Remove obstacles to sharing health data with researchers outside of the European Union

COVID-19 has shown that international collaborations and global data sharing are essential for health research, but legal obstacles are preventing data sharing for non-pandemic-related research among public researchers across the world, with potentially damaging effects for citizens and patients.

Heidi Beate Bentzen, Rosa Castro, Robin Fears, George Griffin, Volker ter Meulen and Giske Ursin

International sharing of pseudonymized personal data among researchers is key to the advancement of health research and is an essential prerequisite for studies of rare diseases or subgroups of common diseases to obtain adequate statistical power.

Pseudonymized personal data are data on which identifiers such as names are replaced by codes. Research institutions keep the 'code key' that can link an individual person to the data securely and separately from the research data and thereby protect privacy while preserving the usefulness of data for research. Pseudonymized data are still considered personal data under the General Data Protection Regulation (GDPR) 2016/679 of the European Union (EU)[1] and, therefore, international transfers of such data need to comply with GDPR requirements. Although the GDPR does not apply to transfers of anonymized data, the threshold for anonymity under the GDPR is very high; hence, rendering data anonymous to the level required for exemption from the GDPR can diminish the usefulness of the data for research and is often not even possible.

The GDPR requires that transfers of personal data to international organizations or countries outside the European Economic Area (EEA)—which comprises the EU Member States plus Iceland, Liechtenstein and Norway—be adequately protected. Over the past two years, it has become apparent that challenges emerge for the sharing of data with public-sector researchers in a majority of countries outside of the EEA, as only a few decisions stating that a country offers an adequate level of data protection have so far been issued by the European Commission. This is a problem, for example, with researchers at federal research institutions in the United States. Transfers to international organizations such as the World Health Organization are similarly affected[2]. Because these obstacles ultimately affect patients as beneficiaries of research, solutions are urgently needed. The European scientific academies have recently published a report explaining the consequences of stalled data transfers and pushing for responsible solutions[3] (Table 1).

A balancing act

From identifying complex pathways to understanding and preventing diseases, to comparing determinants of disease outcomes across populations and improving health care, data sharing is essential for health research and for citizens and patients. At the same time, appropriate protection of personal health data, as envisaged by the GDPR[1], is key to fulfilment of the fundamental right to protection of personal data as enshrined in the EU Charter of Fundamental Rights[4], and is essential for fostering trust among citizens and patients.

Although both aims—protection and sharing of data—should be addressed, it has become apparent that there are statutory conflicts between EU fundamental rights and data-protection legislation on the one hand, and the legislation of other countries on the other hand, that create considerable obstacles to the transfer of data outside the EEA. Counterintuitively, these problems are greater when data are shared with researchers at public institutions outside of Europe, despite the paramount importance of public institutions in advancing research in the interest of patients and the public at large.

Scientific academies in Europe (the European Academies Science Advisory Council, the Federation of European Academies of Medicine, and the European Federation of Academies of Sciences and Humanities)[3] have joined forces to call attention to the challenges that affect not only European scientists but collaborators worldwide. Science is and should be a truly global endeavor that requires that reliable data be made available to researchers across geographical borders[5]. The protection of research participants' personal data is a potential concern with data transfer, but the joint report[3] found strong support from patients for using data for scientific research[6], including through a roundtable with stakeholders.

Issues about data sharing outside the EEA have been raised in the past[7], but these have become even more urgent due to recent developments, such as the Court of Justice of the European Union's 2020 *Schrems II* judgment[8] and subsequent guidance from the European Data Protection Board (EDPB). The *Schrems II* judgment[8] invalidated the EU–US Privacy Shield because US surveillance legislation, given priority over Privacy Shield, was found to be in violation of the EU Charter of Fundamental Rights[4]. The court decided that the European Commission's standard contractual clauses (SCCs) are still valid as a transfer mechanism, but these must be accompanied by thorough legal assessments and supplementary measures, which complicates transfers. There is a growing need for collaborative research to address the long-term health effects of the COVID-19 pandemic, as well as research on cancer and other diseases, many of which have poor prognoses and require more health data (Fig. 1). New research and innovation opportunities can come from big data and artificial intelligence, but they require suitable mechanisms for sharing research data across borders[9].

Sharing is fundamental

International data transfers—which comprise both transfer of data and provision of remote access to data[10]—are necessary for studying and comparing genetic and epidemiological risk factors for the optimization of prevention or treatment. Pooled analyses of data from many countries are particularly needed for sufficient statistical power to be obtained in studies of rare diseases or rare subgroups of common diseases. Additionally, sharing of samples and data from European citizens is essential for ensuring that findings from international studies apply to European populations,

Table 1 | Key messages from International Sharing of Personal Health Data for Research[3]

Key message	Explanation
Health research is crucial and its value should be emphasized	The value of health research should be highlighted and better communicated; health research benefits patients, population health, the development of health-care systems, social cohesion and stability.
Pseudonymized personal health data for public-sector research should be shared outside of the EEA	Sharing of pseudonymized personal health data with public-sector researchers outside of the EEA makes effective use of limited resources and maximizes the value of contributions made to research by patients and volunteers.
Health data must be shared safely and efficiently to advance research	Addressing potential privacy concerns about data sharing is critical for taking account of patients' views, as well as for building trust in research and researchers.
Implementation of the GDPR has resulted in impediments to data sharing with researchers outside the EEA	Sharing of data with researchers outside of the EEA is currently affecting both the direct transfer of data and remote access to data at its original location, as well as secondary uses of the data by foreign institutions.
Increased commitment is needed to overcome the barriers to sharing data, preferably under Article 46 of the GDPR	Solutions for sharing data for research outside of the EEA call for operational options within Article 46 of the GDPR, as well as additional guidance by the EDPB, and tangible examples to provide further guidance for health researchers.
Other methodological and technical quality issues need to be resolved	Other issues, such as interoperability in the use of data and other methodological and technical quality issues, need to be addressed to facilitate efficient and secure data sharing for research.
Privacy-enhancing technologies do not offer a complete solution for all international transfers of health data for research	Although privacy-enhancing technologies can improve data security, their use does not circumvent the data-transfer requirements of the GDPR, except in the cases in which there is no transfer of personal data and no remote access.

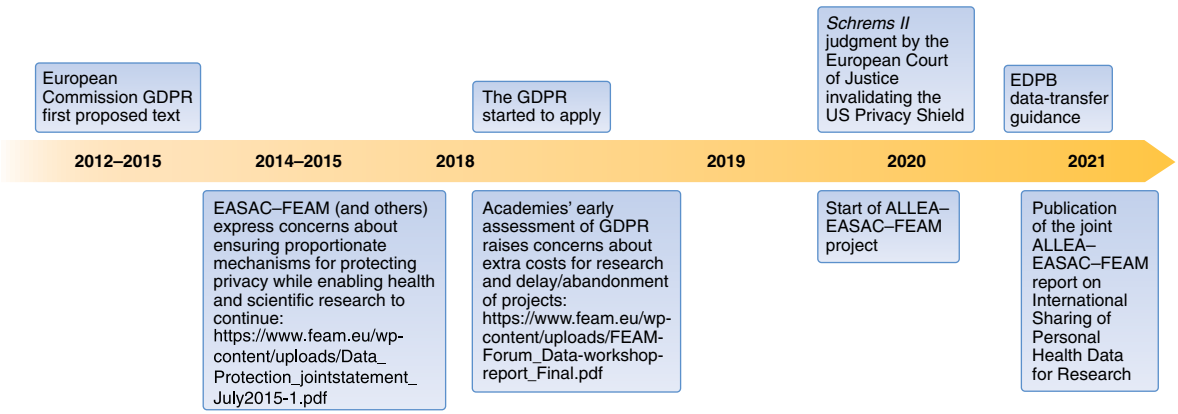

Fig. 1 | Involvement of academies in the international sharing of health data for research. A timeline of European data-protection legislation and the involvement of European academies.

with their genetic composition and specific lifestyle factors.

Increasingly, international researchers are provided temporary remote access to trusted research environments so data can be securely accessed without leaving the host country. GDPR requirements still apply, as remote access is also considered international data transfer[10]. Furthermore, if European data can only be accessed remotely, while the rest of the international data can be combined in one pooled analysis, this is cumbersome for researchers and could result in European studies' being dropped.

Privacy-enhancing technologies such as homomorphic encryption, differential privacy, federated analyses and use of synthetic data offer new ways for protecting the privacy of individuals[11]. These technologies can be helpful, but they have limitations, such as the extent to which they can be applied to real-world challenges, the noise level, or how well they protect privacy when the number of data points from each country or study is small. Combining multiple technologies may be key to reducing risk[12]. Moreover, the use of privacy-enhancing technologies did not circumvent the need to transfer data in some studies.

Legal obstacles

An operational mechanism for sharing pseudonymized health data with public-sector institutions is currently lacking for many countries outside of the EEA[7]. This is the case for several research-intensive countries and key partners for European researchers, as the European Commission has so far recognized only a few countries as providing 'adequate' protection of personal data[13]. After Brexit, the transfer of health data for research collaborations with the UK has also been at risk. An 'adequacy decision' for transfers of personal data from the EU to the UK has been issued by the European Commission and has recently been approved by EU Member States' representatives[14], but it includes a 'sunset clause' that limits its duration to four years, at which time the adoption process needs to start again if the commission decides to renew the adequacy finding.

There are about 5,000 collaborative projects between the US National Institutes

Table 2 | GDPR data-transfer mechanisms

International transfers: options under the GDPR	Data-transfer mechanism	Limitations
(1) Best option: adequacy	Adequacy: the European Commission has decided that an adequate level of protection is ensured (Article 45, GDPR)	• This is available only for Andorra, Argentina, Canada (only commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland, the UK and Uruguay. The European Commission has also launched the procedure to adopt adequacy decisions for South Korea. • No adequacy decision are in place for the United States (or other countries not mentioned above). • The EU–US Privacy Shield Framework (applying to self-certified US businesses) has been invalidated by the Court of Justice of the EU.
(2) Second-best option: appropriate safeguards	Appropriate safeguard: bespoke contract between public bodies (Article 46(2)(a), GDPR)	• EDPB guidelines exist but introduce statutory conflicts with US federal law.
	Appropriate safeguard: authorized administrative arrangement between public bodies (Article 46(3)(b), GDPR)	• EDPB guidelines exist but introduce statutory conflicts with US federal law. • There is a lengthy authorization process.
	Appropriate safeguard: SCCs adopted by the European Commission (Article 46(2)(c), GDPR)	• SCCs are operational and valid but include clauses in statutory conflict with US federal law. • Sstatutory conflicts remain in the newly revised SCCs and scientific research exceptions that mirror the GDPR are not included.
	Appropriate safeguard: SCCs adopted by a supervisory authority and approved by the European Commission (Article 46(2)(d), GDPR) Appropriate safeguard: approved code of conduct (Article 46(2)(e), GDPR) Appropriate safeguard: approved certification (Article 46(2)(f), GDPR) Appropriate safeguard: authorized bespoke contract in which one or both parties are not a public body (Article 46(3)(a), GDPR)	• There is a lack of EDPB guidelines (these are included in the 2021/2022 EDPB work program). • There is a lengthy approval process.
Supplementary measures	Supplementary measures to be used in addition to the appropriate safeguard if necessary to achieve an adequate level of data protection (CJEU *Schrems II* judgment and EDPB recommendations 01/2020 and 02/2020)	• These require an assessment of the law in the country to which the data is transferred. • Supplementary measures are to be added if the law in the country to which the data is transferred impinges on the effectiveness of the appropriate safeguard. • EDPB recommendations exist, and although they are non-exhaustive, they do not offer feasible options for scientific health research.
(3) Last resort: derogations for specific situations	Derogation: explicit consent following information about the possible risks of the transfer (Article 49(1)(a), GDPR)	• This can be used only exceptionally; e.g., for initial transfer of pandemic data. • This cannot be used for repetitive transfers that are part of a long-lasting research project, even in a pandemic, per EDPB guidance. • Consent can be withdrawn any time. • Blanket consent for non-EEA transfer is not valid. • Use of this derogation entails increased risk for the research participant.
	Derogation: public interest (Article 49(1)(d), GDPR)	• This requires a basis in EU or Member State law. • This can only be used exceptionally; e.g., for initial transfer of pandemic data. • This cannot be used for repetitive transfers that are part of a long-lasting research project, even in a pandemic, per EDPB guidance. • Use of this derogation entails increased risk for the research participant.
	Derogation: vital interests (Article 49(1)(f), GDPR)	• This is to be used in situations in which transfers are necessary to protect vital interests, and the research participant is physically or legally incapable of providing consent. • It must be to provide essential healthcare to an individual person, not for general medical research in which the advantages to people's health are in the future. • Use of this derogation entails increased data-protection risk for the research participant.

Continued

Table 2 | GDPR data-transfer mechanisms (Continued)

International transfers: options under the GDPR	Data-transfer mechanism	Limitations
	Derogation: where no other data-transfer mechanism can be used (Article 49(1)(2), GDPR)	• This is a very narrow derogation that can be used only if no other transfer mechanism, including other derogations, can be used and a number of additional conditions are met. • The transfer cannot be repetitive. • The transfer must involve only a limited number of research participants. • The transfer must be necessary for the purposes of compelling legitimate interests pursued by the research institution that are not overridden by the interests and freedoms of the research participant. • The research institution must, on the basis of an assessment of all circumstances of the transfer, provide suitable safeguards for protection of personal data. • The supervisory authority must be informed of the transfer. • The research participants must be informed of the transfer and the compelling legitimate interests pursued. • Use of this derogation entails increased risk for the research participant.

Overview of available GDPR data-transfer mechanisms for sharing personal data from the EEA to a non-EEA country for scientific research purposes, with data transfers from the EEA to the Unites States as an example. CJEU, Court of Justice of the EU.

of Health (NIH) and EEA countries[15]. At least 40 clinical and observational studies on risk factors and exposures for cancer have been suspended or delayed because of the current legal challenges[16]. Multiple research projects within the National Cancer Institute Cohort Consortium, where cohort studies from all over the world participate, have also been suspended or delayed, as the European participating studies cannot proceed with data transfers[7]. Statens Serum Institut in Denmark halted transfers of personal data to the NIH as part of a long-standing collaboration on diabetes due to the lack of an operational data-transfer mechanism[3,17]. The World Health Organization's International Agency for Research on Cancer has been negatively affected, as it cannot receive research data from collaborating European studies[2,18].

Without an adequacy decision, the GDPR requires appropriate safeguards (Article 46) or, when such safeguards are unavailable, resorts to derogations for specific situations (Article 49). The use of derogations is considered an exceptional measure, as it places increased risk on the research participants, and the EDPB has reiterated that whereas initial transfers using Article 49 derogations were justified for initial COVID-19 research activities, other repetitive transfers and long-lasting research related to the ongoing pandemic still need to rely on appropriate safeguards under Article 46 (refs. [19,20]) (Table 2).

Safeguards

The appropriate safeguards envisaged by Article 46 of the GDPR include SSCs, administrative arrangements between public bodies, bespoke contracts, and codes of conduct. These safeguards could potentially provide the best options for workable international transfers with public-sector researchers. However, due to conflicts with US laws, the European Commission's SCCs are unavailable for key public research partners, such as the NIH[21]. EDPB guidance for the use of other mechanisms envisaged under Article 46 (e.g., administrative arrangements and bespoke contracts) are also in contradiction of US or other foreign laws[22], with the main difficulty in the United States being that federal institutions are protected by sovereign immunity. Furthermore, some of the appropriate safeguard mechanisms require lengthy approval processes or lack guidance from the EDPB.

Supplementary measures may be needed, in addition to the chosen Article 46 mechanism, to achieve an adequate level of data protection[8,10], but it should be possible to tailor these measures to enable health research with a wide range of scientific methods[23]. The EDPB considers pseudonymization a sufficient supplementary measure for data protection, but it describes pseudonymization in a manner that is not possible to achieve for health-research datasets that contain many variables or unique identifiers[10,23]. A range of complementary supplementary measures, including encryption and other privacy-enhancing technologies and legal and organizational measures, would provide better protection for research participants while being practically feasible for health research[23].

Implications for researchers

Previous attempts to solve international transfers of data outside of the EEA, such as the EU–US Privacy Shield Framework, in which entities could certify to provide an adequate level of data protection, focused on the private sector, despite the importance of public-sector research. Privacy Shield has now been invalidated by the *Schrems II* judgment[8]. In this decision, the court reiterated that although SCCs are a valid data-transfer mechanism, a complex legal analysis should be undertaken to exclude conflicts between the laws of the recipient country and the requirements of the SCCs. This is the case with US federal law, which, among other legal conflicts, blocks individual judicial redress for non-US citizens and residents[24].

The way forward

GDPR has become a privacy standard other countries seek to follow, which gives the EU an important role in the global discussion on privacy and the necessity of data sharing for health research for the benefit of society. This places the EU in a position to exert pressure on other countries to reform their regulations to enable reciprocity in privacy-enhanced data sharing. For this data sharing to happen, the EU must now work with other countries to resolve statutory conflicts, but this will also require cooperation from those countries. The European Parliament has urged the European Commission not to adopt any new adequacy decision in relation to the United States unless meaningful legal reform is first introduced in the United States[25] The United States should be encouraged to establish enforceable data subject rights and effective legal remedies for European and other non-US research participants whose

data are processed by US researchers. The voice of the health-research community must be heard by decision-makers at the national level, at the EDPB, and within the EU Commission Directorates-General involved, such as in the areas of justice, health and research. Without a quick resolution, European research potential will not be realized, and European citizens will fall behind. ❐

Heidi Beate Bentzen[1,2,8], Rosa Castro[3,8]✉, Robin Fears[4], George Griffin[5], Volker ter Meulen[4] and Giske Ursin[2,6,7]

[1]Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, Oslo, Norway. [2]Cancer Registry of Norway, Oslo, Norway. [3]Federation of European Academies of Medicine, Brussels, Belgium. [4]European Academies Science Advisory Council, German National Academy of Sciences Leopoldina, Halle (Saale), Germany. [5]Department of Infectious Diseases and Medicine, St. George's University of London, London, UK. [6]Institute of Basic Medical Sciences, University of Oslo, Oslo, Norway. [7]Department of Preventive Medicine, Keck School of Medicine, University of Southern California, Los Angeles, Los Angeles, CA, USA. [8]These authors contributed equally: Heidi Beate Bentzen, Rosa Castro.

✉*e-mail: rosa.castro@feam.eu*

Published online: 02 August 2021

https://doi.org/10.1038/s41591-021-01460-0

References

1. European Union. *EUR-Lex* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 (2016).
2. European Data Protection Board. https://edpb.europa.eu/system/files/2021-05/edpb_letter_out2021-0086_un_en.pdf (2021).
3. The European Academies Science Advisory Council, the Federation of European Academies of Medicine & the European Federation of Academies of Sciences and Humanities. https://doi.org/10.26356/IHDT (2021).
4. European Union. *EUR-Lex* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT (2012).
5. Wilkinson, M. D. et al. *Sci. Data* **3**, 160018 (2016).
6. Richter, G. et al. *Eur. J. Hum. Genet.* **27**, 841–847 (2019).
7. Ursin, G. et al. *Lancet* **394**, 1902–1903 (2019).
8. Court of Justice of the European Union. *InfoCuria Case-law* https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (2020).
9. Shilo, S., Rossman, H. & Segal, E. *Nat. Med.* **26**, 29–38 (2020).
10. European Data Protection Board. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (2021).
11. Royal Society. https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf (2019).
12. Scheibner, J. et al. *J. Med. Internet Res.* **23**, e25120 (2021).
13. European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 2 May 2021).
14. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183 J (28 June 2021)
15. Eiss, R. http://www.iscintelligence.com/archivos_subidos/robert_eiss_gdpr_us-eu_cooperation_in_biomedical_science_isc_gdpr_seminar_19_nov_2019.pdf (2019).
16. Eiss, R. *Nature* **584**, 498 (2020).
17. Rabesandratana, T. *Science* https://doi.org/10.1126/science.aba2926 (2019).
18. United Nations Secretariat on behalf of United Nations System Organisations. https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf (2020).
19. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (2018).
20. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (2020).
21. Peloquin, D., DiMaio, M., Bierer, B. & Barnes, M. *Eur. J. Hum. Genet.* **28**, 697–705 (2020).
22. Norwegian Institute of Public Health & Cancer Registry of Norway. https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/edpb_guidelines_niph_crn_comments_20200518.pdf (2020).
23. Nordic Society of Human Genetics and Precision Medicine. https://edpb.europa.eu/sites/edpb/files/webform/public_consultation_reply/nshg-pm_comments_edpb_recommendations_012020.pdf (2020).
24. Bovenberg, J., Peloquin, D., Bierer, B., Barnes, M. & Knoppers, B. M. *Science* **370**, 40–42 (2020).
25. European Parliament. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0256_EN.html (2021).

Acknowledgements

We acknowledge the support of the European Academies Science Advisory Council, the Federation of European Academies of Medicine, and All European Academies, as well as all members of the working group that contributed to writing the joint report[3].

Author contributions

All authors contributed to writing this Comment.

Competing interests

The authors declare no competing interests.