Clarifying the legal requirement for cross-border sharing of health data in POPIA: Recommendations on the *draft Code of Conduct for Research*

L Abdulrauf,[1,2,3] LLB, BL, LLM, LLD; **A Adaji,**[1,4] LLB, BL, LLM, PhD; **H Ojibara,**[5] LLB, BL, LLM, PhD

[1] *School of Law, University of KwaZulu-Natal, Durban, South Africa*
[2] *Department of Public Law, University of Ilorin, Nigeria*
[3] *Center for Advanced Study in the Behavioural Sciences, Stanford University, California, USA*
[4] *College of Law, Osun State University, Ifetedo, Nigeria*
[5] *Department of Private and Property Law, University of Ilorin, Nigeria*

Corresponding author: *L Abdulrauf (abdulrauf@unilorin.edu.ng)*

The *draft Code of Conduct for Research* is an important initiative towards assisting the scientific community in complying with the provisions of the *Protection of Personal Information Act 4 of 2013* (POPIA). However, its approach towards cross-border data sharing should be reconsidered to clarify the ambiguities inherent in the legal requirements for the cross-border sharing of health data in the POPIA. These ambiguities include the concept of 'transfer of information', the application of *adequacy* as a legal mechanism for transfer, the nature of consent for cross-border sharing and the scope of the recipient third party. We suggest that the *draft Code of Conduct for Research* can be improved by:

- Explaining or defining the concept of 'transfer of information' and when it applies to cross-border sharing in research
- Clarifying the application of *adequacy* as a legal mechanism for transfer vis-à-vis the other alternatives
- Expanding on the interpretation and application of consent as a legal mechanism for cross-border transfers
- Expanding the category of persons who may be recipients of personal information in a third country

S Afr J Bioethics Law 2024;17(1):e1696. https://doi.org/10.7196/SAJBL.2024.v17i1.1696

The transnational nature of health research and patient care makes cross-border data sharing inevitable. African researchers are increasingly realising the need to collaborate and are doing so among themselves, sharing resources including data.[1] Intra-Africa collaborations and data exchange have increased, especially with the COVID-19 pandemic. The cross-border sharing of health data (and associated resources) for research purposes raises peculiar legal concerns, making it subject to specific regulations in various legal frameworks. Under the *Protection of Personal Information Act 4 of 2013* (POPIA), there is an outright restriction on data transfer outside of South Africa (SA). Extra limitations are applicable if such data includes health data considered to be special personal information. Indeed, these restrictions are not intended to stifle scientific research or cross-border data sharing but rather, to ensure that personal data protection is not undermined when data is transferred to third countries with little or no protection.[2]

The legal requirement regarding the cross-border sharing of data for research purposes under the POPIA is complex, especially for scientists not grounded in the interpretation of the law. Recently, the Academy of Science of South Africa (ASSAf) published its latest *draft Code of Conduct for Research* (draft CCR) to assist scientists in complying with the POPIA.[3] While the initiative is a welcome development, applying the current draft as it is will likely result in greater uncertainties for scientists. The objective of this article is to analyse the inherent legal complexities in the application of section 72 of the POPIA on cross-border data sharing and the extent to which the draft CCR attempts to provide clarity on the subject to the research community. We argue that the draft CCR's provision on transborder information flow is vague and does not clarify the complex rules in applying the POPIA. Thus, it is necessary to re-think and elaborate on certain key concepts and their application.

The significance of cross-border data sharing for health research

The significance of cross-border data flows is widely acknowledged in SA as well as globally. Uninhibited cross-border data exchange is explicitly mentioned as one of the key objectives of POPIA. Apart from the objective of balancing the right to privacy against other rights, section 2 points out that POPIA seeks to protect interests, 'including the free flow of information within the Republic and international borders' (section 2(*a*)(*ii*)). In the context of health research, the importance of cross-border sharing of data cannot be over-emphasised especially with the recent surge in transborder diseases. Health data should be able to move freely for research purposes, as argued by Hallinan *et al.*[7] for three major reasons that are largely in the public interest.[4-7] The first reason is that most health research depends entirely on the international exchange of personal data,[4,7] including research aimed at addressing questions that require comparing large datasets from multiple populations

in different regions.[7] The second reason is that most health research necessitates the accessibility of health data to facilitate the synthesis and advancement of the research.[7] Third, there is an ethical argument supporting cross-border data sharing in health research, which aids research resourcing and collaboration by reducing the time and resources required to collect personal data *de novo*. This, in turn, maximises the contributions of individuals and institutions in advancing scientific knowledge.[7] In essence, cross-border data sharing for the purposes of health research is widely regarded as being in the public interest.

Analysing the legal requirements for cross-border sharing of health data in the POPIA

Despite the widely recognised significance of unhindered health data flow for research purposes, there exist inherent risks in this endeavour. Hence, there is a clear requirement to safeguard the privacy and confidentiality of patients and research participants. Consequently, the POPIA restricts cross-border data sharing, also known as 'transfers of personal information outside the Republic' (Section 72). A responsible party (in SA) is prohibited from transferring personal information to a third party (recipient) outside of SA except under certain circumstances.[6] The first circumstance is that the recipient in a foreign country must be subject to a law, binding corporate rules (BCR) or a contract that provides adequate protection (section 72(1)(*a*) of POPIA). While POPIA does not categorically define the concept of *adequacy,* it provides some guidance on what it entails. Accordingly, adequacy suggests that the law, BCR or contract to which the recipient is subject must maintain/contain principles for reasonable processing of information *substantially similar* to those contained in Chapter 3 of POPIA (on provisions for lawful processing of data). In addition, such legal instruments (law, BCR or contract) must also contain provisions restricting further cross-border data sharing between the recipient and a third party, which is *substantially similar* to that in the POPIA (section 72(1)(*a*)).[6]

The second circumstance in which personal data may be transferred outside of SA is where the data subject consents (section 72(1)(*b*) of POPIA). The consent, in this case, must be 'specific, voluntary and informed' (section 1 of POPIA). Although this exception does not include the right to withdrawal of consent in section 11(3)(*b*), it is arguable that voluntariness in the consent also entails a right to withdrawal. Necessity is the third circumstance and, in this case, it could be a necessity for the performance of a contract or implementing pre-contractual measures between the data subject and the responsible party or a necessity for the conclusion or performance of a contract concluded in the interest of the data subject (section 72(1)(*c*) and (*d*) of POPIA). Finally, personal information may be transferred outside of SA if the transfer is for the benefit of the data subject, and his/her consent cannot reasonably be obtained or, if it can, it is unlikely to be denied (section 72(1)(*e*) of POPIA).

POPIA does not stop there. Further provisions are applicable where the cross-border transfer involves health data, most often considered as 'special personal information' (section 26 of POPIA). In this case, if the recipient is subject to a law, BCR, or contract which is not *adequate*, then the responsible party (data transferor) must obtain prior authorisation from the Information Regulator (section 57(1)(*d*) of POPIA).

The important role of a code of conduct in simplifying cross-border data sharing

SA is about to join a small group of countries with a data protection code of conduct for health research. While the European Union (EU) is working on a proposal for a Code of Conduct for Health Research,[8] the Committee on Regulation of Health Research in the Netherlands has recently adopted a code of conduct which applies to both health data and human biological material. A code of conduct could be a potentially influential legal mechanism in facilitating the cross-border sharing of data for health research purposes. If properly drafted, the code of conduct will assist in clarifying the provisions of POPIA and providing clear guidance on the contextual application of the principles of cross-border data sharing. According to members of the drafting committee:

> '*[T]he Code for Research will need to include provisions to guide researchers in transferring or sharing personal information outside of South Africa and will need to take into account the developing international best practice in this regard, in order to ensure that South African researchers remain internationally competitive*'.[9]

Apart from clarifying and providing guidance to scientists, the important role of a CCR is further recognised in the POPIA, especially in the cross-border sharing of health data. According to the POPIA, although authorisation of the Information Regulator is required for the cross-border transfer of 'special personal information' including health data, this requirement is, not necessary where a code of conduct has been made, and is in force, in terms of Chapter 7 of POPIA (section 58). Therefore, a code of conduct is especially important in cross-border data sharing, as it can alleviate the burden on researchers by minimising the need to seek authorisation from the Information Regulator.[6]

The foregoing points to the necessity of an intricately crafted CCR to genuinely serve as a valuable legal instrument for ensuring scientists' compliance with the POPIA. However, this may not hold true when analysing its provisions pertaining to cross-border data sharing. In this context, we have identified four primary concerns in the implementation of Section 72 of POPIA, which a Code of this nature ought to clarify. Subsequently, we will analyse the extent to which it has addressed these concerns.

The meaning of 'transfer of personal information'

The POPIA lacks a specific definition for the term 'transfer of personal information', and the draft of the CCR fails to provide clarity on this matter. Indeed, the meaning of the concept *transfer of personal information* within the context of POPIA (and other data protection instruments) is far more complicated than it appears.[10] This is especially so with the internet and cloud computing, which has complicated how information moves. Indeed, the flow of information is no longer a situation of *physical* transfer or actual change of location with the aid of a memory disk or other physical storage device. De Stadler *et al*.[10] capture this complexity aptly when they observe that:

> '*[W]e are certainly glad about faster internet connections, but the effortless sharing of personal information across borders has introduced a devilish level of complexity when it comes to complying with data protection regulation. With the advent of cloud computing, even simple questions like 'where is the personal information stored?' have become tough to answer*'.

The above shows that data transfer can be effected in this internet age without being actively transferred in the actual sense of the word. This makes the definition of 'transfer' critical. At a preliminary level, it is essential to point out that *transfer* is a type of processing based on section 1 of POPIA. This was also confirmed in the judgment of *Maximillian Schrems v. Data Protection Commissioner*,[11] where the Court of Justice of the European Union (CJEU) contended that 'the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data'.[11] This means that in cross-border transfers, the responsible party must also comply with conditions for lawful processing before complying with the extra requirements for cross-border transfer. Unlike POPIA, which uses the concept of 'transborder information flow' (section 72), the EU *General Data Protection Regulation 2016* (GDPR)[12] uses the concept of 'international data transfers' (recital 101, GDPR). Based on jurisprudence from the EU, merely placing or publishing personal data on a website does not constitute a cross-border transfer. The CJEU in *Bodil Lindqvist*[13] distinguished between making data *accessible* and *transferring* data, where it contended that only the latter case is covered by rules on transborder data flow in the EU.[12] According to Kuner,[14] the court's decision in this case 'was based on the fact that the information was not being sent automatically from the server to other internet users…'.[14] This decision has been subject to much criticism, signifying the continuous lack of clarity in the use of the concept of *transfer*. In health research, understanding when a transfer occurs seems even more complex. For example: Professor A of the University of KwaZulu-Natal and Professor B of the University of Ilorin are joint Principal Investigators in a health research project on cancer in tropical Africa. They both have access to a biobank located in SA for their research. The biobank contains biological materials and associated data from South Africans and Nigerians collected over the past 10 years. When do we say that a transfer has occurred in this scenario?

The above means that we must rethink how data protection instruments approach the concept. There is a need for guidance on when a transfer has occurred in the context of (health) research. A CCR's purpose should take care of this complexity. The draft CCR deals with this issue rather casually, stating that 'Research activities often require that Personal Information must be transferred to other countries',[3] without additional information.

Our suggestion in this regard is that the concept of *transfer* should be explained with an annotation of a few examples of where a transborder transfer has taken place in the context of scientific research involving collaborating partners. Some lessons can be taken from Kenya in this regard, where the *Data Protection (General) Regulations, 2021* (pursuant to the *Data Protection Act, 2019*) defined the concept of 'data sharing', which is *arguably* synonymous with the concept of transborder transfer or sharing.[15] According to the Data Protection Regulations, data sharing may include the following:

- Provision of personal data to a third party by whatever means by the data controller/processor.
- Receipt of personal data for a data controller or data processor as joint participants in a data sharing agreement.
- Exchange or transmission of personal data.
- Provision of a third party with access to personal data on the data controller's information systems.
- Separate or joint initiatives by data controllers/processors to pool personal data making the data available to each other or a third party subject to entering into an agreement as may be applicable.
- Routine data sharing between data controllers on a regular or pre-planned basis.[14]

Complications in the adequacy requirement

The intricacies of the adequacy requirement within POPIA may prove challenging for scientists to fully grasp, and the draft CCR does not provide any elucidation on this matter. The lawful transfer of health information to a recipient in another country requires a legal mechanism (section 72 of POPIA), in addition to a legal basis (section 11 of POPIA) and a derogation for special personal information (section 27 of POPIA). The POPIA recognises four legal mechanisms for cross-border transfer: adequacy, consent, necessity and data subjects' interest (section 72). Unlike the POPIA, the GDPR recognises three legal mechanisms: adequacy, appropriate safeguards and derogations for specific situations. Adequacy is the most favoured legal mechanism for cross-border data sharing, especially in the context of health research.[16] It was rightly noted, particularly regarding the EU, that 'full adequacy decisions for jurisdictions are the results of a long process of intense negotiations'.[10] That is why the GDPR makes 'appropriate safeguards' in standard contractual clauses, BCRs and data transfer agreements as independent legal mechanisms. This means that there is a 'country-level' (adequacy) and then an 'individual-level' (appropriate safeguards) mechanism in the GDPR. Satisfying the requirement of adequacy as a country-level mechanism is largely beyond the control of a researcher, research institution or data controller. It is only the appropriate safeguards that are largely within the control of the data controller. Therefore, in the absence of adequacy, a researcher can conveniently rely on appropriate safeguards, which seem 'less stringent than the rubric of case law that applies to adequacy decisions'.[10] Unlike the GDPR, the POPIA lumps together the country-level and the individual-level mechanisms for cross-border data sharing, which has consequences for compliance.

In the GDPR, an independent mechanism is set up to determine adequacy at the country level, and an adequacy stamp means that data can flow freely between the EU and a third country. While attempting to adopt this approach, the POPIA creates further problems for cross-border data sharing. First, there is no independent mechanism to determine adequacy. Second, it imposes stringent requirements on the individual-level mechanisms, making them not only highly subjective but challenging to comply with. On the first issue, while POPIA requires an *adequate* 'law, BCR or binding agreement' (section 72(1)(*a*)), it does not prescribe an assessment methodology. De Stadler *et al.*[10] argue that:

> *'Article 45 of the EU GDPR caters for transfers based on an 'adequacy decision' made by the European Commission. POPIA does not give the Information Regulator similar powers. This means that it is each responsible party who must make this decision'.*

While it is not clear if this is the intention of the POPIA, leaving this decision to the responsible parties would be challenging. Although the draft CCR requires each responsible party to have an Information Officer with knowledge of the law,[3] determining adequacy is

substantially subjective. De Stadler *et al*.[10] capture this problem very succinctly when they argue that:

> *'Many countries have data protection laws, and they are quite diverse. The first challenge is to know whether a country has a law, and the second is comparing it to the POPIA. Comparing legislation is a labour intensive (and tedious!) task fraught with problems; it presupposes that the person doing the comparing is both proficient in POPIA and the law (and legal system) that he or she is comparing it to. We do not anticipate seeing many legal professionals with the confidence to assert that a foreign data protection law is 'substantially similar' to POPIA without confirmation from the Information Regulator'*.

Furthermore, the POPIA seems to have imported the stringent requirement of adequacy to the other less cumbersome mechanisms, such as data transfer agreements.

The draft CCR does nothing to offer clarity to this conundrum. Instead, it ends up further muddling up the issue. It provides that transferring personal information to other countries must satisfy some requirements, one of which is that 'The country must have laws that are equivalent to POPIA. The Code considers countries in the European Union or a country that has received an adequacy decision from the European Commission as equivalent'.[3] Therefore, since determining adequacy has been made the responsibility of the responsible party in POPIA, why should the draft CCR now import/rely on an assessment by an international institution? This has two implications. First, based on the draft CCR, a responsible party cannot determine adequacy. Second, intra-African cross-border data sharing will be restricted since no African country is yet considered to provide an adequate level of protection by the European Commission. The latter issue will be more elaborately addressed in a subsequent article. In all, the uncertainties in the POPIA are not made any better by the draft CCR.

We suggest that the draft CCR should clarify the relationship between the adequacy requirement and the other legal mechanisms for cross-border data transfer.

The restrictive path to consent

Consent is not only one of the conditions for processing personal information (and special personal information), but it is also a legal mechanism for transferring personal information outside of SA. According to the POPIA, the transfer of personal information is allowed to a third party in a foreign country where the data subject consents to the transfer (section 72(1)(*b*)). Consent under the POPIA is specific, informed and unequivocal consent to transferring personal information outside of SA. The draft CCR goes further to expand on the consent requirement in transborder information flows by clarifying that consent includes the right to withdraw consent; hence in addition to giving his/her consent, 'there must be a process in place to facilitate the withdrawal of POPIA consent'[3] (paragraph 4.3.10.1.5). While this provision is quite striking, we believe that it remains slightly restrictive. The reason is that informed consent, as a pathway to cross-border data sharing, should not only be based on the knowledge of the data subject of the transfer but also the knowledge of risks involved in the transfer to a third country in the absence of *adequacy*. Indeed, there is a reason why consent is not usually the first legal basis for cross-border data sharing in most data protection instruments (unlike the conditions for processing data generally or even special personal information). This is because of the need to provide greater protection for the personal information of data subjects in a third country with the requirement of adequacy. Therefore, consent can be a legal basis in the absence of adequacy. In this case, the data subject (or research participant) must be informed that their data is to be transferred to another jurisdiction or a third party without a guarantee of adequacy and the possible risks involved. This is the approach of the GDPR (Article 49(1)(*a*)), and we believe that this should be the approach to interpreting POPIA, which the draft CCR ought to clarify.

The recipient: third party in a foreign country

Section 72 of the POPIA only applies where 'personal information about a data subject [is transferred] to a third party who is in a foreign country'. The POPIA neither defines such a third partner nor a foreign state. Drawing inspiration from the UK Information Commissioner's Office guidance on cross-border data sharing, De Stadler *et al*.[10] contend that such a third party must not be under the direct authority of the responsible party. Thus, the receiver must be 'legally distinct' from the responsible party making the transfer. This interpretation is wide enough to accommodate every person to a responsible party who possibly wants to transfer information to another country.

The draft CCR seems to have surreptitiously restricted the application of the concept of a 'third party in a foreign country'. In listing the requirement for the transfer of data outside of SA, the draft CCR recognises only a restricted category of recipients of personal data. The restricted category includes a co-responsible party (paragraph 4.3.10.1.2), an operator (paragraph 4.3.10.1.3) or a recipient who belongs to a 'group of undertakings' (paragraph 4.3.10.1.4).[3] This approach implies that personal information cannot be transferred to a third party in a foreign country without equivalent law (paragraph 4.2.10.1.1), consent (paragraph 4.2.10.1.5) or the transfer being to the research participant's benefit (paragraph 4.3.10.1.6).[3] This appears to restrict the application of section 72 of POPIA, which permits transfer to 'the third party who is subject to a binding corporate rule or binding agreement'. We suggest that the draft CCR reconsider this provision.

Conclusion

The draft CCR is a noteworthy initiative towards assisting the scientists in complying with the provisions of the POPIA. While the draft CCR is potentially a critical instrument for the research community, there is still room for improvement. Specifically, the provisions on cross-border data sharing, which is noted to be a very crucial element of collaborative [health] research, need to be given more interpretative depth. This is especially so given the vagueness of the POPIA in this regard and the fact that the Information Regulator has yet to publish any guidance document on cross-border data sharing. SA will ultimately seek an adequacy assessment from the EU, and the draft CCR will be vital in making this decision. In this regard, more needs to be done in the draft CCR to clarify most of the legal uncertainties associated with the vague provisions of POPIA regarding cross-border data sharing. Many of the issues identified above result from the somewhat casual manner in which the draft CCR deals with the issue of cross-border data sharing. This should not be so. While it is always encouraged to couch data protection instruments in a *technological-neutral* manner and to make the law clear to researchers, the substance should not be sacrificed on the altar of brevity.

Indeed, as much as health research needs informed and trustful research participants, samples, data, secure infrastructures and datasets, it also needs clear and detailed rules that researchers can easily understand and implement.[18] In the case of cross-border sharing of health data for research this is imperative because clear, comprehensive provisions in an approved code of conduct can be implemented in a data transfer agreement and obviate the fraught exercise of determining the adequacy of data protection laws in the data recipient's country, or the administrative burden, time and costs of applying for prior authorisation for the transfer from the Information Regulator.

Recommendations

In short, the CCR is a window of opportunity to operationalise the aims of ensuring data access for scientific discovery and innovation. The CCR should not be submitted to the Information Regulator for approval until it provides clear provisions. Our specific recommendations are:

- There is the need to introduce a (sub) section on the meaning of 'transfer of personal information' in cross-border data sharing. The Kenyan Data Protection Regulation has provided some guidelines that the ASSAf drafting committee can learn from.
- The drafting committee should further clarify the concept of *adequacy* as a legal mechanism for transfer vis-à-vis the other alternatives.
- The need to expand the provision for consent as a legal mechanism for cross-border transfer. In this regard, the consent for cross-border data sharing should include consent having been informed of the risks involved in transferring personal information to a third country that is not found to be adequate. The consent provision may be made an alternative to adequacy.
- Expanding the category of persons who may be recipients of personal information in a third country in line with the clear provisions of section 72 of POPIA.
- Providing much more detail regarding the application of the legal requirements of cross-border data sharing.

Declaration. None

Acknowledgements. The authors acknowledge the members of the DS-I Africa Law group for their comments on the previous drafts of the article. We specifically acknowledge the comments from Prof. Donrich Thaldar and Dr. Dusty-Lee Donnelly. All errors, however, remain our own.

Author contributions. LA conceptualised the paper, wrote the first draft and revised subsequent drafts. AA and HO also contributed to revising the draft. All the authors provided edits on the various drafts. All authors read and approved the final manuscript.

Funding. We acknowledge the support of the US National Institute of Mental Health and the US National Institutes of Health (award number U01MH127690). The content of this article is solely our responsibility and does not necessarily represent the official views of the US National Institute of Mental Health or the US National Institutes of Health.

Conflicts of interest. None

1. Townsend B. The lawful sharing of health research data in South Africa and beyond. Inf Commun Technol Law 2022;31(1):17-34. https://doi.org/10.1080/13600834.2021.1918905
2. Jervis CEM. International transfers: Johnson v Secretary of State for the Home Department [2020] and diplomatic missions. Int Data Priv Law 2022;12(1):53-62. https://doi.org/10.1093/idpl/ipab026
3. Academy of Science of South Africa (ASSAf). Draft Code of Conduct for Research. ASSAf;2022. https://www.assaf.org.za/wp-content/uploads/2022/09/20220923_ASSAF_Draft-Code_V8.7.pdf (accessed 1 July 2023).
4. Staunton C, Adams R, Botes M, et al. Enabling the use of health data for research: Developing a POPIA code of conduct for research in South Africa. S Afr J Bioethcs Law 2021;14(1):33-36. https://doi.org/10.7196/SAJBL.2021.v14i1.740
5. Thalder D. Research and the meaning of 'public interest' in POPIA. S Afr J Sci 2022;118(3/4):1-3. http://dx.doi.org/10.17159/sajs.2022/13206
6. Thalder D, Townsend B. Exempting health research from the consent provisions of POPIA. Potchefstroom Electr Law J 2021;24:1-32. https://doi.org/10.17159/1727-3781/2021/v24i0a10420
7. Hallinan D, Bernier A, Cambon-Thomsen A, et al. International transfers of personal data for health research following Schrems II: A problem in need of a solution. Eur J Hum Genet 2021;29:1502-1509. https://doi.org/10.1038/s41431-021-00893-y
8. BBMRI-ERIC. The Code of Conduct for Health Research. https://www.bbmri-eric.eu/services/the-code-of-conduct-for-health-research/ (accessed 27 October 2022)
9. Adams R, Adeleke F, Anderson D, et al. POPIA Code of Conduct for Research. S Afr J Sci 2021;117(/6):1-12. https://doi.org/10.17159/sajs.2021/10933
10. De Stadler E, Hattingh IL, Esselaar P, Boast J. Over-thinking the Protection of Personal Information Act. Juta (Pty) Limited; 2021. ISBN: 9781485136828.
11. Maximillian Schrems v. Data Protection Commissioner (C-362/14). EU:C:2015:650. https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=5700244
12. General Data Protection Regulation (EU) 2016/679, European Union.
13. Bodil Lindqvist (C-101/01). ECLI:EU:C:2003:596. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN
14. Kuner C. Transborder data flows and data privacy law. Oxford: Oxford University Press; 2013. https://doi.org/10.1093/acprof:oso/9780199674619.001.0001 (accessed 1 July 2023).
15. The Data Protection (General) Regulations, 2021. Kenya. http://161.35.8.237:8080/wp-content/uploads/2021/06/Data-Protection-General-regulations.pdf
16. Slokenberga S. Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: Adequacy considerations and Convention 108. Int Data Priv Law 2020;10(2):132-145. https://doi.org/10.1093/idpl/ipaa006
17. BBMRI-ERIC. A Code of Conduct for Health Research. https://code-of-conduct-for-health-research.eu/

Accepted 4 March 2024.