Maximizing the GDPR potential for data transfers: first in Europe

Heidi Beate Bentzen,[a,b] Hilde Kvammen Olav,[a] and Giske Ursin[a,c,d,*]

[a]Cancer Registry of Norway, Oslo, Norway
[b]Centre for Medical Ethics, Faculty of Medicine, University of Oslo, Oslo, Norway
[c]Institute of Basic Medical Sciences, Faculty of Medicine, University of Oslo, Oslo, Norway
[d]Department of Preventive Medicine, Keck School of Medicine, University of Southern California, Los Angeles, CA, USA

The Lancet Regional Health - Europe 2023;27: 100600
Published Online 6 March 2023
https://doi.org/10.1016/j.lanepe.2023.100600

During the pandemic, rapid international data sharing was key to finding medical solutions. Legal derogations made some pandemic data transfers possible.[1] However, non-pandemic medical research, including cancer research, follows regular legal rules, and these rules currently create data transfer stalls, delaying medical advancements.[1]

Data transfers from the European Union (EU) to federal institutions in the United Stated (US) for medical research are currently impeded for legal reasons.[2–4] Transfers to most of the US private sector can proceed provided appropriate safeguards are in place, but presently, US cloud providers such as Amazon Web Services, Google Cloud, and Microsoft Azure that provide large-scale, advanced data processing solutions can often not be used.[5]

Legal challenges therefore affect clinical trials when 1) the pharmaceutical company uses a US subcontractor providing a cloud-based analysis platform, and/or 2) legally mandated information including safety data must be reported to regulatory authorities such as the US Food and Drug Administration (FDA).

In the following, we describe the use of a very narrow safety valve derogation in the EU General Data Protection Regulation (GDPR) 2016/679 to enable such transfers. The Norwegian Data Protection Authority (DPA) concurred with our use of this legal option. To our knowledge, this is the first time-use of this derogation in Europe.

Current situation for clinical trials

The GDPR regulates processing of personal data, including the collection, analysis and storage of pseudonymized (key-coded) data for scientific research purposes. The objective of the GDPR is twofold – to achieve both protection and free movement of personal data within the European Economic Area (EEA). When personal data is to be transferred outside the EEA, there are rules in the GDPR to ensure that the EEA level of data protection is upheld, see Fig. 1.

With the application of the GDPR, the Court of Justice of the EU (CJEU) *Schrems II* judgment, and subsequent guidance from the EEA DPAs in the European Data Protection Board (EDPB), two legal problems materialized: 1) US cloud providers and other US electronic communication service providers can as a main rule no longer be used[3]; and 2) Previously used legal data transfer mechanisms provided for in domestic European laws were repealed and already transferred data must rely on another legal transfer mechanism. In attempting to identify a new legal data transfer mechanism, it has become clear that because US federal institutions such as the FDA and the National Institutes of Health are protected by sovereign immunity, it is, as a main rule, no longer possible to transfer personal data from the EEA to them.[5,6]

Since the European Commission has not decided that the US offers an adequate level of protection to that in the EU (Article 45 of the GDPR), such data transfers must as a general rule be based on provision of appropriate safeguards (Article 46 of the GDPR), see Fig. 1.

The use of US cloud services

It is often possible to use the EU Standard Contractual Clauses (SCC) for international transfers or another of the Article 46 appropriate safeguards for data transfers to US pharmaceutical companies. However, if the company does not use an internal dedicated server, but a cloud-based platform from a US provider, appropriate safeguards cannot be established.[6] This is because US intelligence legislation, found by the CJEU to be in violation of EU fundamental rights, allows US authorities legal access to the data the US cloud providers process.[5] Supplementary measures of a technical or organizational nature cannot usually remedy this challenge.[6]

The US and the European Commission have announced a new Trans-Atlantic Data Privacy Framework, which, when in place, will likely re-enable use of US cloud providers. The European Commission has published a draft adequacy decision, which is now subject to an adoption process lasting until the summer of 2023.[7] However, Schrems has already announced the framework will be challenged in Court unless it meets EU legal requirements, noting that he does not see how the draft decision will survive a challenge before the Court of

*Corresponding author.
E-mail address: gu@kreftregisteret.no (G. Ursin).

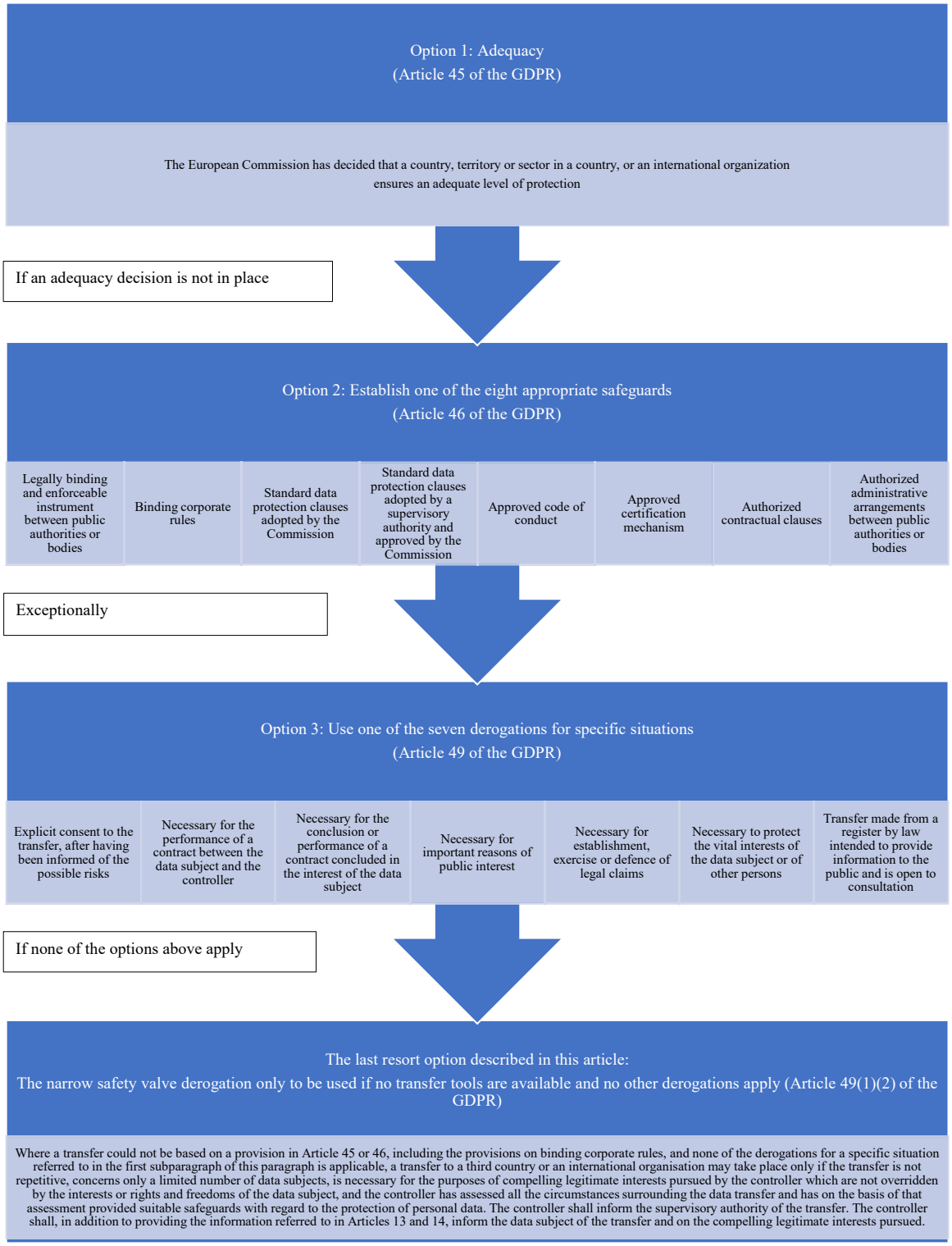

Fig. 1: **The tiered process of establishing a legal transfer mechanism for data transfers from the European Economic Area to non-European Economic Area according to the GDPR.**

Justice of the European Union.[8] This implies that the use of US cloud providers, including their EEA servers, will likely be subject to longer-term legal uncertainty.

Transfer of individual level safety data to the FDA

The other challenge relates to the requirement of regulatory agencies to obtain individual level data in certain instances from pharmaceutical companies. This is a safety precaution, to ensure that companies do not overlook possible hazards.

One of the requirements for using any of the eight appropriate safeguards in Article 46 of the GDPR, is that enforceable data subject rights and effective legal remedies are in place. The FDA and other US federal institutions provide this for US citizens and permanent residents in the United States Privacy Act of 1974, but not for other individuals. Thus, the FDA does not meet the requirements for establishment of an Article 46 appropriate safeguard for potential onward transfers of individual level data. The proposed Trans-Atlantic Data Privacy Framework will not facilitate data transfers from the EEA to US federal institutions and will thus not solve this problem.

The seven derogations (exceptions) for specific situations cannot be used

Derogations in Article 49 of the GDPR, are last resort options only to be used when there is no adequacy decision and appropriate safeguards cannot be established.[9] The derogations place additional data protection risk on the research participants. This risk is acceptable only in rare instances, for instance if a specific individual's life is at stake.

One of the derogations is explicit consent to specified data transfers after the participant has been informed of the risk of the transfer. However, consent cannot be used as a transfer mechanism to the FDA or other non-EEA country regulatory authorities in clinical trials, as the participants cannot withdraw this consent. Note that consent to international data transfer is different from informed consent to research participation.

The cumulative conditions of Article 49(1)(2) GDPR	Recommendations for how to fulfill the conditions
The transfer:	
– could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable	Provide an explanation for why any other rules cannot not be used (as summarized above).
– is not repetitive	Clinical trials often require several data transfers, and some may have been conducted prior to 2018, when the GDPR started to apply. If so, argue that the transfers constitute one comprehensive study set, and explain why multiple transfers over time are necessary. For instance, multiple transfers may be necessary to quickly identify any failure in medication effect or safety.
– concerns only a limited number of data subjects	List the exact number of research participants, for instance 650.
– is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject	Explain the specific compelling legitimate interests for which the transfers must take place. For instance, argue that the transfer is necessary for the compelling legitimate interest of necessary surveillance, required for regulatory approval, and hence for public health. Refer to Recital 113 GDPR, which states that if the transfer is for scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration. If relevant, you may also add the assumption that it is also in the participants' interest, for instance to increase the knowledge of a medication's efficacy, reliability and safety. Refer to measures implemented to reduce the privacy risk for the participants.
The controller:	
– has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data	Conduct a risk assessment in collaboration with the data importer where all circumstances related to the transfer and the implications to the data subjects are considered. This should include the nature of the data, the purpose and duration of the processing, and the situation in the importing country. Based on the assessment, describe the mitigating measures implemented to protect fundamental rights and freedoms of the participants, for instance pseudonymization.
– shall inform the supervisory authority of the transfer	Send your legal assessment to the DPA, alongside a copy of the information letter to the research participants.
– shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued	Send letters to all participants with the required information on the transfer, mitigating measures, and the compelling legitimate interests pursued.
According to paragraph 6 of Article 49, the controller or processor shall also document the assessment as well as the suitable safeguards in the records referred to in Article 30	Controllers, meaning the ones responsible for deciding the purpose and means of the data processing, are obliged to maintain a record of data processing activities under their responsibility. Document and share your legal assessment with the DPA.

Table 1: **The conditions of Article 49(1)(2) of the GDPR and how to fulfill them.**

The European Commission included a provision in the new SCC allowing onward transfers from pharmaceutical companies to regulatory authorities.[10] However, in some cases, the SCC cannot be used, for instance where the data importer uses a US cloud provider.

We have also asked the Norwegian DPA specifically whether the derogation in Article 49(1)(e), which is phrased quite similarly to the SCC provision, could be used for an onward transfer to regulatory authorities where the SCC could not be used. Their response was not to use Article 49(1)(e) for this onward transfer.

Our recommendation

Where there is no adequacy decision, no appropriate safeguard, and the seven derogations for specific situations do not apply, there is a very narrow safety valve derogation in the GDPR in Article 49(1)(2).

This derogation can only be used in residual cases where specific, cumulative conditions are met. Formal DPA acceptance is not required. However, we requested feedback for the first-time use of the derogation, as the DPA has corrective power to suspend data flows. The Norwegian DPA agreed with our use of this derogation, including that none of the Article 46 GDPR data transfer mechanisms nor other Article 49 derogations were applicable. Although there is no guarantee, it is likely that other DPAs would share this assessment. Table 1 describes each of the legal conditions for using the safety valve derogation in Article 49(1)(2) and recommendations for how to address them, based on our successful experience. The Table thereby creates a legal step-by-step recipe and a useful tool to re-enable some data transfers.

Medical research needs sustainable legal data transfer mechanisms. Although using the narrow Article 49(1)(2) derogation is resource-demanding and not a panacea for medical research transfers in general, it may at least – and at last – legally re-enable data transfers in some clinical trials that are now stalled. And that is a step in the right direction.

Contributors

H.B.B. drafted the manuscript, and H.K.O. and G.U. edited it for content. All three authors approved the final version.

Declaration of interests

The Cancer Registry of Norway has an ongoing research collaboration with MSD to study the impact of the HPV vaccine in Norway. This paper describes the legal data sharing solution used for transfer of data for a clinical trial under this collaboration. The authors declare no other conflicts of interest.

Acknowledgements

The authors thank trial partner site Principal Investigators Mari Nygård, Bo Terning Hansen, Espen Enerly and Thea Falkenthal, and trial sponsor MSD's Deputy Chief Privacy Officer Christopher Foreman, for constructive dialogue.

References

1 European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. Adopted on 21 April 2020.
2 Bentzen HB, Castro R, Fears R, Griffin G, ter Meulen V, Ursin G. Remove obstacles to sharing health data with researchers outside of the European Union. *Nat Med*. 2021;27(8):1329–1333. https://doi.org/10.1038/s41591-021-01460-0.
3 Bentzen HB. Exchange of human data across international boundaries. *Annu Rev Biomed Data Sci*. 2022;5:233–250. https://doi.org/10.1146/annurev-biodatasci-122220-110811.
4 U.S. Food and Drug Administration, Messick H. *How a European data law is impacting FDA*; 9 August 2022. Available at: https://www.fda.gov/international-programs/global-perspective/how-european-data-law-impacting-fda. Accessed February 6, 2023.
5 Court of Justice of the European Union Grand Chamber. *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Case C-311/18* 16 July 2020. ECLI:EU:C:2020:559.
6 European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021.
7 European Commission. *Adequacy decision for the EU-US data privacy framework*; 13 December 2022. Available at: https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en. Accessed February 6, 2023.
8 *Noyb. Statement on US adequacy decision by the European Commission*; 13 December 2022. Available at: https://noyb.eu/en/statement-eu-comission-adequacy-decision-us. Accessed February 6, 2023.
9 European Data Protection Board. Guidelines 2/2018 on derogations of Article 49 under regulation 2016/679. Adopted on 25 May 2018.
10 European Commission. *The new standard contractual clauses – questions and answers*; 25 May 2022. Available at: https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf. Accessed February 6, 2023.