this does not require an explicit legislative act. Nevertheless, 'such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it', according to the case law of the Court of Justice

at https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_en (accessed 12 September 2025).

of the EU and the European Court of Human Rights (ECtHR). The ECtHR has developed rigorous standards for what constitutes a sufficiently clear basis in law. In particular, any interference with the rights enshrined in the European Convention on Human Rights must meet three fundamental criteria: first, it must be accessible: the law must be publicly available and accessible to individuals who need to understand their legal obligations;[35] secondly, it must be foreseeable: the law must be formulated with sufficient precision to enable individuals to regulate their conduct accordingly, by providing adequate indication of the circumstances and conditions under which public authorities may interfere with rights, including the scope of discretion and manner of its exercise;[36] thirdly, it must be non-arbitrary: the application of the law must not be arbitrary and must be necessary and proportionate.[37]

An alternative legal basis that may be relevant to research data processing is the pursuit of legitimate interests by the controller or a third party, unless the interests and fundamental rights of the data subject that require the protection of personal data outweigh such legitimate interests (Article 6(1)(f) GDPR). This specific legal basis does not require a basis in EU or domestic law. However, public authorities cannot rely on this legal basis when performing their tasks (Article 6(1), second subparagraph, GDPR).

Turning now to the GDPR principle of purpose limitation under Article 5(1)(b), before further processing the data, the controller must assess the compatibility of the purpose of the intended further processing with the purpose for which the data were collected (Article 6(4) GDPR). Article 5(1)(b) of the GDPR establishes that further processing for scientific research purposes is compatible with the initial purposes, subject to 'appropriate safeguards' under Article 89 of the GDPR. Importantly, Recital 50 of the GDPR states that, if the further processing is compatible with the initial purposes, 'no legal basis separate from that which allowed the collection of the personal data is required'.

The compatibility clause under Article 5(1)(b) of the GDPR and the wording of Recital 50 lend themselves to two different yet related ambiguities that require some unpacking. The first ambiguity stems from the fact that the notion

35 *Sunday Times v. United Kingdom*, App. No. 6538/74, judgment of 26 April 1979, para. 49. See also *Selahattin Demirtaş v Turkey* (No 2), App No 14305/17, Grand Chamber judgment of 22 December 2020.

36 *Malone v. the United Kingdom:* Malone v United Kingdom, App No 8691/79, judgment of 2 August 1984, (1984) 7 EHRR 14. See also Big Brother Watch and Others v United Kingdom, App Nos 58170/13, 62322/14 and 24960/15, Grand Chamber judgment of 25 May 2021.

37 *Klass and Others v. Germany:* Klass and Others v Germany, App No 5029/71, judgment of 6 September 1978, (1979–80) 2 EHRR 214. See also Breyer v Germany, App No 50001/12, judgment of 30 January 2020.

of 'further processing' is not clearly defined in the GDPR. In line with the scientific notion of secondary uses of data, further processing may be defined as including all the subsequent data (re)uses that differ from the use for which the data was initially collected from the data subjects (the so-called primary use).[38] However, the case has been made that Article 5(1)(b) of the GDPR actually adopts a narrower definition of further processing of personal data, focusing on the perspective of the controller, rather than on the data itself. This is based on the premise that '[t]he GDPR focuses always on the fact that data are processed and why they are processed, building its definitions and framework around the processing operations and the purposes'.[39]

The same applies to Article 5(1)(b) of the GDPR. This Article relates the notion of further processing to the purpose for which a specific controller collects the data. Thus, every time a controller collects the data and determines the purposes of the data processing, this is *primary* processing. This is irrespective of whether this specific controller obtained the data directly from the data subject or from another source. This also applies to a downstream controller that receives the data from an upstream controller. In this case, the downstream controller collects the data and determines the purpose of the data processing at data collection. Thus, the data processing operations that are in line with such a purpose are primary processing and not further processing. Further processing occurs when a controller (re)uses the data they already collected, regardless of their source, for a purpose that was not envisaged when that same controller collected the data.

A second, related ambiguity concerns the wording of Recital 50 of the GDPR. This suggests that, if data are further processed for research, and appropriate safeguards are implemented under Article 89(1), the controller can always rely on the legal basis selected for the primary processing. However, this specific passage of Recital 50 is not reflected in any of the Articles of the GDPR. Although the EDPB is yet to release guidance on this, it is reasonable to argue that any preamble-based derogation from the principle of lawfulness under the GDPR is 'hard to justify'.[40] Indeed, the French DPA adopted the position

38 R. Becker D. Chokoshvili, G. Comandé, E.S. Dove, A. Hall, C. Mitchell, F. Molnár-Gábor, P. Nicolàs, S. Tervo and A. Thorogood, 'Secondary use of personal health data: when is it "further processing" under the GDPR, and what are the implications for controllers?', *European Journal of Health Law* 30 (2023) 129–157, 137–138.

39 Becker *et al.*, *supra* note 38, 138.

40 Becker *et al.*, *supra* note 38, 149.

that 'even when the further processing is compatible, a valid legal basis must always be identified'.[41]

When special categories of data are processed under Article 9 GDPR, such as health-related or genetic data, the controller must also make sure that one of the exceptions to the general prohibition to process such 'sensitive' personal data applies. For research, these are most likely the explicit consent of the data subject (Article 9(2)(a) GDPR); reasons of substantial public interest (Article 9(2)(g) GDPR); reasons of public interest in the area of public health (Article 9(2)(i) GDPR); and scientific research purposes, according to Article 89 of the GDPR (Article 9(2)(j) GDPR). The exceptions in letters g, i, and j of Article 9(2) of the GDPR must have a basis in EU or national law which is clear, precise, and foreseeable (Recital 41) and must 'provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject'. In the case of substantial public interest and scientific research, the law must also be 'proportionate to the aim pursued' and 'respect the essence of the right to data protection' (Article 9(2)(g) and (j) GDPR).

Furthermore, the principle of transparency may be derogated from when data is processed for research. Article 14(5)(b) of the GDPR allows controllers to avoid providing information to data subjects where 'the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing'. In such cases, Article 14(5)(b) requires that 'the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available'.

Finally, if data is processed for research, a series of rights of the data subject may be limited under Article 89(2) GDPR. For instance, the right to erasure (or 'to be forgotten') under Article 17 does not apply if the data are processed for research and appropriate safeguards are implemented, provided that the exercise of such a right 'is likely to render impossible or seriously impair the achievement of the objectives of that processing' (Article 17(3)(d) GDPR). Also, if data are processed for research based on a 'public task' or legitimate interests (Articles 6(1)(e) and 6(1)(f) GDPR), and the processing is necessary for the performance of a task carried out for reasons of public interest, then the right of

41 CNIL, *Ensuring the lawfulness of the data processing*, available online at www.cnil.fr/en/ensuring-lawfulness-data-processing (accessed 12 September 2025).

the data subject to object to the processing of their personal data on grounds of their particular situation does not apply (Article 21(6) GDPR).

Importantly, as already pointed out above, when data is processed for research, Article 89(1) of the GDPR requires controllers to implement 'appropriate safeguards' to protect the fundamental rights and interests of the data subjects. Such safeguards must ensure, in particular, respect for the principle of data minimisation and may consist of pseudonymisation or, if possible, anonymisation. The EDPB has clarified that such safeguards may include conducting a data protection impact assessment (DPIA), appointing a data protection officer, notifying a data breach, and guaranteeing data security under Articles 35, 37, 33 and 32 GDPR, respectively.[42] Appropriate technical and organisational measures must be implemented to ensure a sufficient level of security under Article 32(1) GDPR. Such measures should at least consist of pseudonymisation, encryption, NDAs and strict access role distribution, as well as access role restrictions and access logs, as specified in Articles 25 and 32 GDPR.[43] The EDPB also stated that, in the case of further processing of data for research, an appropriate safeguard is to deliver the information to the data subject within a reasonable time before the research project is implemented,[44] to allow the data subject to become aware of the research and exercise their rights.

While these examples relate narrowly to the right to data protection, other key guidance documents point to the role of further ethical and legal regulations that might assist the GDPR in its broader objective of protecting the fundamental rights of the data subjects, which, as per Article 1(2) of the GDPR, include, but are not limited to, the right to data protection.[45] For instance, the EDPS pointed out that 'professional ethical standards governing a particular research project would also be considered a safeguard'.[46] Relatedly, ethical review by an independent ethics committee, as a traditional safeguard for research participants, may provide an adequate safeguard. Indeed, Council of Europe Recommendation CM/Rec(2019)2 provides that 'the conditions in which health-related data are processed for scientific research must be

42 EDPB, *supra* note 34, para. 10.

43 EDPB, *supra* note 34, para. 51.

44 EDPB, *supra* note 34, para. 34.

45 C. Staunton, S. Slokenberga, A. Parziale and D. Mascalzoni, 'Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research', *Frontiers in Genetics* 13 (2022) 719317, doi: 10.3389/fgene.2022.719317.

46 EDPS, *A Preliminary Opinion on data protection and scientific research* (6 January 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (accessed 12 September 2025)

assessed, where necessary, by the competent independent body (for example, an ethics committee)'. Data minimisation, which is explicitly mentioned in Article 89 of the GDPR, can be achieved by 'specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions'.[47] Compliance with research regulations under independent oversight would, therefore, be an appropriate safeguard under Article 89 of the GDPR.[48]

5 Sharing Data in the Public Interest and for Public Health Reasons under the GDPR

The previous paragraph noted that the GDPR also affords special consideration to the processing of personal data in the pursuit of the public interest or public health objectives under Articles 6(1)(e) and 9(2)(g)-(i), and that these may overlap with the GDPR framework for research under Article 9(2)(j). Public interest and public health reasons may warrant specific legal bases for the processing of data different from the consent of the data subject under Article 6(1) of the GDPR. Secondly, the pursuit of the public interest or public health can warrant exemptions from the general prohibition to use 'sensitive' data in accordance with Article 9(2) of the GDPR.

Similarly to the GDPR research regime, this raises the question whether the GDPR provides adequate protection against excessive data sharing operations, such as in the scenario being considered, despite its public interest/public health flexibilities. This calls for a discussion of such flexibilities first.

At the outset, the controller does not need to assess the compatibility of the further processing of data with the original purposes if the controller can rely on the consent of the data subject or the processing is based on an EU or national law that is 'necessary and proportionate' to safeguard the objectives under Article 23(1) GDPR. These include national security, defence, and 'other important objectives of general public interest', including 'public health' (Article 6(4) GDPR).

More generally, Article 23 of the GDPR allows EU or domestic law to introduce restrictions, by a legislative measure, to the obligations and rights under Articles 12 to 22 and the relevant provisions of Article 5. The Court of Justice has emphasised that such restrictions must be implemented through formal legislative measures, not through administrative practices or informal

47 EDPB, *supra* note 34, para. 46.
48 Staunton *et al.*, *supra* note 45.

procedures.[49] In the *VP* case, concerning gender identity data rectification, the Court clarified that administrative practice requiring specific evidence for data rectification, without a proper legislative foundation, cannot constitute a valid restriction under Article 23.[50]

Such a restriction must respect the essence of the fundamental rights and freedoms and is necessary and proportionate in a democratic society to protect, *inter alia*, 'important objectives of general public interest' of the EU or an EU Member State, 'including [...] public health' (Article 23(1)(e) GDPR). The Court of Justice has consistently held that the essence of fundamental rights represents an absolute limit that cannot be transgressed even in pursuit of legitimate public interests.[51] In the *Endemol Shine* case, which concerned access to criminal conviction data, the Court demonstrated how even legitimate public interests, such as public access to official documents, must yield when they would undermine the essence of data protection rights.[52]

In this connection, the EDPB clarified that the respect of the essence of the right to data protection 'means that restrictions that are extensive and intrusive to the extent that they void a fundamental right of its basic content, cannot be justified'.[53] This includes 'a general exclusion of data subjects' rights with regard to all or specific data processing operations or with regard to specific controllers'.[54] The case law of the Court of Justice upholds this principle by requiring that any restriction be tailored to specific circumstances and objectives, rather than imposing blanket limitations on data subject rights.[55]

The EDPB also clarified that necessity and proportionality mean that 'the content of the legislative measure cannot exceed what is strictly necessary to safeguard the objectives listed in Article 23(1)(a) to (j) GDPR'.[56] For instance, if restrictions aim at protecting public health in a state of emergency, the restrictions must be limited to the emergency state period.[57]

In addition, Article 23(2) of the GDPR provides that restrictive measures must have a minimum content of provisions regarding, 'where relevant', the

49 Case C-247/23, VP v Országos Idegenrendészeti Főigazgatóság, EU:C:2025:172, para. 44.

50 *Ibid.*, paras 43–44.

51 Case C-740/22, Endemol Shine Finland Oy, EU:C:2024:216, para. 52.

52 Case C-740/22, paras 54–58.

53 EDPB, *Guidelines 10/2020 on restrictions under Article 23 GDPR* (13 October 2021), available onlnie at https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf (accessed 12 September 2025).

54 EDPB, *supra* note 53, para. 14.

55 EDPB, *supra* note 53, para. 45.

56 EDPB, *supra* note 53, para. 42.

57 EDPB, *supra* note 53, para. 44.

purposes of the processing, the categories of personal data, the safeguards to prevent abuse or unlawful access or transfer, the controllers, the storage periods, the rights of the data subjects, the risks to the rights of the data subjects, the right of the data subject to be informed about the restriction (letters (a) to (h)). Regarding the wording 'where relevant', the EDPB clarified that '[a]s a rule, all the requirements detailed below should be included in the legislative measure imposing restrictions under Article 23 GDPR' and exceptions 'need to be duly justified by the legislator'.[58]

The EDPB also explained that the safeguards to prevent abuse or unlawful access or transfer (Article 23(2)(d) GDPR) refer, in particular, to organisational or technical measures necessary to prevent breaches or unlawful transfers (e.g., the safe storage of physical documents).[59] As regards the risk to the rights of the data subjects (Article 23(2)(g) GDPR), the EDPB stated that their assessment is 'a very important step' to provide 'an overview of the potential impact of restrictions on data subjects' as well as 'elements for the necessity and proportionality test of the restrictions'.[60] If 'applicable', a DPIA should be considered under Article 35 GDPR.[61] The EDPB noted that Member States must consult DPAs under Article 36(4) of the GDPR before adopting the restrictions.[62] If they are not duly consulted, the DPA can issue their opinions to the national parliament, government or other institutions and to the public.[63] Naturally, the European Commission can also take action where national measures fail to comply with EU law, including the GDPR.[64]

Furthermore, the GDPR restricts certain rights of the data subjects in the public interest. In particular, the right to erasure (or 'to be forgotten') does not apply if the processing is necessary for reasons of public interest in area of public health according to Articles 9(2)(h), 9(2)(i), and 9(3) of the GDPR (Article 17(3)(c) GDPR).

Finally, another instance where the public interest and public health play a role relates to cross-border data transfers under Chapter V GDPR. Indeed, the EDPB clarified that the 'combatting serious cross-border threats to health'

58 EDPB, *supra* note 53, paras 45–46.
59 EDPB, *supra* note 53, para. 56.
60 EDPB, *supra* note 53, para. 60.
61 *Ibid.*
62 EDPB, *supra* note 53, para. 68.
63 EDPB, *supra* note 53, para. 70.
64 EDPB, *supra* note 53, para. 77.

exception may play a role in a public health emergency like the Covid-19 epidemic.[65] In particular, the EDPB stated that:

[T]he fight against COVID-19 has been recognised by the EU and most of its Member States as an important public interest, which may require urgent action in the field of scientific research (for example to identify treatments or develop vaccines), and may also involve transfers to third countries or international organisations.

This prominent public interest may, therefore, legitimise a data transfer outside the EEA under Article 49(1)(d) GDPR, even without the explicit consent of the data subject. While the EDPB acknowledged that the public interest derogation is not limited to occasional transfers, 'this does not mean that data transfers on the basis of the important public interest derogation under Article 49 (1) (d) can take place on a large scale and in a systematic manner'.[66]

6 Where the GDPR Provides Protection

The analysis of the GDPR research and public interest/public health flexibilities conducted above enables an orderly assessment of whether the GDPR protects excessive mass-scale data sharing operations. First, the GDPR would require the specification of the personal data or categories of personal data that are the object of the data sharing operation under Articles 13(1)(c) and 14(1)(c). The principles of purpose limitation and data minimisation under Article 5(1)(b) and (c) require controllers to identify the data that are needed to achieve the purposes of the data processing. Neither the research nor the public interest or public health GDPR flexibilities provide for exceptions to this. Thus, the GDPR would not tolerate open-ended expressions like the one to be found in the Israel–Pfizer agreement ('[e]ach data transfer will include, at a minimum …').

Secondly, the GDPR would require the disclosure of information regarding the data sharing operation to the data subjects under Articles 13 and 14. On the one hand, the disclosing State (DS) intending to share citizens' vaccination

65 EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (10 November 2020), available online at https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (accessed 12 September 2025).

66 EDPB, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* (25 May 2018), available online at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (accessed 12 September 2025).

data would have to inform the data subjects before that further processing according to Article 13(3) of the GDPR. This is unless the data subject already has the information (Article 13(4) GDPR).

On the other hand, the recipient company (RC), which would receive the data from the DS and not from the data subjects, could rely on the exemption provided in Article 14(5)(b) of the GDPR, as informing all the citizens of a Member State would likely involve a 'disproportionate effort'.[67] However, the RC would have to implement appropriate measures to protect the rights of the data subjects, including making the information publicly available. Thus, the GDPR would not admit a confidential data sharing agreement, as the Israel–Pfizer agreement initially was.

Thirdly, the GDPR could permit the sharing of health-related data without explicit consent, provided there is a sufficiently clear legal basis and specific safeguards under Article 9(2)(g), (i), and (j). According to our reading of the notion of further processing and of the role of Recital 50 of the GDPR, this would apply not only to the RC, for which the processing of the data received from the DS is a primary processing of data, but also to the DS, for which, subject to appropriate safeguards under Article 89(1), sharing citizens' data for research is a (compatible) further processing of data. In particular, other than the consent of the data subjects or compliance with a legal obligation, the DS may rely on the legal bases of the performance of a task carried out in the public interest under Article 6(1)(e). Also, the substantial public interest, public interest in the area of public health, and scientific research exceptions to the general prohibition on the processing of special categories of personal data, including health-related data, would apply under Article 9(2)(g), (i), and (j). However, all these legal bases and exceptions under Articles 6 and 9 of the GDPR must have a sufficiently clear and foreseeable basis in the law.

On the other hand, the RC may rely on the legal basis of the pursuit of legitimate interests under Article 6(1)(f).[68] This legal basis does not require a basis in EU or national law. However, if the RC does not intend to rely on the explicit consent of the data subjects under Article 9(2)(a) of the GDPR for the processing of health-related data, the RC will likely have to rely on the substantial public interest, public health, or scientific research exceptions under

67 Recital 62 of the GDPR states that the 'number of data subjects [...] should be taken into consideration'.

68 Conversely, the RC is unlikely to be able to rely on the legal basis of the public interest task. The French and Italian DPAs confine this legal basis to public actors (S. Aidinlis, *supra* note 2, 117).

Article 9(2)(g), (i), and (j) of the GDPR. These do require a basis in the law and must provide for specific safeguards.

The protection afforded by the GDPR to the data subjects continues after the data is transferred from the DS to the RC. Once the RC has received the data, the GDPR does not allow the RC to indefinitely reuse the same data for unspecified purposes without informing the data subjects. The RC is not permitted to reuse the data for non-research (e.g., commercial) purposes without, before that further processing, performing a compatibility assessment (Article 6(4) GDPR); identifying a valid legal basis (Articles 6(1) GDPR); and informing the data subject individually or, if an exception applies, by making the information publicly available, along with other 'appropriate measures' (Article 14(1–2) and (5)(b) GDPR).

Naturally, if the RC intended to process the data for research further, the RC would be exempted from performing the compatibility assessment under Article 5(1)(b). However, the RC would still need to implement appropriate safeguards under Article 89(1), select a valid legal basis for the further processing, and inform the data subjects in accordance with Articles 13 and 14.

Thus, the GDPR would not tolerate generic statements of good intentions, such as those in the Israel–Pfizer agreement ('PFIZER shall not use the Project Data for any purpose or in any manner which does not serve to improve health care, public health, or is discriminatory in respect of insurance or employment or has otherwise an inappropriate social purpose …')[69] lacking clear information on the further reuses of the data and specific, actionable safeguards for the data subjects. The downside is that, despite an increasing body of regulatory guidance, controllers retain broad discretion in selecting and implementing appropriate safeguards under Article 89 of the GDPR.

In addition, the data subjects would maintain most of their rights under the GDPR. Indeed, the GDPR only derogates from a minority of such rights if data is processed for research, in the public interest, or for public health reasons. Further derogations would need to be outlined in the law, be necessary and proportionate, and provide for safeguards to prevent abuse, according to Article 23 of the GDPR. While this framework can protect against generalised suspensions of GDPR rights, it still leaves legislators with broad leeway on whether and to what extent to restrict data subjects' rights in an emergency, leveraging flexible notions of necessity and proportionality and a lack of clarity on the safeguards mentioned in Article 23 of the GDPR.

69 'Real-world epidemiological evidence collaboration agreement', *supra* note 3, section 7.8.

Regardless of the use of Article 23, since the data sharing operation in question would involve the mass-scale sharing of health-related data to the industry, it would most likely need to undergo a DPIA (Article 35 GDPR and EDPB Guidelines 10/2020).[70] For the same reason, the DPIA would probably indicate that there are high risks if the controller does not take risk mitigation measures. As a consequence, before processing the data, the DS and the RC would need to consult the competent DPA (Article 36 GDPR).

The DPA is not necessarily the only independent body that would be involved in the data-sharing operation in question. We argued above that the mass-scale sharing of epidemiological data to assess the effectiveness of a vaccine would constitute observational research, subject to independent oversight by an ethics committee. This could constitute an appropriate safeguard under Article 89 of the GDPR. For these reasons, the GDPR would be unlikely to tolerate the mass-scale sharing of health-related data without any independent review, either by a DPA or an organ competent for the evaluation of (observational) research studies.

Finally, subject to the considerations above, the GDPR would allow for mass-scale and systematic transfers of health-related data to a third country only in the presence of an adequacy decision by the European Commission under Article 45, appropriate safeguards under Article 46, or the explicit consent of the data subjects. While the derogation for important reasons of public interest under Article 49(1)(d) of the GDPR, which includes cross-border health emergencies, may legitimise non-occasional transfers, the EDPB stated that this does not authorise large-scale and systematic data transfers.[71] Thus, the GDPR would not permit a data-sharing operation where the health-related data of millions of individuals is seamlessly transferred outside the EEA (e.g., 'weekly', as in the Israel–Pfizer agreement) in the absence of an adequacy decision, appropriate safeguards, or the explicit consent of the data subjects.

7 The Role of the Data Governance Act and EHDS

Under the remit of the European Data Strategy, EU lawmakers have been adopting further pieces of legislation that do not derogate from the GDPR

70 EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (13 November 2019), available online at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (accessed 12 September 2025).

71 EDPB, *supra* note 66, 11.

yet aim to facilitate the sharing and reuse of data. Among such pieces of legislation, of particular importance for G2B data sharing are Regulation (EU) 2022/868 (Data Governance Act, DGA) and Regulation (EU) 2025/327 establishing the European Health Data Space (EHDS).[72]

There are concerns in the literature that these might reduce the level of protection and control that the GDPR affords to data subjects, especially in relation to the role of the opt-out mechanism established in the EHDS (see below at paragraph 7.2).[73] This raises the question of whether these further pieces of legislation would enable excessive mass-scale G2B data sharing operations.

7.1 *The Data Governance Act*

Starting with the DGA, this is not limited to G2B data sharing. The DGA provides rules on G2B, G2C (government-to-consumer), B2G (business-to-government) and C2G (consumer-to-government) data sharing. G2B data sharing is the focus of Chapter II of the DGA (Articles 3–9 DGA), which provides rules on the re-use of protected government-held data, including data protected as personal data (Article 3(1)(d) DGA). Such conditions for re-use are dictated in Article 5 of the DGA. In particular, Article 5(1) of the DGA states that public sector bodies that grant or refuse access for re-use under national law must make the conditions for re-use publicly available. Such conditions must be 'non-discriminatory, transparent, proportionate and objectively justified' and must not be used 'to restrict competition' (Article 5(2) DGA).

Notably, Article 5(3) of the DGA requires public sector bodies to make sure that the 'protected nature of the data' is preserved, 'in accordance with Union or national law'. Article 5(3) of the DGA provides public sector bodies with a list of potential requirements for access to, and re-use of, protected data. These include the anonymisation of personal data (Article 5(3)(a)(i) DGA); accessing and re-using data remotely in a 'secure processing environment' provided or controlled by the public sector body (Article 5(3)(b) DGA); and, if remote access jeopardises the rights and interests of third parties, accessing and re-using data

72 Another key piece of the EU data legislation is Regulation (EU) 2023/2854 (Data Act, DA), which will become applicable in September 2025. However, this article does not cover the DA. This is because the DA does not seem relevant to the scenario under consideration. Indeed, the DA mostly concerns 'the making available of product data and related service data to the user of the connected product or related service' (Article 1(1)(a) DA). Our scenario does not concern this practice.

73 T. Sokol, 'European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance?', *European Journal of Health Law* 31 (2024) 365–388. *See also* L. Marelli et al., 'The European health data space: Too big to succeed?', *Health Policy* 135 (2023) 104861, doi: 10.1016/j.healthpol.2023.104861.

'within the physical premises in which the secure processing environment is located in accordance with high security standards' (Article 5(3)(c) DGA).

In any event, under Article 5(5) of the DGA, the re-user must adhere to a confidentiality obligation prohibiting the disclosure of any information jeopardising the rights and interests of third parties. The re-user must also 'take technical and operational measures to prevent re-identification and to notify any data breach resulting in the re-identification of the data subjects concerned to the public sector body'.

Overall, the DGA seems to add little value to the GDPR framework for G2B data sharing. Indeed, the G2B provisions of the DGA do not assign a specific status to the re-use of government-held personal data for purposes of scientific research or public interest/public health objectives. Indeed, the only (non-binding) reference to research can be found in Recitals 15 and 16 of the DGA. The former states that the 'conditions for re-use should be designed in a manner promoting scientific research so that, for example, privileging scientific research should, as a rule, be considered to be non-discriminatory'. Conversely, Recital 16 of the DGA provides that '[i]n order to facilitate and encourage the use of data held by public sector bodies for the purposes of scientific research, public sector bodies are encouraged to develop a harmonised approach and harmonised processes to make that data easily accessible for the purposes of scientific research in the public interest. That could mean, inter alia, creating streamlined administrative procedures, standardised data formatting, informative metadata on the methodological and data collection choices and standardised data fields that enable the easy joining of data sets from different public sector data sources where relevant for the purposes of analysis. The objective of those practices should be to promote the publicly funded and produced data for the purposes of scientific research in accordance with the principle of 'as open as possible, as closed as necessary'.

7.2 *The EHDS*

Compared to the DGA, the EHDS Regulation has the potential to play a greater role in mass-scale data sharing operations. The EHDS Regulation has been published in the Official Journal of the European Union on 5 March 2025. It will gradually become applicable according to the schedule set out in Article 105 of the EHDS Regulation (hereinafter also referred to simply as EHDS).

The EHDS aims to facilitate 'access to electronic health data for the purposes of primary and secondary use of these data' (Article 1(1) EHDS). Primary use means 'the processing of electronic health data for the provision of healthcare' and 'for relevant social, administrative or reimbursement services' (Article 2(2)(d) EHDS). Conversely, secondary use means 'the processing of

electronic health data for purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced' (Article 2(2)(e) EHDS). The mass-scale sharing of data collected in the context of healthcare to assess the effectiveness of a vaccine in a pandemic would likely constitute a secondary use of data for the purposes of the EHDS.

Regarding secondary uses specifically, access to data is permitted only for the purposes listed in Article 53 of the EHDS. These include 'public interest in the area of public and occupational health, such as activities for protection against serious cross-border threats to health and public health' (Article 53(1)(a) EHDS) and 'scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators …' (Article 53(1)(e) EHDS). Access to electronic health data for public interest or public health purposes (e.g., under Article 53(1)(a) EHDS) can only be granted to public sector bodies and EU institutions (Article 53(2) EHDS). A mass-scale data sharing operation to assess the effectiveness of a vaccine in a public health emergency would fit both purposes. However, a private company would not be allowed to seek access to data for secondary uses to pursue a public interest/public health purpose. They would need to rely on an alternative purpose, e.g., scientific research. In particular, in the scenario under consideration, they could claim that access to data is sought for research that 'contributes to public health' under Article 53(1)(e) of the EHDS.

The electronic health data that data holders must make available if a data permit is released include electronic health data from electronic health records (EHRs); aggregate data on the 'provision of and access to healthcare'; 'healthcare-related administrative data'; genetic data; public health registries; 'data from clinical trials, clinical studies and clinical investigations'; and health data from biobanks (Article 51(1) EHDS). Member States may add further categories of data (Article 51(2) EHDS). In the scenario under consideration, epidemiological data on the vaccination campaign would likely fall under the data categories listed in Article 51 of the EHDS.

From a procedural point of view, the EHDS sets up a system where data users submit applications to health data access bodies (HDABs) to access electronic health data held by data holders. Under Article 67 EHDS, such health data access applications must include, *inter alia*, information on the health data applicant; the purposes under Article 53(1) for which access to data is requested; an explanation of the intended use of the electronic health data, the expected benefit, and how this benefit would contribute to the purposes under

Article 53(1); a description of the requested electronic health data; an explanation whether the electronic health data are needed in a pseudonymised or anonymised format, and, if access is requested to pseudonymised data, a justification why the processing cannot be carried out in an anonymised format; proportionate safeguards to prevent any misuse of the electronic health data and protect the rights and interests of the health data holder and the natural persons concerned, including to prevent their re-identification; a justified indication of the period during which the data are needed for processing; if applicable, information on any assessment of ethical aspects of the processing, as required by national law; a justification to exceptionally access the data relating to a natural person that opted out from the processing of data for secondary use under Article 71(4) of the EHDS.

Regarding this last aspect, it is worth mentioning that, under the EHDS, individuals have a right to opt out of the processing of data for secondary use (Article 71(1) EHDS). If an individual opts out, their data cannot be made available or otherwise processed in accordance with a data permit (Article 71(3) EHDS). However, national laws can establish mechanisms to make the data available even after an individual opts out, subject to strict conditions set out in Article 71(4) of the EHDS. In particular, the data access application must come from a public sector body or an EU institution. Access to the data is necessary to achieve the public interest or for research for important reasons of public interest. The data cannot be obtained by alternative means as timely and effectively. The applicant provides a justification. National laws that foresee this exception must provide specific and suitable measures to protect the fundamental rights of natural persons, respect the essence of the fundamental rights, and be necessary and proportionate. In the scenario under consideration, it would be easy for a Member State to justify such an exception to the right to opt out to fight a pandemic.

The health data access applications are reviewed by HDABs (Article 68 EHDS). In particular, HDABs check whether the requirements under Article 67 of the EHDS Regulation are met, and whether 'the processing complies with Article 6(1) of Regulation (EU) 2016/679'. This means that the processing of the data by the user must rely on a valid legal basis under the GDPR. Relatedly, Recital 52 of the EHDS Regulation clarifies that it 'provides for a legal basis for the secondary use of personal electronic health data, including the safeguards required under Article 9(2), points (g) to (j), of Regulation (EU) 2016/679 to allow the processing of special categories of data, in terms of lawful purposes, trusted governance for providing access to health data through the involvement of health data access bodies, and processing in a secure processing environment, as well as arrangements for data processing, set out in the data permit'.

If the review of the application has a positive outcome, the HDAB releases a data permit, which is valid for no longer than 10 years. This period of validity can be extended up to 10 years if justified. HDABs must make information on the conditions under which electronic health data are made available for secondary use publicly available. The data holders must then 'make relevant electronic health data referred to in Article 51 available upon request to the health data access body, in accordance with a data permit' (Article 60(1) EHDS). When accessing such data in a secure processing environment, the health data user is bound to the terms of the data permit (Article 61(1) EHDS). Health data users are not allowed to provide access to the electronic health data to third parties not mentioned in the data permit (Article 61(2) EHDS) or re-identify (or attempt to re-identify) the natural persons to whom the electronic health data relate (Article 61(3) EHDS).

In the scenario under consideration, the actual application of the EHDS data access procedure would depend on the national legal arrangements regarding electronic health records (EHRs) and other relevant categories of electronic health data. If the Ministry of Health has 'the right or obligation, in accordance with applicable Union or national law and in its capacity as a controller or joint controller, to process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policy making, official statistics or patient safety or for regulatory purposes' (Article 2(2)(t)(i) EHDS), then they can qualify as a data holder under the EHDS. In this case, the company seeking access to electronic health data would need to apply to an HDAB for a permit to access the data. In the context of a cross-border public health emergency, it would not be difficult for the company to indicate in the data access application that access is requested for research purposes contributing to public health, under Article 53 of the EHDS Regulation, especially if they intend to collaborate with the Ministry of Health.

Conversely, suppose the Ministry of Health does not have the right or obligation to process the relevant data under Article 2(2)(t)(i) EHDS. In that case, they need to apply for data access from the actual data holder. In doing so, the Ministry would likely indicate in the data access application that they are pursuing public interest / public health purposes in connection with a cross-border health threat. However, the Ministry could then be allowed to share and process the data with the company only if the data permit states so.

In either case, the HDAB would play a key role in scrutinising the proposed data sharing operation, ranging from the intended use of the data and how this contributes to the purpose stated by the applicant in the data access application, to the data concerned, and information on ethical aspects. Importantly,

the HDAB must assess whether the data will be processed based on a valid legal basis under Article 6 of the GDPR and in compliance with other key GDPR principles (such as purpose limitation and data minimisation). Also, if access to the data is sought for research purposes, the HDAB must check that the stated research purpose 'contributes to public health' in accordance with Article 53(1)(e) of the EHDS. Thus, HDABs do have the tools to limit corporate access to electronic health data.[74]

Once a data permit is released, the EHDS does convey some simplifications that can facilitate G2B data sharing. In particular, once the HDAB releases a data permit, the data holder has a legal obligation to make the data available. Therefore, this data sharing operation relies on the legal basis referenced by Article 6(1)(c) of the GDPR. Also, the EHDS enables the data user to rely on the exceptions under Article 9(g) to (j) of the GDPR. Finally, the patient's consent is not required as an opt-out system applies, and the EHDS transparency obligations are less demanding than those set out in the GDPR.

However, as already mentioned, all this applies only after the HDAB has checked that the processing of data by the user complies with the GDPR key principles of lawfulness, purpose limitation, and data minimisation. More generally, the processing of the data by the data user(s) in accordance with the terms set out in the data permit falls squarely under the remit of all the GDPR principles and rules. This is irrespective of whether these latter are explicitly referenced by the EHDS or not. This is because the EHDS does not derogate from but 'specifies and complements the rights' of the GDPR (Article 1(2)(a) EHDS). Thus, the Ministry of Health and the company would need to rely on a valid legal basis under Article 6 of the GDPR, inform the data subjects, and be bound to the limitations foreseen for the further processing of the data. Naturally, they could use the GDPR research or public interest / public health exemptions; however, to do so, they would be required to implement appropriate safeguards or otherwise defined measures to protect the rights of the data subjects.

It follows that the EHDS is unlikely to substantially lower the level of protection already offered by the GDPR against excessive G2B data sharing operations. In fact, the HDAB's responsibility to assess whether the requested access to the data is actually in the public interest adds a further layer of *ex-ante* control on the data sharing operation that is not foreseen in the GDPR, where the principle of accountability emphasises the role of the data controller(s), subject to potential *ex-post* action by competent authorities.

74 Marelli *et al.*, *supra* note 73.

8 Conclusions

The analysis so far has helped answer several interconnected research questions, which can be summarised as follows. Regarding the first research question (i.e., whether an EU Member State could follow the steps of the Israeli MoH in circumventing data protection and research regulations), the analysis indicates that such circumvention would face substantial legal obstacles. On one hand, the EU framework's reliance on flexible definitions creates avenues for strategic interpretation during emergencies. The distinctions between personal and anonymous data, as well as between research and non-research, remain open to interpretation and are context dependent. On the other hand, we found that DPAs and ethics committees have the capacity to assert jurisdiction over large-scale G2B data sharing operations similar to the Israel–Pfizer agreement. Notably, the GDPR re-identifiability standard under Recital 26 makes it challenging to convincingly argue that aggregated health data, segmented by multiple demographic criteria, is truly anonymous. The EDPB's cautious stance on anonymisation, especially in research contexts, suggests that large epidemiological datasets are likely to qualify as personal data requiring GDPR compliance. Furthermore, the broad concept of scientific research under EU law covers observational studies and real-world evidence collection. This makes it difficult to argue that vaccine effectiveness monitoring lies outside the scope of research regulations.

Regarding the second research question (in essence, whether the GDPR offers sufficient protection against extensive mass-scale data sharing despite its many flexibilities when data is processed for research, public interest, or public health reasons), the analysis reveals a framework that imposes several meaningful constraints on governments and corporate actors. These include requiring legal bases or exceptions under Article 9 GDPR with a sufficiently clear basis in the law, making relevant agreements publicly available, mandating data protection impact assessments for high-risk processing, and requiring prior consultation with data protection authorities.

Regarding the third research question (i.e., whether the DGA and EHDS could facilitate excessive mass-scale data sharing operations), we found that the EHDS actually adds additional procedural safeguards through health data access bodies and standardised review processes, rather than weakening existing protections.

However, this analysis also reveals a fundamental tension in current EU data governance. The multi-layered approval processes established by these frameworks do offer essential safeguards (health data access reviews, data protection impact assessments, and ethics committee approvals). Yet, they also

create procedural complexities that can delay data-driven responses to public health emergencies.

One potential solution to this conundrum could be to develop pre-approved emergency protocols during non-emergency periods. Such protocols should establish clear procedures for data sharing with specific categories of private partners. However, procedural solutions alone are insufficient. The challenge lies in developing data sharing and data governance mechanisms that can respond rapidly to emergencies while maintaining legitimacy and public trust.

This suggests the need for approaches that incorporate meaningful public engagement in the design, evaluation and review of emergency protocols, moving towards more collective forms of democratic governance over data use. This is a promising avenue for further research.

Acknowledgements

The authors thank the Department of Innovation, Research University and Museums of the Autonomous Province of Bozen/Bolzano for covering the Open Access publication costs.