EU data transfer rules and African legal realities: is data exchange for biobank research realistic?

Santa Slokenberga*, Jane Reichel**, Rachel Niringiye***, Talishiea Croxton****, Carmen Swanepoel***** and June Okal******

Key Points

- To effectively collaborate in biobanking and build capacity in low and middle-income countries, data transfer from European Union (EU) Member States to states in Africa is crucial.
- Although under the General Data Protection Regulation (GDPR) avenues for data transfer exist, the ones feasible for transcontinental data exchange for biobank research rely on EU enforcement which in essence means limited oversight possibilities and, consequently, considerable risks to the EU data subject's privacy.
- To ensure effective data protection for data subjects in biobanking, raising the data protection bar in data recipient countries is crucial. Although Kenya, Nigeria, South Africa, and Uganda have taken considerable steps towards developing data protection frameworks, only that of South Africa and Nigeria's Protection of Personal Information Bill seem to be such to meet the protection level set out by the GDPR. The legislative initiatives in Kenya and Uganda require revisions to ensure that protection of privacy is not undermined when data are being sent to these countries.
- Currently, considerable responsibility is placed in the hands of the legislatures in the countries of concern—and notably in Kenya, and Uganda—to set foundations for ending research and research integrity-harming practices. In Nigeria, these foundations are defined in the Protection of Personal Information Bill, but not adopted yet. South Africa, however, has taken a big step towards building routes for genuine biobank capacity-building in the country and collaboration in that regard.

Introduction

Biobanks and biobank research are essential for understanding the human genome, disease aetiology and translation, as well as for furthering medicine.[1] However, several preconditions are essential to carry out this type of research. Among these are the existence of the necessary research infrastructures and the availability of both a sufficient amount and appropriate quality of samples and data. Over the past decades, investments in biobank research infrastructures in scientifically advanced countries have been commonplace.[2] In Europe alone, the number of biobanks is

* Santa Slokenberga, Lund University, Faculty of Law, Lund, Sweden; Uppsala University, Center for Research Ethics & Bioethics, Uppsala, Sweden. Email: Santa.Slokenberga@jur.lu.se

** Jane Reichel, Stockholm University, Faculty of Law, Stockholm, Sweden; Uppsala University, Center for Research Ethics & Bioethics, Uppsala, Sweden

*** Rachel Niringiye, Aegis Advocates, Uganda

**** Talishiea Croxton, University of Maryland, Baltimore, Maryland, USA

*****Carmen Swanepoel, Division of Heamatology, Department Pathology, National Health Laboratory Services (NHLS), Faculty of Medicine and Health Sciences, Stellenbosch University, South Africa

******June Okal, Univesity of Nairobi, Nairobi, Kenya. The authors would like to thank the two anonymous reviewers and the editors of the journal for their valuable comments, as well as ILRI team for discussions on Kenyan data protection framework and Samuel Iheanyi Nwankwo for his insights in Nigerian data protection law. This article is part of the B3Africa Project http://www.b3africa.org/, which has received funding under grant agreement nr 654404 from the European Union Horizon 2020 research and innovation programme. Comparative analysis for Kenya, Nigeria, South Africa and Uganda is carried out taking into consideration legal developments as of May 10, 2018. In June Kenyan Data Protection Bill, 2018 has been released which is not accounted for in this article.

1 JE Olson and others, 'Biobanks and Personalized Medicine' (2014) 86 Clin Genet 50.

2 Don Chalmers and others, 'Has the Biobank Bubble Burst? Withstanding the Challenges for Sustainable Biobanking in the Digital Era' (2016) 17 BMC Med Ethic 39.

considerable and growing. For example, a study in 2010 identified and surveyed 126 biobanks in 23 European countries,[3] whereas by 2016 Holub and others reported that BBMRI-ERIC Directory embraced 515 biobanks with over 60 million biological samples.[4] Likewise, a number of initiatives have been taken to further biobanking in low and middle-income countries and advance collaboration within Africa and beyond. At different periods in time, the region has benefited from various capacity- and collaboration-enhancing activities. Among the former initiatives is the HapMap project that focused on the common patterns of DNA sequence variation in the human genome and freely available information in that regard.[5] Among key current initiatives are such projects as Bridging Biobanking and Biomedical Research across Europe and Africa (B3Africa) which aim to improve and facilitate the development of a better, predictive, preventive and personalized healthcare and to empower researchers in Africa to employ their scientific potential locally.[6] Human Heredity and Health in Africa (H3Africa) project also works towards improving the health level of African populations through furthering the study of genomics and environmental determinants of common diseases.[7] Another project is the Genomic Epidemiology Network Malaria (GEN) which brings together a number of other projects to analyse genome variation and better understand the interaction between humans, malaria parasites, and mosquito vectors.[8]

The necessity for samples and data, as well as the untapped potential that genetic diversity can offer, has contributed to biobank research becoming collaborative and, as such, global. In the past, it was common practice to export cellular samples from developing countries to those countries with strong research infrastructures often without regard to developing capacity in the country from which the samples originated.[9] This parachute research led to situations where research integrity was affected. Not only did researchers in those states have limited possibilities to benefit from the studies because of, eg failure to recognize their contributions, but it was also uncertain to what extent, if at all, the intended collaboration contributed to directly advancing healthcare in the area.[10] As evidenced by more recent outbreaks that have attracted global attention (eg the Zika and Ebola outbreaks), parachute research has not yet been eradicated.[11] A number of voices have been raised to stop these practices as they are public health and research integrity insensitive, and scholars have called for further collaboration instead.[12] Nowadays, there is a growing consensus about the need for collaborative research that entails not only the possibility to receive samples and data from other countries but also to export samples and data to those countries, as well as *inter alia* identify the clear benefits of the intended studies for the populations concerned.[13]

Legal solutions should be in place for effective collaboration that entails data and sample exchange. Currently, however, the regulatory responses are local,[14]

3 Eleni Zika and others, 'Biobanks in Europe: Prospects for Harmonisation and Networking' (European Commission, JRC-IPTS 2010) EUR 24361 EN-2010.

4 Petr Holub and others, 'BBMRI-ERIC Directory: 515 Biobanks with over 60 Million Biological Samples' (2016) 14 Biopreserv Biobank 559.

5 Furthermore, a multi-phase International HapMap project that seeks 'to determine the common patterns of DNA sequence variation in the human genome and to make this information freely available in the public domain'. 'International HapMap Project' (National Human Genome Research Institute (NHGRI)) <https://www.genome.gov/10001688/international-hapmap-project/> accessed 8 May 2018.

6 'B3Africa—Bridging Biobanking and Biomedical Research Across Europe and Africa' <http://www.b3africa.org/> accessed 19 September 2017. On B3Africa's contribution to research integrity, see Santa Slokenberga, Roxana Merino Martinez and Jane Reichel, 'Legal and Ethical Governance of Intercontinental Biobanking—Some Experience from a H2020 Project' [2017] Förvaltningsrättslig tidskrift.

7 'H3Africa' <http://h3africa.org/> accessed 19 September 2017. On H3Africa contribution to "ELSI" as for ethical, legal and social issues see De Vries Jantina and others, 'Regulation of Genomic and Biobanking Research in Africa: A Content Analysis of Ethics Guidelines, Policies and Procedures from 22 African Countries' (2017) 18 BMC Med Ethic 8, as well as the soft law, see Aminu Yakubu and others, 'Model Framework for Governance of Genomic Research and Biobanking in Africa—a Content Description' (2018) 1 AAS Open Res 13.

8 'Malaria Genomic Epidemiology Network' <https://www.malariagen.net/projects> accessed 9 May 2018.

9 Ciara Staunton and Keymanthri Moodley, 'Community Engagement for Biobanking Research: Perspectives from Africa' (2016) 20 Asia Pac Bio News 14. See also Ciara Staunton and Keymanthri Moodley, 'Challenges in Biobank Governance in Sub-Saharan Africa' (2013) 14 BMC Med Ethic 35.

10 For insignts in the perspectives of researchers working with biospecimens and/or biobanks in South Africa, see Keymanthri Moodley and Shenuka Singh, '"It's All about Trust": Reflections of Researchers on the Complexity and Controversy Surrounding Biobanking in South Africa' (2016) 17 BMC Med Ethic 57. Such issues as the ones above listed are tackled in a policy framework, focusing on biobank research in Africa. Jantina de Vries and others, 'The H3Africa Policy Framework: Negotiating Fairness in Genomics' (2015) 31 Trends Genet: TIG 117.

11 Nathan L Yozwiak and others, 'Roots, Not Parachutes: Research Collaborations Combat Outbreaks' (2016) 166 Cell 5.

12 David L Heymann, Joanne Liu and Louis Lillywhite, 'Partnerships, Not Parachutists, for Zika Research' (2016) 374 New England J Med 1504; Yozwiak and others, ibid.

13 H3Africa Framework, 'Ethics and Governance Framework for Best Practice in Genomics and Biobanking Research in Africa' <https://www.sun.ac.za/english/faculty/healthsciences/rdsd/Documents/Final%20Framework%20for%20African%20genomics%20and%20biobanking_SC_February%202017%20II%20.pdf> accessed 9 May 2018.

14 Haidan Chen and others, 'A Call for Global Governance of Biobanks' (2015) 93 Bullet World Health Organiz 113. On how this affects collaboration within Sub-Saharan Africa, see Staunton and Moodley, 'Challenges in Biobank' (n 9).

which in itself is a hurdle that needs to be tackled in order to further the research.[15] There are a number of organizations, initiatives, and resources that support the development of harmonized platforms for biobanks and biobank-based science.[16] In addition to these initiatives, soft tools, such as WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks, and general requirements for biobanking, such as ISO standards, have been adopted.[17] At the European level, the Council of Europe has adopted the Recommendation CM/Rec(2016)6 of the Committee of Ministers to Member States regarding research on biological materials of human origin with a view to safeguard fundamental rights of the persons whose biological materials are intended for biomedical research. Under the leadership of H3Africa Ethics and Regulatory Issues Working Group, the 'Ethics and Governance Framework for Best Practice in Genomics and Biobanking Research in Africa' has been developed with a view to address the needs, interests, and rights of the peoples of Africa. Yet, international and legally binding biobank regulatory frameworks that set out uniform requirements and levels of protection do not exist. Instead, for the purposes of collaborative research, researchers must follow the conflicts of law approach and navigate through complex sets of rules to see to what extent, if at all, the intended collaborative research is feasible and possible.[18]

Although the EU lacks legislative competence to regulate biobank research in a comprehensive manner, EU competence is triggered to the extent that data protection matters are concerned. The EU considers its data protection as the 'gold standard'[19] which, in regard to personal data, is delineated in the GDPR, in force from May 2018.[20] This standard is to be applied in situations when data are being processed in the EU regardless of whether or not the data originated from an EU data subject, as well as when EU data subjects' data are being transferred to third countries or international organizations. At a time when data protection requirements are only beginning to be shaped in certain regions, eg Africa,[21] meeting the strict and high EU data protection requirements might appear to be rather challenging. This can affect collaboration possibilities and capacity-building activities, including those supported by the EU through its generous research strategies.

Therefore, given the discrepancies in data protection frameworks in the EU and Africa, this article aims to examine whether transcontinental data exchange for biobank research between the EU Member States and selected African states (Kenya, Nigeria, South Africa, and Uganda), all of which are members of the B3Africa consortium, is at all realistic, and if so, what challenges may arise. In doing so, the article identifies the data protection standard mandated by the GDPR for biobanking (section 'Biobanking under the GDPR') and examines rules for data transfer to third countries (section 'EU data transfer requirements'). Thereafter, it examines the existing and evolving data protection frameworks in regard to biobanking in selected African jurisdictions (section 'Biobanking and data protection') and analyses whether and under what circumstances data transfer in biobanking could take place between the EU and Kenya, South Africa, and Uganda (section 'Concluding analysis'). It argues that although data transfer between the EU Member States and the selected African jurisdictions is possible, in part, due to the blind trust the EU legislature has regarding the oversight of the data transfers subject to appropriate safeguards, in order to ensure genuine data protection in biobanking and further capacity building legislative steps are to be taken nationally in the respective African states. This could also be a step forward to eradicate the capacity building and research integrity harming practices, such as parachouting.

Biobanking under the GDPR

The GDPR, as a technology- and activity-neutral legal instrument, does not expressly address biobank research activities. Nonetheless, the applicability of the GDPR in the course of biobanking is difficult to avoid. Not only

15 Santa Slokenberga, 'Biobanking Between the EU and Third Countries—How Can Data Sharing Be Facilitated? Strategies in B3Africa Project' European J Health Law (forthcoming).

16 Jennifer R Harris and others, 'Toward a Roadmap in Global Biobanking for Health' (2012) 20 European J Human Genet 1105. As classified by Harris and others, they include Regional and international organizations, Science and infrastructure initiatives, as well as resource tools and databases. Ibid, table 1.

17 'ISO/DIS 20387—Biotechnology—Biobanking—General Requirements for Biobanking' 20387 <https://www.iso.org/standard/67888.html> accessed 27 December 2017.

18 Slokenberga, Martinez, Reichel (n 6).

19 European Commission, 'European Commission—Press Release—Commission to Renegotiate Council of Europe Data Protection Convention on Behalf of EU' <http://europa.eu/rapid/press-release_MEMO-12-877_en.htm> accessed 10 March 2016.

20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1. The GDPR replaces the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31 (Data Protection Directive).

21 For an overview of data protection laws in Africa, see Alex B Makulilo, *African Data Privacy Laws* (Springer 2016).

are personal data, as defined in Article 4 of the GDPR, crucial to ensure quality and reliability in scientific research[22] but also under the GDPR genetics serves as one of the identifiers of a person.[23] Although a fraction of a DNA strand is probably insufficient to identify a person, a long enough strand under certain circumstances could be regarded as personal data and could lead to identification of a research participant.[24]

The GDPR does not fundamentally alter the approach for scientific research that was set out in the Data Protection Directive. However, it brings updates; revises and introduces new terminology (including the definition of genetic data);[25] expands the list of special categories of data including genetic data in that category; revisits and expands data protection principles; introduces new individual rights; and finally strengthens data security and oversight related procedures, all of which are activities that affect biobank research. The GDPR, as did the Data Protection Directive, allows for exceptions related to scientific research to be adopted by the EU Member States. However, some scholars question whether the research exemption under the GDPR is not going too far, thus leaving the data subjects without proper protection.[26]

The GDPR, similar to the Data Protection Directive, is built around principles related to processing of personal data, securing obligations to the biobankers and rights to the data subjects in that regard, and ensuring effective oversight and enforcement. However, compared with the Data Protection Directive, it not only strengthens the content of the principles but also introduces new ones of importance to biobanking.

According to Article 5 GDPR, data in biobanking should be processed lawfully, fairly and in a transparent manner in relation to the data subject. They should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. What is lawful and how purpose limitation is handled could differ between the EU Member States as the GDPR, through deferring to the national legislatures, accommodates various scientific research-related data collection practices.[27] As it will be shown, these principles are a shell only; the nucleus could differ in different EU Member States.

The data in biobanking should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. They should also be accurate and, where necessary, kept up to date. Furthermore, they should not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed, except for situations when the EU Member States has opted to implement Article 89 GDPR which permits derogations from certain rights and obligations, on condition that appropriate safeguards exist. Lastly, the data in biobanking shall be processed in a manner that ensures appropriate security of the personal data, which is the responsibility of biobankers. Also under the GDPR biobankers are responsible for compliance with the GDPR in their roles as controllers or processors. Furthermore, it is their responsibility to demonstrate that the applicable requirements are met.

The GDPR sets out a number of rights for data subjects although their relevance to biobanking could differ in different EU Member States due to derogations which Article 89 GDPR allows for. Moreover, other derogations in specific situations in biobanking could exist, for example, under Article 19 and 20 GDPR. Individual rights include the right to information,[28] right of access,[29] right to rectification,[30] right to erasure,[31] right to restriction of processing,[32] notification entitlement,[33] right to data portability,[34] right to object,[35] right to lodge a complaint with a supervisory authority,[36] right to an effective judicial remedy,[37] right to representation and right to compensation.[38] Pursuant to Article 89 GDPR for biobanking purposes right of access, right to rectification, right to restriction of processing and right to object could be restricted. While on the surface it might seem that a right to information, notification entitlement, right to portability and right to erasure remains with the data subjects, as specified in Articles 13, 14, 17, 19 and 20, in certain situations relevant to biobank research also these rights can be lifted. Thus, leaving the

22 Gauthier Chassang, 'The Impact of the EU General Data Protection Regulation on Scientific Research' (2017) 11 Ecancermedicalscience 709.

23 GDPR (n 20) art 4.1 and recital 34.

24 Erika Check Hayden, 'Privacy Protections: The Genome Hacker' (2013) 497 Nat News 172.

25 In accordance with art 4.13 GDPR 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

26 Kärt Pormeister, 'Genetic Data and the Research Exemption: Is the GDPR Going Too Far?' (2017) 7 Int Data Priv Law 137.

27 GDPR (n 20) arts 9.2.j and 89.

28 Ibid arts 13, 14, and 34.

29 Ibid art 15.

30 Ibid art 16.

31 Ibid art 17.

32 Ibid art 18.

33 Ibid art 19.

34 Ibid art 20.

35 Ibid art 21.

36 Ibid art 77.

37 Ibid arts 78 and 79.

38 Ibid arts 80 and 82.

data subject with means only to protect the rights (right to lodge a complaint, right to an effective judicial remedy, right to representation, right to compensation). This will mean that the exact set of data subject's rights differs in different EU Member States and, moreover they could differ in different situations within the same Member State, which could risk causing serious confusion for the data subjects about the extent of protection of their transferred data for biobank research purposes within the EU.

Pursuant to the principle of accountability, the biobanker as a controller bears considerable responsibility to ensure and demonstrate that the requirements that stem from the GDPR in regard to biobank research are being satisfied. Having considered the risks that data processing in the course of biobank research raises, appropriate technical, and organizational measures should be put in place to ensure and demonstrate that the processing complies with the GDPR.[39] This mandates not only undertaking a risk assessment but also acting on that to ensure that data are safeguarded by design and default as required under Article 25 GDPR, and appropriate measures to ensure security are in place.[40] The measures should thereby ensure that such principles as data minimization and integrity, and confidentiality are upheld. As explained by Chassang, data protection by design is well known in the area of scientific research; research funding-seekers have often been asked to demonstrate the robustness of the data protection systems for the intended research.[41] The requirement of securing data protection by default seems to be a novelty which mandates implementing 'appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed'.[42] In the course of collaborative research or on other occasions when processors are involved, the controller is responsible for using those processors that can uphold the requirements set out in the GDPR.[43] In the event of a high risk to the rights and freedoms of the data subjects, a data protection impact assessment should be carried out as in most cases biobank research could be interpreted as large-scale processing.[44] Generally, despite Article 29 Working Party's attempt to clarify situations when the data protection impact assessment is necessary, a clear line between when the assessment is necessary and when it is not necessary remains difficult to be drawn. However, in biobanking it is necessary by virtue of Article 35.3.b GDPR. A data protection officer should be designated when such large-scale processing arises.[45] In regard to the research that is being conducted, the controller should maintain records of processing activities.[46] Moreover, in the course of effective oversight and enforcement of the data protection requirements and individual rights, the biobanker is required to cooperate with the supervisory authority and notify it in the event of a breach,[47] as well as communicate and collaborate/assist the data subject.[48]

An independent supervisory authority is key to securing effective oversight of the application of the GDPR. To effectively protect their rights and interests, data subjects are entitled to lodge a complaint with a supervisory body[49] and have a right to an effective judicial remedy vis-à-vis the authority and the biobanker acting in the capacity of a controller or a processor,[50] as well as a right to compensation.[51] In that regard, the data subject is entitled to representation.[52] The biobankers could also be subjected to penalties and fines for violations of the GDPR.[53]

Overall, EU law sets out a thick layer of data protection requirements that are applicable to biobanking. As mentioned above, Article 89 GDPR allows Member States to adopt legislation that gives exceptions to several of the requirements, and further derogations are possible directly relying on the GDPR provisions. In reality, this will mean a fragmented research regulatory framework, the consequences of which are yet to be appraised.[54]

EU data transfer requirements

General principles of data transfer to third countries or international organizations

In order for data transfer from the EU to third countries or organizations for research purposes to take place, both requirements that stem from the general principles of data transfer as prescribed by the GDPR and a specific legal ground for the transfer must be upheld. The

39 Ibid art 24.
40 Ibid art 32.
41 Chassang (n 22) 709.
42 Ibid art 25.2.
43 Ibid art 28.1.
44 Ibid art 35.
45 Ibid art 37(1)(c).
46 Ibid art 30.
47 Ibid arts 31 and 33.
48 Ibid arts 34, 12.1, and 19.
49 Ibid art 77.
50 Ibid arts 78 and 79.
51 Ibid art 82.
52 Ibid art 80.
53 Ibid arts 83 and 84.
54 Santa Slokenberga, Olga Tzortzatou and Jane Reichel (eds) *Individual Rights, Public Interest and Biobank Research: Article 89 GDPR and European Legal Responses* (Springer 2019 forthcoming).

GDPR does not define 'transfer to third countries'.[55] Nonetheless, its content can be ascertained by considering the situations to which the intra-EU rules do not directly apply.[56] Whether and to what extent data can be transferred to the third countries and international organizations (external transfer) differ depending on a number of considerations, including the possible legal grounds for data transfer, data protection level in the third country or international organization, and the overall legal situation therein. The general principles of data transfer to third countries will be reviewed below. The legal grounds for data transfer will be considered in the next subsection.

Chapter V of the GDPR sets out conditions for external data transfer. As derived from Article 44, in order for external data transfer to take place applicable provisions of the GDPR should be applied and the detailed data transfer conditions should be met. Furthermore, they are to be applied in a manner that upholds the level of protection set out by the GDPR. Thus, this article cannot be viewed in isolation from other sources of EU law in the area of privacy and data protection, particularly Article 7 of the CFREU[57] which grants everyone the right to respect for private life and Article 8.1 CFREU which grants everyone the right to protection of their personal data. Under the GDPR,[58] as well as previously under the Data Protection Directive, the rights provided under EU law cannot be undermined just because the data are being transferred to a third country or international organization.[59] For data transfer for biobanking purposes this means that the high standard warranted by the EU law should be externalized vis-à-vis collaborative research institutions in the third countries. The avenues for externalizing EU data protection requirements will be reviewed below.

Conditions for data transfer to third countries

As provided in Articles 45–47 GDPR, data transfer can be based on an adequacy decision, by way of appropriate safeguards, eg by way of binding corporate rules or a code of conduct approved by a competent authority, under possible derogations or, finally, following a judgment or administrative decision of a third country if based on an international agreement in force. Likewise, Article 49 GDPR allows for an exemption provided preconditions for derogations are met, eg for those with the informed consent of a data subject that also entails opting out of the rights provided under the EU law,[60] or for important reasons of public interest if research is so defined in national laws.[61]

An *adequacy decision* means that the Commission has found that 'a country, a territory or one or more specified sectors within that country . . . ensures an adequate level of protection'.[62] The existence of such a decision enables data transfer between the EU and that country or organization in relation to which the decision has been adopted. For countries with such a decision in place, data for research can be rather easily transferred, and consequently collaboration can be enabled.

In order for an adequacy decision to be adopted, the Commission must arrive at the conclusion that the respective actor (a third country, a territory or one or more specified sectors within a third country, or an international organization) ensures an adequate level of protection. Whether the level of protection is adequate is assessed through the following key elements: the rule of law, existence of an independent supervisory authority and international commitments in particular in the area of data protection.[63] The construction of Article 45.2 GDPR suggests that the three key elements are illustrative rather than exhaustive, and the Commission has discretion to consider other elements it deems necessary for evaluating the standard of protection in the third country. Although each of the listed criteria is further specified in regards to its content, the GDPR is silent on the extent to which and how these criteria are to be met. The GDPR does not further specify the application of Article 45.2 (assessment for adequacy decision), in particular, how the assessment will be made. It can be derived from the *Schrems*-case which indicates that the EU does not require the EU rules to be replicated.[64] Instead, 'the test lies in whether, through the substance of privacy rights and their effective implementation, enforceability and supervision, the foreign system concerned as a whole delivers the required high level of

55 Bianka Makso, 'Exporting the Policy-International Data Transfer and the Role of Binding Corporate Rules for Ensuring Adequate Safeguards' [2016] Pecs J Int Eur L 79, 81.

56 More on extraterritoriality, see Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law' (2015) 5 Int Data Priv Law 235.

57 Charter of the Fundamental Rights of the EU [2010], OJ C 83/389.

58 GDPR (n 20) recitals 103–105.

59 C-362/14 *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, para 39.

60 GDPR (n 20) art 49.1(a).

61 Generally, under art 49.4 GDPR, the public interest exemption may either be defined nationally or at the EU level.

62 GDPR (n 20) art 45.

63 Ibid art 45.2.

64 *Schrems* (n 58) para 76, see also Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalized World Brussels, 10 January 2017 COM(2017) 7 final, p 6.

protection'.[65] Although the Commission has found that a variety of states meet adequacy or partial adequacy requirements, thus allowing the Commission to arrive at an adequacy or partial adequacy decision, no African state is among them.[66] Therefore, it remains unclear to what extent African states, given the peculiarities of the national legal systems and emerging protection of privacy and data protection in the region, could meet the requirements prescribed in Article 45 GDPR.[67] In the absence of further specifications of assessment and means of speculating whether and to what extent African states could meet the requirements that are necessary for an adequacy decision, it is rather evident that such a solution does not meet short-term needs. The ongoing collaborations and research capacity-building activities require finding immediate ways of collaboration, should they exist. An adequacy decision, because of the assessments that need to be done, can hardly be seen as an immediate solution. Rather, it is the foundation for further and relatively stable collaborations with the respective actors beyond the EU.

In the absence of an adequacy decision, other possibilities to carry out an external data transfer exist in the course of collaborative biobank research under the GDPR and could be utilized. The GDPR envisages that data may be transferred if the controller or processor has provided *appropriate safeguards* and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[68] While the question of data subject rights could be ascertained with a degree of certainty (leaving the question of impact of Article 89 and other permissible derogations under, for example, Articles 13, 14, 17, 19 and 20 GDPR for external data transfers for interpretation), the question of effective legal remedies mandates further consideration.

A right to effective legal remedy is part of the EU fundamental rights catalogue in Article 47 CFREU. It is inherent in the rule of law in the EU legal order[69] and in the context of personal data protection it is also an explicit requirement under the GDPR. Chapter VIII of the GDPR contains a right to both administrative and judicial redress, as well as to compensation.[70] The right to redress in regards to a transfer based on an appropriate safeguard is addressed in recital 108 of the preamble, which puts emphasis on an 'effective administrative or judicial redress and to claim compensation, in the Union or in a third country'. What is meant by 'effective administrative or judicial redress' is not specified.[71] The question may be raised whether access to a *court* is necessary or whether administrative redress, eg an independent review board connected to the receiving organization (a research institution or a biobank), a data privacy ombudsman or similar could be sufficient to ensure the data subject's rights. Within the sphere of application of the GDPR itself, Article 79 holds that the availability of an administrative redress-mechanism does not preclude the right to judicial redress before a court.[72] Consequently, it could be argued that that there is not much leeway in accepting redress-mechanisms other than judicial redress in order to ensure data subject's rights after transfer to third countries.

The concept of appropriate safeguards for the data subject entails the controller or processor taking the necessary measures to compensate for the lack of data protection in the third country in question.[73] The safeguards that are to be taken in that regard can be divided into two categories: those requiring further authorization from a supervisory authority (Article 46.3 GDPR), and those not requiring further involvement of a supervisory authority upon each individual transfer, once the safeguard has been approved by competent authorities (Article 46.2 GDPR). All in all, these safeguards are an expansion and an elaboration of what the Data Protection Directive had set forth and what was permissible under the directive.[74]

A transfer, dependent on further authorization from a supervisory authority in an individual case, could take place in two different ways: first, through contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in

65 Communication from the Commission (n 63) p 6–7.

66 The list of adequacy decisions 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries—European Commission' <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 27 December 2017.

67 Makulilo (n 21).

68 Art 46 General Data Protection Regulation Previously regulated in art 26.2 in the Data Protection Directive, however, the requirement to ensure that the rights of the data subject are enforceable was not explicitly mentioned.

69 *Schrems* (n 58) para 95.

70 Ch VIII of GDPR contains rules on remedies, liability, and penalties. Among those, an individual's right to lodge a complaint with a supervisory authority (art 77), right to an effective judicial remedy against a supervisory authority (art 78 GDPR), as well as right to an effective judicial remedy against a controller or processor (art 79 GDPR), and right to compensation and liability (art 82 GDPR).

71 See further, Mike Varney, 'Effective Redress of Grievance in Data Protection: An Illusion?' (2016) 23 Maastricht J Euro Compar L 550.

72 Art 77.1 reads 'without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation'.

73 GDPR (n 20) recital 108.

74 For a detailed account on changes, see European Commission, Communication from the Commission (n 63) p 4–5.

the third country or international organization; secondly, through provisions to be inserted into administrative arrangements between public authorities or bodies that include enforceable and effective data subject rights. In the context of biobank research this means that parties could agree on data transfer and compensatory measures for the lack of data protection in the third country; this agreement should be approved by a competent data protection authority before the transfer takes place. The content of the agreement should then be assessed on a case-by-case basis, depending on the exact and intended collaboration.

Article 46.2 GDPR sets out six different means for ensuring adequate safeguards in situations when further authorization from a supervisory authority for an individual transfer is not necessary once the safeguard has been approved initially by the competent authority.

First, through legally binding and enforceable instruments between public authorities or bodies. This option or mechanism could be relevant since biobanks can often be run by public bodies, hospitals, and universities.

Secondly, binding corporate rules in accordance with Article 47 GDPR. Although this mechanism is aimed at developing a certain level of protection within a group of undertakings or a group of enterprises engaged in a joint economic activity,[75] one could argue that it also includes partners not necessarily sharing joint commercial objectives.

Thirdly, standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) GDPR.

Fourthly, standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) GDPR. Generally, standard data protection clauses (either adopted by the Commission or adopted by a supervisory authority and approved by the Commission) aim at ensuring data protection when the data are being processed in the third country on behalf of the exporter.[76] Specifically, the clauses adopted by the Commission for the purposes of applying a similar provision in the Data Protection Directive require the specification of the assignment. In the area of biobank research, however, this means that the data exporter remains in charge of the research done in the third country and the envisaged research will be done with close influence from the exporter. Although from the data protection view such a requirement arguably contributes to the aspired and, on the surface, high level of protection for the data subject, it could also be seen as affecting research. If the ultimate goal is to build research capacity in Africa, standard contractual clauses could be seen as patronizing and in fact a means of hampering independent work of the scientists in Africa.[77] A similar criticism could be made of the standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2) GDPR. Furthermore, this approach also rests on an assumption that an effective oversight by the Member States' supervisory authorities could be ensured. This is challenging from the principles of national administrative law, and hence rather than contributes to genuine protection of privacy, it creates an illusion of protection, which the Commission seems to be well-aware of.[78]

Fifthly, an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. In accordance with Article 40 GDPR, a code of conduct could specify the application of the GDPR on a number of data protection questions in a particular area. In the context of biobank research in the EU, such an association is BBMRI-ERIC. In January 2017, its director announced a pressing need to develop such a code in the area of life sciences and launched the Health & Life Science GDPR Code of Conduct.[79] Although the list provided in Article 40.2 GDPR and quoted above is illustrative, data subjects' rights will be addressed in order for the code of conduct to be relevant to data exchange with third countries.[80] Further, such a code has to be approved. The process of approval depends on the intended use of the code of conduct. However, should the Commission deem it appropriate, by way of implementing acts the Commission could decide on the general validity of the code of conduct within the EU.[81]

75 GDPR (n 20) recital 110 and art 4.20.

76 The clauses adopted under the Data Protection Directive: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593).

77 'Model Contracts for the Transfer of Personal Data to Third Countries—European Commission' <http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm> accessed 27 December 2017.

78 Commission Decision of 5 February 2010 (n 82) clause 1(e) and clause 4(b), as well as Exchanging and Protecting Personal Data in a Globalized World (n 80) p 12–13.

79 Jan-Eric Litton, 'We Must Urgently Clarify Data-Sharing Rules' (2017) 541 Nat News 437.

80 GDPR (n 20) art 40.3.

81 Ibid art 40.9.

Sixthly, an approved certification mechanism pursuant to Article 42 GDPR together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. This mechanism entails the establishment of data protection certification mechanisms and of data protection seals and marks either at the EU or Member States level, for the purpose of demonstrating compliance with this regulation, establishment of the certification mechanisms is voluntary.

Lastly, in the absence of either an adequacy decision or appropriate safeguards, derogations envisaged in Article 49 GDPR could also be relied upon.[82] The latter possibility is formed in the way of an exception rather than a general rule and is applicable only in highly limited situations. It is therefore unsatisfactory for collaborative research purposes and capacity-building activities. On the other hand, recital 113 of the preamble specifically refers to the legitimate expectations of society for the expansion of knowledge to be taken into consideration when assessing the possibility of making an exception on the transfer of personal data for research purposes. The usability of this rule could differ depending on the research situation in question.

The above indicates there are several ways external data transfer for the purposes of research could take place. Among those of particular usability for research are contractual clauses in an individual transfer situation, as well as mechanisms such as binding corporate rules, standard contractual clauses, a code of conduct, and a certification mechanism. While each of these mechanisms offers different routes and poses different obligations, they have a common feature. All of them are based on the idea of compensating for the lack of data protection in the third country. While the easiest way could be to agree on EU law as the applicable law, and hence externalize the GDPR by virtue of private international law, there are obvious challenges with this approach. It is unclear how effective the oversight would be for data handling in the third country concerned. Prima facie, the mechanism established under the Data Protection Directive (and retained under the GDPR) gives a false sense of security for an effective oversight as its functioning in practice requires considerable hurdles to be overcome and lacks evidence that this oversight effectively functions in practice. In order to secure effective protection of EU data subjects' privacy, it is essential that the data protection bar is raised nationally in the third countries. It is argued here that domestic oversight and control could be much more effective than extraterritorial and contracted external oversight. Consequently, for further analyses on whether and how data transfer could take place, and what risks it could pose, detailed insight into data protection requirements in third countries and organizations is necessary.

Biobanking and data protection in selected African jurisdictions: an overview

Regional data protection

Although in many ways inter-state collaborations in Africa occur through regional legal constellations and in that respect it resembles the European regional legal environment, when it comes to data protection the approaches are not yet comparable. In the European legal environment, data protection has been strengthened in multiple ways. They include, first, general privacy protection provisions. Second, they include data protection specific instruments, in particular, (the original and modernised) Convention 108 and sector specific recommendations, in the Council of Europe system,[83] the Data Protection Directive and the GDPR in the EU. In contrast, in Africa, at the regional level the protection of privacy is addressed within a human rights regional system, the African Union, as well as within the Regional Economic Communities (RECs). In 2014, the African Union adopted the Convention on Cybersecurity and Personal Data Protection 2014. The overall objective of the Personal Data Protection section is for states to develop a legal framework to protect donor rights and information which will be applicable to the 'collection, processing, transmission, storage or use' of personal data processed by automated or non-automated means.[84] This convention addresses personal data protection in Chapter 11 under which it requires the parties to the Convention to implement data protection legislation in their countries. The requirements for the legislation include, but are not limited to, common elements such as an independent authority for personal data protection, guiding principles for processing personal data, data subjects' rights and requirements for data controllers.[85] The treaty will not be enforced until ratified by 15 members; it has been signed by nine

82 Corresponding to art 26.1 Data Protection Directive (n 25).

83 'Modernisation of Convention 108' (*Data Protection*) <https://www.coe.int/en/web/data-protection/convention108/modernised> accessed 9 May 2018.

84 See African Union Convention on Cybersecurity and Personal Data Protection, 2014, art 9.

85 African Union Convention on Cybersecurity and Personal Data Protection (n 82).

countries[86] and ratified by Senegal only.[87] Therefore, in as much as the convention was adopted, it has not yet come into force.

Africa's RECs include eight sub-regional bodies which are the building blocks of the African Economic Community established in the 1991 Abuja Treaty which provides the overarching framework for continental economic integration. Within the REC, multiple trade blocks are established that are predominantly concerned with trade (Community of Sahel-Saharan States (CEN-SAD), Common Market for Eastern and Southern Africa, East African Community (EAC), Economic Community of Central African States, Economic Community of West African States (ECOWAS), Intergovernmental Authority on Development, Southern African Development Community (SADC), and Arab Maghreb Union).[88] In some regions, eg EAC and ECOWAS, further frameworks on data protection have been adopted. In ECOWAS, the Supplementary Act on Personal Data requires Member States to enact legislation for the regulation of personal data 'collection, processing, transmission, storage and use'.[89] However, not all states that have signed it have acted towards implementing the requirements at the national level, eg Nigeria. In the SADC, a draft SADC Model Law on Data Protection has been developed which could affect the way laws are shaped in the community. In EAC, the only approximation to the AU Cybersecurity Convention is the EAC Legal Framework for Cyber Laws 2008 that was adopted by the EAC in 2010.[90] One of the fundamental principles of the treaty is the recognition, promotion, and protection of human and peoples' rights in accordance with the African Charter on Human and Peoples Rights (ACHPR). The EAC also passed the Protocol on the Establishment of the EAC Common Market which obliges members to also observe human rights. The EAC Legal Framework for Cyber Law laid down the procedure that the partner states should follow in establishing REC data protection policies.[91] This document contains recommendations addressed to the governments regarding national legal reforms to facilitate electronic commerce and further protection of data. Yet, its implementation rests with the national lawmakers rather than the regional actors. Therefore, the level of protection of personal data in biobanking can differ in different African countries, depending on their individual external commitments and additional national approaches in safeguarding informational privacy.

Kenya

The protection of privacy in Kenya is not only a constitutional obligation under Article 31 of the Kenya's new Constitution, which broadly interpreted could also be argued to embrace the protection of personal data,[92] but also an international obligation under Article 12 of UDHR[93] and Article 17 of ICCPR[94], which in accordance with Article 2(5) of the Kenyan Constitution forms part of the law of Kenya. However, as of now Kenya has no specific data protection law in force. To give full effect to the constitutional provision of privacy, Kenya developed its Data Protection Bill 2013 (Kenyan Bill).[95] Although considerable time has elapsed since the adoption of the bill, it is still in the legislative process, and therefore it is referred to in identifying what the Kenyan position would be.

Under the Kenyan Bill personal data are defined in a broad and inclusive manner as 'information about a person' in order to accommodate different types of data, such as various individual-related traits and characteristics, including health, medical records, blood, and fingerprints.[96] However, no special data category regime, such as that under the GDPR, is established under the Kenyan Bill. Although this is an inconsistency vis-à-vis the GDPR, in itself it might not necessarily be a challenge provided that a comparable level of protection as set out by the GDPR for special categories of data is secured for all types of data under the Kenyan Bill. While the bill provides a considerable list of information that is regarded as personal data, other information not listed there could also be regarded as personal data, eg genetic data. Furthermore, *prima facie* the definition fails to accommodate indirect identification, which then

86 'African Union Convention on Cyber Security and Personal Data Protection' <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection > accessed 9 May 2018.

87 Ibid.

88 'Regional Economic Communities | United Nations Economic Commission for Africa' <https://www.uneca.org/oria/pages/regional-economic-communities> accessed 27 December 2017.

89 Iheanyi Samuel Nwankwo, 'Information Privacy in Nigeria', African Data Privacy Laws (Springer 2016) 71.

90 For an overview of data protection laws in the region, see Makulilo (n 21).

91 Ronald Kakungulu-Mayambala, 'Privacy and Data Protection in Uganda', *African Data Privacy Laws* (Springer 2016) 117–142.

92 However, as explained by Makulilo, 'the Kenyan courts have not so far determined the scope of Article 31 of the Kenyan Constitution in terms of informational privacy'. Alex B Makulilo and Patricia Boshe, 'Data Protection in Kenya', *African Data Privacy Laws* (Springer 2016) 326.

93 UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

94 UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

95 Data Protection Bill 2013, Kenya <http://icta.go.ke/pdf/DATA_PROTECTION_BILL_FROM_AG_for_publication_to_Parliament.pdf> accessed 9 May 2018, s 3(a).

96 Ibid s 2.

could affect the extent to which individuals are protected. In order to maximize the scope of protection set up by the bill, as well as align the bill with the requirements of the GDPR, the notion of a person should be interpreted broadly to embrace not only identified but also identifiable persons. A narrow interpretation of personal data could affect the application of the bill to biobanking in which the practices of pseudonymization are commonplace. While it could be domestically seen as a research-enabling approach, it could be detrimental to international collaborations that would want to rely on the mechanism set up by the bill.

Data protection principles listed in the bill contain the data subject's rights and the biobankers acting as an 'agency' obligations, and correspond to those set out in the GDPR; their content, however, as discussed below, differs. The principle of lawfulness in biobanking requires that the data are collected for a lawful and explicitly defined purpose and are processed in a way that does not intrude on privacy. Furthermore, these data should be collected from the data subject with the data subject's consent, subject to appropriately informing the data subject. However, information without data subject's consent could be used for research provided it is not published in a form that allows the data subject to be identified.[97] The information is subject to storage limitation which requires that it is not kept longer than necessary for the purpose it was collected. In relation to the processing of personal data, accuracy, integrity, and data security should be ensured. Moreover, on a principles level, the data subject is provided with access rights and a right to demand the correction of the personal data. Although accountability is not part of the listed principles in the Kenyan Data Protection Bill, it is addressed through the obligations relating to the biobankers. It could be argued that lack of an explicit reference to a principle is not a challenge in itself from the perspective of the GDPR provided the content this principle embraces is enshrined in the bill.

Data subjects under the Kenyan Bill are endowed with a number of rights to oversee the lawful use of their personal data in biobanking from which further derogations are not foreseen. Among the rights that are of particular relevance to biobanking are the right to privacy,[98] to be notified of the fact and purpose of data collection,[99] identity of data collection agency, recipient of information for informed consent, consequences of refusal to supply required information, information of place of origin of the data, intended use of the data, intended recipients, access to data,[100] rectification of incorrect personal information, and deletion of illegally processed data or false or misleading data.[101] The data subjects have a right to lodge a complaint with the Commission of Administrative Justice.[102] Although under the Kenyan Bill these rights cannot be derogated from or waived by the data subjects, it is too early to conclude that as far as biobank research is concerned the data subjects will be equipped with broader set of rights than the lowest standard possible under the derogations under Article 89 GDPR and further derogations under Articles 13, 14, 17, 19 and 20 as the bill does not include some of the rights the GDPR allows derogations from (eg such rights as the right to restricting processing, notification entitlement, as well as data portability and the right to object to data processing). Although the bill sets out a number of obligations, including ensuring data security, the relevant provisions in the bill lack specificity. This means that although they could be interpreted broadly and inclusively, it is uncertain whether they would be able to accommodate such obligations as privacy by design and default, risk assessment, as well as involvement of a data protection officer.

Biobankers under the Kenyan Bill as data controllers or processors are subject to a number of obligations. They include non-disclosure of personal information, maintenance of privacy and confidentiality,[103] grant of access to information,[104] lawful processing,[105] purpose limitation use of data,[106] notification on change of purpose,[107] notification that waiver amounts to consent,[108] to inform the data subject of the purpose of data collection and get consent,[109] rectification of incorrect data, deletion of false or misleading data, the right to erasure of illegally processed data,[110] implementation of security safeguards,[111] limited storage of information,[112] and non-commercial use of information except when granted consent.[113]

An independent supervisory authority—the Commission of Administrative Justice—that operates under the Kenyan Constitution is in place to ensure

97 Ibid s 9(g)(ii).
98 Ibid s 5.
99 Ibid s 7.
100 Ibid s 12.
101 Ibid s 13.
102 Ibid s 22.
103 Ibid s 11.
104 Ibid s 12.
105 Ibid s 8.
106 Ibid.
107 Ibid s 7 (5).
108 Ibid s 7 (6).
109 Ibid s 7 (1).
110 Ibid s 13.
111 Ibid s 11.
112 Ibid s 15.
113 Ibid s 17.

oversight of the implementation of the Kenyan Bill and enforce it.[114] The bill enables data subjects to submit complaints to the Commission for violations of the provisions of the bill.[115] The Commission is empowered to declare violations under the bill as well as make orders restraining biobankers from further violations, request remedy of violations and decide on an appropriate relief.[116] However, should the Commission decide to take no action on the issue, the bill does not expressly provide a right to appeal. Unless appeal avenues exist through other relevant requirements, the effectiveness of the oversight of the Commission could be hampered. As violations of the data protection requirements set out in the bill are offences, biobankers risk facing a fine not exceeding 100,000 shillings or imprisonment for a term not exceeding two years or both. Furthermore, the data subject could be advised to seek damages in court against the biobanker. In that situation, the burden of proof lies with the biobanker to demonstrate compliance with the applicable data protection requirements.[117]

Overall, the Kenyan Bill creates a framework for the protection of personal data. It sets out internationally acknowledged principles for data protection, albeit filling it with a localized content, which on a number of occasions is a quite simplified and generalized version of the requirements stemming from the GDPR. Although the bill enables processing of data for biobanking, some concerns can be raised concerning the protection that will be afforded to the data subjects given the uncertainty about the scope of personal data and lack of special protection of genetic data (or lower levels of protection of personal data), as well as a lack of detailed obligations on the part of biobankers. Should the bill pass, it could be relatively difficult for Kenya to uphold the data protection standard set out by the GDPR.

Nigeria

The protection of privacy in Nigeria is a constitutional obligation under section 37 of the Constitution of the Federal Republic of Nigeria 1999, as well as a state's international obligation. Currently, there is no specific national legislation governing personal data protection; however, there are policies under consideration. The Data Protection Bill 2010 was the first drafted to address data protection in Nigeria; however, it was not passed. In 2016, Nigeria's Protection of Personal Information Bill (Nigeria's Bill) was adopted for inter alia promoting the protection of personal information and give effect to the constitutional right to privacy.[118]

Under section 1, 'personal information' means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to traits and features listed in the bill. While physical and mental health, as well as blood type and biometric information is *expressis verbis* listed in the bill, genetic data is not. However, part B of the bill distinguishes between special personal information and other personal information; this includes health information and alludes to 'information concerning inherited characteristics'. Inherited characteristics could arguably be interpreted as genetic information. Processing of this information is prohibited, unless exceptions set forth in the bill apply.[119] For example, health data is accessible according to a contract and with consent, and information concerning inherited characteristics is accessible for scientific research; thus, the limitations do not appear pre-emptive. The Bill could align with the GDPR by ensuring that genetic data has comparable protection. Similar to the Kenyan Bill, Nigeria's Bill refers to identifiable persons, arguably excluding indirectly identifiable persons from its scope. For Nigerian biobanks to access data from EU entities, Nigerians must protect information attainable by pseudonymization, as they would identifiable persons.

Nigeria's Protection of Personal Information Bill refers sets forth data protection principles that correspond to those enshrined in the GDPR. Sections 8–11 detail processing limitations, subjecting responsible parties to the requirement of lawfulness. The principles of lawfulness established in Chapter 3, enable data collection, following legitimate grounds. The Bill requires provider consent for biobankers to collect,[120] process,[121] and/or retain,[122] personal information. Similarly, secondary use and international distribution are only possible pending consent.[123] Purpose specification requires that personal information be collected for a specific, explicitly defined, and lawful purpose related to a function or activity of the responsible party[124] and storage

114 Ibid s 20.1.

115 Ibid s 22.1.

116 Ibid s 25.

117 Ibid s 26.

118 Preamble and s 2.1 'Nigeria's Protection of Personal Information Bill 2016' <https://www.nassnig.org/document/download/8938> accessed 10 May 2018.

119 In regard to health data that are listed in s 30 'Nigeria's Protection of Personal Information Bill 2016', see Nigeria's Bill, ibid.

120 Nigeria's Bill (n 115) ss 11 and 15.

121 Ibid ss 10 and 15.

122 Ibid s 14.

123 Ibid ss 15 and 69.

124 Ibid s 12.

limitation prohibits information retention longer than is necessary for achieving the purpose for which the information was collected or processed, unless stated exceptions apply.[125] In regard to research, section 14.2 makes an exception, allowing further retention if the responsible party has established appropriate safeguards against the records being used for other purposes. Hand in hand with the storage limitation goes the principle of further processing limitation. Research is listed among the exceptions, and thus further processing is possible, if the responsible party ensures that the further processing is performed solely for research purposes and will not be published in an identifiable form.[126] Nonetheless, what is meant by research is unspecified in the bill. The information quality principle mandates to ensure accuracy and take steps in that regard. Furthermore, section 17 enshrines openness, mandating transparency vis-à-vis the data subject, and the principle of data subject participation, enabling subject access. Through the principle of security safeguards, data security and confidentiality are guaranteed.[127] Under section 7, the responsible party is required to give effect to the principles set forth in the bill. However, the protection provided by these principles is not absolute. Under section 34(2)(e), the Information Protection Regulator may authorize processing of personal information despite a breach of an information protection principle for research activity. While this option may seem research-enabling, additional attention is essential to prevent abuse of discretion.

Data subjects are empowered with a host of rights pursuant to the Nigeria's Protection of Personal Information Bill. As discussed, access to personal information is restricted and limited by informed consent and the language thereof. Thus, consent provides means for the data subject to grant/deny secondary access, use in specific types of research, additional processing, and long-term retention. Even if consent is given, the subject may object to the processing of their personal information at any time.[128] After consent, the responsible party must ensure the information is 'complete [and] accurate.'[129] Additionally, the provider reserves the right to access his/her personal information and have any discrepant information rectified by the responsible party.[130] More specifically, a subject can request for the biobank to correct or delete inaccurate, irrelevant, excessive, incomplete, misleading or unlawfully obtained personal information; and destroy or delete information stored beyond the retention period.[131] Data subjects must be informed of the purpose for which their information will be used,[132] the information to be collected, responsible party's name and address, whether disclosure is voluntary, consequences of nondisclosure, recipients or categories of recipients of the information, the nature of the information, and applicable law mandating collection.[133] Providers also have the right to file a complaint.[134] Similar to Article 89 of GDPR, there are derogations from individual rights for research, subject to authorization from the Regulator.[135]

Under the bill, biobankers acting as controllers and processors ('Responsible Party') must register with the Regulator and are accountable to the Regulator.[136] As such biobankers must inform the regulator of intentions to process personal information, the purpose, the description of categories of information, and intention to share information,[137] as well as fulfil a number of other obligations, including the retention of processing records as required by law or code of conduct; safeguard information against loss, damages, destruction, and unauthorized use;[138] report suspected and/or potential unauthorized access;[139] ensure rectification or erasure.[140] The biobanker has additional obligations to the data subjects in order that their rights be genuinely exercised.[141] Moreover, the biobanker is under an obligation to ensure fulfilment of other principles, eg data accuracy,[142] and fulfil specific obligations when granting additional processing.[143] Not only are biobankers required to maintain confidentiality and generally accepted security practices, they must also ensure that anyone processing information in their behalf abides by these measures,[144] and take specific steps in case of data transfer.[145] In the event of data protection breaches, the biobankers must report breaches to the Regulator and the subject in writing.[146]

125 Ibid s 14.1.
126 Ibid s 15(3)(e).
127 Ibid ss 18–21.
128 Ibid s 10.
129 Ibid s 16.
130 Ibid s 17.
131 Ibid s 23.
132 Ibid ss 13 and 17.
133 Ibid s 17.
134 Ibid Ch 10.
135 Ibid Ch 4.
136 Ibid s 48.
137 Ibid s 51.
138 Ibid ss 18 and 14.
139 Ibid s 21.
140 Ibid ss 23 and 55.
141 Ibid s 17.
142 Ibid s 16.
143 Ibid s 15.
144 Ibid s 19–20.
145 Ibid s 51.
146 Ibid s 21.

Under the bill, the Information Protection Regulator is established, as an independent data protection authority operating under the Nigerian Constitution.[147] The regulator, inter alia is tasked to monitor and enforce compliance by public and private bodies of the provisions of this Act.[148] Persons alleging interference with the protection of the personal information of a data subject can submit complaints to the Regulator,[149] which then is obliged to duly investigate them.[150] The Regulator may decide whether to take action and determine if the case should be handled by another body. If action is deemed necessary, the Regulator may prescribe recommendations and/or issue an enforcement notice to take or suspend specific activities. Noncompliance with an enforcement notice or knowingly providing false statements is subject to fine and/or imprisonment. Parties may appeal decisions of the Regulator, and the Data subject or the Regulator may file a civil action in court for damages.[151] Damages can relate to patrimonial and non- patrimonial loss, aggravated damages, interest, and trial costs.[152] Parties may settle. Settlements and agreements may be published in public media.[153]

Once implemented, Nigeria's Bill will provide a stronger foundation for personal information protection, upon which policy statements such as the current National Health Research Ethics Committee's (NHREC) Policy Statement on Biobanks can rest. The bill reflects many of the principles and requirements observed in international law pertaining to data protection. Considering the legal framework surpasses biobanking the efforts required to inform persons of what is required, monitor ongoing activities and adjudicate non-conformities may limit effectiveness. For efficiency, the regulator may seek to engage discipline specific organizations, such as NHREC to assist in education, implementation, and monitoring.

South Africa

The right to privacy is protected as a fundamental right under Chapter II, section 14 of the South African Constitution. The constitutional protection of privacy extends to those aspects of a person's life regarding which the person has a legitimate expectation of privacy.[154] In order to give effect to the constitutional right to privacy as well as effectively protect data subjects from harm, South Africa adopted the Protection of Personal Information Act No 4 of 2013 (POPI).[155] However, this Act has not yet been fully implemented.[156] Its effective date is still uncertain as it is at the President's discretion to proclaim the date.[157] For the purposes of this review, however, POPI in full will be analysed.

Under POPI, personal information is defined as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing, juristic person, including, but not limited to, physical or mental health or the biometric information of the person.[158] Although the provision is constructed rather narrowly, similar to the Kenyan Data Protection Bill it could be argued that identifiable relates to the directly and indirectly identifiable information as set out in section 6 of POPI where it is emphasized that the Act does not apply to data that have been de-identified to the extent that they cannot be re-identified again. Therefore, it could be said that POPI has adopted a similar approach to that found in the GDPR. POPI makes a distinction between special personal information, which includes information about health and biometrics (which in itself includes DNA analysis), as well as other types of personal information, enshrining a general prohibition to process the latter unless exceptions apply.[159] Under POPI, research falls under a general exception provided that the purpose serves a public interest and the processing is necessary for the purpose concerned or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.[160] In that way, POPI not only requires privacy protection in research, albeit implicitly limiting the data subject's rights in that regard, but also requires the research to serve a public interest which is in line with the aspirations of the

147 Ibid s 35.
148 Ibid s 43(d).
149 Ibid s 71(a).
150 Ibid s 73.
151 Ibid Ch 10.
152 Ibid s 94.
153 Ibid Ch 11.
154 Anneliese Roos, 'Data Protection Law in South Africa', *African Data Privacy Laws* (Springer 2016) 196.
155 Preamble of POPI, as well as Ch 1, s 2 'Protection of Personal Information Act 4 of 2013' <https://www.gov.za/documents/protection-personal-information-act> accessed 9 May 2018.
156 'Protection of Personal Information Act: Commencement of Section 1, Part A of Chapter 52 and Sections 112 and 113' < https://www.gov.za/documents/protection-personal-information-act-commencement-section-1-part-chapter-52-and-sections> accessed 9 May 2018.
157 It is likely not to be before the Information Regulator is operational, which might be towards the end of 2018 but may only be in 2019. Thus the POPI compliance deadline might only be at the end of 2019 or in 2020 taking in consideration the one-year grace period in accordance to which the Information Regulator will only start enforcing POPI one year from the commencement date.
158 POPI (n 152) s 1.
159 Ibid ss 26–33.
160 Ibid s 27(1)(d).

'Ethics and Governance Framework for Best Practice in Genomics and Biobanking Research in Africa'.

POPI sets out data protection principles that should be observed by the biobanker as the responsible party when POPI applies.[161] Overall, these principles correspond to those set out in the GDPR with an additional principle—that of further processing—which is considered below. The principle of lawfulness is approached as an umbrella-principle to embrace a number of other principles and conditions that must be met in order for data processing under POPI to be permissible. As indicated above, biobanking benefits from a research exception. Moreover, other exceptions could apply if so authorized by the Information Regulator.[162] This discretion, however, should be rather narrowly approached in order not to undermine the level of protection set out by the Act. Although POPI sets out several legal grounds for the collection of personal data, for the purposes of biobanking the consent requirement applies, which is also subjected to purpose specification.[163] However, from that it does not follow that excessive hindrances to research are created as secondary use of personal data for biobanking is permissible provided appropriate measures in that regard are taken.[164] In the course of biobanking, personal information must not only be processed lawfully but also in a reasonable manner that does not infringe the privacy of the data subject,[165] that is in compliance with the purpose it was collected for or meets the requirements for further processing,[166] and that is adequate, relevant and not excessive.[167] Biobanking under POPI is subject to an information quality requirement which mandates that personal information is complete, accurate, not misleading and updated where necessary.[168] Furthermore, biobankers must observe the requirements related to data security and confidentiality.[169] The question of fairness and transparency is addressed through the principle of openness towards a data subject,[170] as well as the principle of 'data subject participation' which relates to a number of rights of the data subject, including access to personal information and correction of information, including its deletion. Furthermore, the biobanker as a responsible party must ensure that all principles are observed and that the necessary steps have been taken to give full effect to the data protect requirements that stem from POPI.[171]

Section 5 of POPI sets out a list of the data subjects' rights, enabling them to actively participate in the protection of their privacy. The rights include those set out in the GDPR such as the right to information, access, rectification and erasure; restriction of processing a right to object; complain; and a right to seek access to justice and redress via the courts.[172] Unlike the GDPR, POPI does not seem to *expressis verbis* address the right to representation and data portability. However, this difference is not likely to be one to affect collaborative research as portability is a right that can be derogated from under Article 20 of the GDPR and representation as enshrined in Article 80 GDPR does not undermine the rights related to access to justice of the data subjects.

Under POPI, persons involved in the processing of personal data are subject to a number of obligations. They resemble those stemming from the GDPR albeit are often labelled differently. They include records of processing activity and security of the processing in regard to which POPI is in alignment with the GDPR. However, these are not specific for biobanking per se but apply to all clinical and health organizations and institutions.[173] Moreover, a data protection officer should be appointed to work towards the data protection requirements in the biobank.[174] The persons processing data are responsible for the cooperation with the supervisory authority and notification of a personal data breach to the authority in that regard.

Under POPI, an independent Information Regulator must be established for the purposes of effective data protection oversight.[175] Among its duties is to monitor and enforce compliance with the Act and address complaints in regard to violations.[176] Any person is entitled to submit a complaint to the regulator[177] who should then act on the issue. It can carry out investigations.[178] Its decisions can range from declaring a matter to be

161 Ibid s 4.
162 Ibid s 27.2.
163 Ibid s 11.
164 Ibid s 14.2.
165 Ibid s 9.
166 In addition to the processing limitation, also the question of 'further processing limitation' is addressed at a principle level under POPI. Although research is not *expressis verbis* mentioned as enabling further processing, providing general pre-conditions are met, research could be argued to be possible. S 15.
167 POPI (n 152) s 10.
168 Ibid s 16.
169 Ibid ss 19–22 and 35.
170 Ibid ss 17 and 18.
171 Ibid s 8.
172 Ibid s 5.
173 Ibid s 8.
174 Ibid Ch 5 Part B.
175 Ibid s 39.
176 Ibid ss 39 and 40.
177 Ibid s 74.
178 Ibid s 81.

trivial[179] to securing a settlement.[180] Decisions taken by the regulator are subject to appeal to the High Court.[181] Moreover, the regulator can carry out compliance assessments on its own initiative or at the request of or on behalf of the responsible party, data subject or any other person. It must make an assessment in the prescribed manner to determine whether an instance of processing of personal information complies with the provisions of this Act.[182] The penalty for a breach of privacy is dependent on the severity of the harm or distress caused. It can include termination of employment, sanctions by the HPCSA (including being struck off the roll of practitioners), a damages award of monetary compensation to the affected data subject (up to ZAR10 million) or imprisonment for a maximum of 10 years.[183] At the data subject's disposal are civil remedies to mitigate the harm suffered by the data subject.[184]

Overall, on the surface, POPI sets out a similar data protection framework for biobank research to that established under the GDPR. However, it is unclear when this framework will come into effect as the remaining parts of POPI must be given effect and a grace period is yet to be applied to allow for compliance with the requirements set out in the Act. When POPI is operationalized, it is likely that collaborative research could take place with a degree of security on the data subject's rights in South Africa.

Uganda

Article 27 of the Constitution of Uganda firmly protects the right to privacy. Although data protection is not *expressis verbis* enshrined in the Constitution, it has been argued that this provision could apply to it.[185] The Data Protection and Privacy Bill 2015 (Uganda's Bill) was developed to lay down detailed protection in the area of data protection as adduced from the bill's objective.[186] Yet, as the law is not in force yet, informational privacy continues to be protected under the Constitution and the country's external commitments, particularly the ICCPR and UDHR, as well as regional instruments in the EAC, particularly the EAC Legal Framework for Cyber Laws. However, for the purposes of this review, Uganda's Data Protection and Privacy Bill will be analysed.

Under the bill personal data means any information in a recorded form about a person from which the person can be identified. It can include such things as nationality, age, occupation, and educational level.[187] Similar to the Kenyan Bill, Uganda's Bill focuses on an identified person; a grammatical interpretation could risk narrowing the scope of application of the bill as defined in Clause 1. Therefore, in order to effectively protect the right to privacy in biobanking where it is common practice for a person to be pseudonymized, the definition of personal data should be interpreted broadly to embrace not only direct identification but also indirect identification. Such an approach could also align the bill with the corresponding approach in the GDPR. The definition of personal data does not *expressis verbis* include health-related or genetic information. Nonetheless, as it is drafted openly it could also accommodate this kind of information. The bill is not data-type neutral; under Clause 5 a distinction is drawn between special personal data and other types of data. However, the special data type group does not include either health, genetic or biometric data. As the bill further delineates a distinction in protection between these two categories of data, leaving genetic data out does not necessarily mean providing them the lowest of two alternative protections, which from the perspective of the GDPR could be challenging. As shown below, data in biobanking *prima facie* could be processed with informed consent only, which means that individuals have control over whether they wish to participate in research or not. Nonetheless, it could be argued that Uganda's Data Protection and Privacy Bill does not accommodate international calls for the protection of genetic data, such as those expressed under the UNESCO[188,189] International Declaration on Human Genetic Data and Universal Declaration on the Human Genome and Human Rights.

Clause 3 sets out principles for data protection which should be complied with by biobankers under the oversight of the authority and for which biobankers are accountable to data subjects.[190] Similarly to the Kenyan

179 Ibid s 77.

180 Ibid s 80.

181 According to Ch 10, s 97 a responsibility party has the right to appeal and the High Court have jurisdiction POPI (n 152).

182 POPI (n 152) s 89(1).

183 South Africa. POPI Act No 4 of 2013. Ch 11: Offences, penalties and administrative fines, ss 100–109. M Buys, 'Protecting Personal Information: Implications of the Protection of Personal Information (POPI) Act for Healthcare Professionals' (2017) 107 South African Med J = Suid-Afrikaanse Tydskrif Vir Geneeskunde 954.

184 POPI (n 152) s 99.

185 Kakungulu-Mayambala (n 90).

186 'The Data Protection and Privacy Bill 2015' <http://parliamentwatch.ug/wp-content/uploads/2016/10/Data-Protection-and-Privacy-Bill-2015.pdf > accessed 9 May 2018.

187 Uganda's Bill (n 183) clause 2.

188 UNESCO, International Declaration on Human Genetic Data (16 October 2003), art.23.

189 UNESCO, Declaration on the Human Genome and Human Rights (11 November 1997), art 22.

190 Ibid clause 3.

and South African offering, Uganda's Bill contains principles that correspond to those in the GDPR, albeit are further in the bill elaborated with departures from the GDPR. Data should be collected and processed fairly and lawfully, which in the context of biobanking means that data should be collected with the consent of the data subject unless other legal grounds exist. In the bill's current draft, Clause 9.2 foresees a possibility of data being collected from a third party and not the data subject. This would mandate the biobanker informing the data subject on the data collection as far as practicable. Furthermore, the bill tasks the biobanker with the responsibility of ensuring data adequacy, accuracy, relevancy, and minimization, as well as retention of the data for the required purpose and period authorized by law.[191]

Further processing is enabled for research purposes[192] provided that it is solely used for research and in the course of publication identity is not revealed. It is also the responsibility of the biobanker to ensure the quality of the information and provide the necessary security safeguards. The data subjects' rights are protected by ensuring that the biobanker has fulfilled transparency and participation requirements, which include observing the data protection principles, and fulfilment of obligations and respect for the rights related to these principles.[193] The biobanker must also ensure the necessary legal and security measures have been put in place.[194] Concerning security, while a data protection officer is not a requirement, risk assessments, safeguard implementation, as well as verification that the safeguards will be effectively implemented and updated do need to be put in place. Moreover, the biobankers are required to observe generally accepted security practices and procedures in biobanking,[195] thus allowing for self-regulation by biobankers and protection of the research.

The data protection framework has empowered individuals with quite a number of rights with regard to collection of their personal data. The bill provides a set of rights to the data subjects, including a right to access their personal information;[196] to prevent the processing of personal data;[197] rectification, blocking, erasure, and destruction of personal data;[198] as well as rights related to data protection oversight and effective judicial remedy addressed below. Although the bill does not expressly provide a right to information for data protection violations, under Clause 19 the National Information Technology Authority-Uganda (NITA-U) may order the biobanker to inform a data subject. Overall, the data subject under Uganda's Bill seems to be equipped with rights similar to those stemming from the GDPR, albeit without notification entitlement and a right to data portability. As these rights can be derogated from under the GDPR in certain situations, it could be argued they are not detrimental to research provided other relevant requirements, such as data security and minimization, are secured.

NITA-U is a government body that was established by the NITA-U Act of 2009 with the mandate to coordinate and regulate information technology services in Uganda. This mandate has been extended to include oversight and enforcement of the Data Protection Bill. The authority's impartiality may be compromised by the fact that the Minister is the ultimate person with powers over the authority. This means that impartiality such as that required by the GDPR is not yet part of Uganda's framework. Individuals, as well as biobankers themselves may complain about breaches and the authority must investigate these claims,[199] as well as appeals against the decisions of the authority to the Minister should an individual be dissatisfied with its decision.[200] In the event an individual suffers damage or distress, they can seek compensation.[201] The bill is silent on what happens when one is dissatisfied with the Minister's decision. However, Article 42 of the Constitution allows for any person that has been aggrieved by a decision of an administrative official or body to apply to court for review of that decision.

Under the bill, not all violations of the revisions set out in Uganda's Bill are offences. The violations classified as offences involve obtaining or disclosing data held by the biobanker or disclosing to a third party without consent which could result in a fine not exceeding 240 currency points or imprisonment not exceeding 10 years or both. In effect, this means that violations of the bill that undermine data subjects' privacy but are not offences risk only a compensation request by the data subject, which in reality might be burdensome for the data subjects—something the GDPR has departed from. If this approach is retained under Uganda's Bill, one could argue that effective protection of informational privacy not only in biobanking but more

191 Ibid.
192 Ibid clause13(3)(e).
193 Ibid clause 3.
194 Ibid clauses 17 and 19.
195 Ibid clause 16.
196 Ibid clause 20.
197 Ibid clasue 21.
198 Ibid clasue 24.
199 Ibid clause 28.
200 Ibid s 30.
201 Ibid s 29.

generally is undermined. Moreover, due to the challenges caused by the literacy levels of a considerable proportion of biobank research participants and other considerations such as the judicial complexities, it is unclear how effective this possibility will be.

All in all, although Uganda's Bill sets out a privacy protection framework for personal data, from the perspective of the GDPR and research regulation it can be argued that it is in need of further attention. Not only has genetic data not received special attention, with numerous calls for its protection being disregarded, but the bill also leaves room for interpretation regarding its scope, which could cause ambiguities in its application. Although a number of rights do not exist in the bill which are provided under the GDPR, its nucleus is enshrined in the bill. As a result, individuals in biobanking will receive a fair degree of protection. That protection, however, could be undermined due to the weak and non-impartial enforcement mechanism set up under Uganda's Data Protection and Privacy Bill. In order to strengthen data protection in the area of research, which is crucial for effective data exchange for research, these points should be addressed, along with revisions of other related clauses of the bill.

Concluding analysis: is data transfer in biobanking between EU and selected African states realistic?

For the purposes of ascertaining whether and to what extent the selected African states could meet the requirements for transfer of data under EU data protection law, and what, if any, challenges could emerge should transfer take place, a further step needs to be taken beyond what has already been done, namely in 'Biobanking under the GDPR', the requirements that the GDPR sets out for biobanking were reviewed; in 'EU data transfer requirements', the possibilities to carry out data transfer were identified; and in 'Biobanking and data protection' the differing national data protection regimes in selected African countries were explored to understand the relevant regional protections in the area. What is left is to examine is whether data transfer in biobanking between EU Member States and selected African states, specifically Kenya, South Africa, Nigeria, and Uganda, is realistic, and what challenges it could bring.

Under the GDPR, an exhaustive list of data protection requirements can only be established in relation to the particular situation in which data are being processed. However, this does not preclude identifying the requirements that are of particular importance to biobanking. As demonstrated in 'Biobanking under the GDPR', first of all, they include compliance with the fundamental data protection principles set out in Article 5 GDPR and further elaborated in the regulation. Other relevant requirements include a duty to implement appropriate technical and organizational measures to ensure and demonstrate compliance with the GDPR, ensure data protection by design and default, the recording of processing activities, a duty to cooperate with the supervisory authority, data security, notification of a data breach to the authority and data subject, as well as data protection impact assessment. Moreover, they include a spectrum of data subject rights that after derogations under Article 89 GDPR might seem on the surface to be as little as the right to information, the right to erasure, data portability, and notification entitlement, complemented with key rights attributed to effective data protection, namely, a right to complain and a right to an effective judicial remedy and representation in that regard, should the data subject wish so. Yet, additional derogations in certain situations relevant to biobank research of right to information, the right to erasure, data portability, and notification entitlement are possible under Articles 13, 14, 17, 19 and 20 GDPR, thus leaving the data subject with means only to protect the rights.

When external data transfer for biobanking occurs, the protection required by the GDPR must be upheld, along with fulfilling the conditions for data transfer. As examined in 'EU data transfer requirements', several avenues for transferring data to African research institutions exist under the GDPR. However, these possibilities do not come without challenges. For collaborative biobanking research with African states, and notably those reviewed (Kenya, Nigeria, South Africa, and Uganda), transfer based on appropriate safeguards is the most feasible option. This option, however, rests on the assumption on the part of the EU that the data protection regime can be easily externalized without undermining the data protection of the EU data subjects. In this article, it has been argued that this externalization is an illusion of protection rather than genuine protection for the data subjects. This relates to the lack of an effective oversight and limitations of the European data supervisory authorities operating under the national administrative laws in the national jurisdictions. Although it appears that the European Commission is aware of this challenge, it will take time and effort to overcome it via such means as Article 50 GDPR that the article instructs the Commission to collaborate internationally on enforcement matters. Moreover, this kind of transfer places the biobank researchers in the EU as data senders in a challenging position and mandates assuming

considerable responsibilities. One might question what the interest is for EU senders to assume the responsibilities that come with the liabilities under the GDPR, and whether this interest could not be furthered by other means which could, however, be detrimental to capacity-building and collaboration, such as parachuting. Raising the privacy bar is essential to genuinely further capacity-building in biobanking as well as protect the privacy of data subjects.

In all four countries that have been reviewed privacy merits constitutional protection which, if broadly interpreted, could embrace data protection. Yet, none of the four reviewed countries currently has a specific and fully effective data protection framework. While in South Africa the framework is partially in force, in Kenya, Nigeria, and Uganda they are yet to be passed. This means that currently the protection of personal data relies largely on the constitutional and international protection granted to the right to privacy. The extent to which it could be enforced and what protection could be afforded to the data subjects remains uncertain as it requires not only considerations as to the rights and interests of the data subjects but also legitimate expectations and legal certainty on the part of biobankers. Therefore, currently, data protection in these counties remains theoretical rather than practical.

The reviewed legislative initiatives in all four countries aspire to give effect to the constitutional right to privacy. The approaches adopted by the countries, however, differ significantly and so also the possible future level of data protection. The South African as well as Nigerian framework, eg has a considerable degree of similarity with the content of the GDPR prima facie, leaving nuances only as differences. The exact importance of these nuances remains subject to further scrutiny. Regarding Kenya and Uganda, more significant discrepancies vis-à-vis the GDPR emerge. Although Kenya and Uganda take a different approach regarding the protection of a special category of data, which in itself has been argued not to be problematic, the challenge vis-à-vis the GDPR emerges when genetic data are offered the lowest of the alternate protection possibilities. Whereas in Nigeria, higher standards are established for health data; although, genetic information is not explicitly identified. For a comparable and high level of protection, the highest possible standard is to be followed, unless the lowest corresponds to the highest standard in the GDPR. Additional challenges regarding Uganda could be seen as risks to data exchange for biobanking; they include the question of impartiality of the supervisory authority, as well as arguably inadequate enforcement possibilities. Should the drafts of Kenya and Uganda be adopted, considerable steps will need to be taken to provide adequate safeguards for data transfer from the EU to be possible. Should the transfers take place, it is unlikely that the risks that emerge under the EU GDPR regime could be mitigated.

In the long term, and taking a positive stand, there does seem to be a broad consensus regarding the need to protect personal data in and after international transfer. If states could agree on the same or at least similar basic rules for processing of personal data, thereby creating mutual trust, administrative cooperation and mutual recognition, in regards to standards of protection may be possible.[202] The opposite development is less reassuring if individual countries enact measures to hinder transfer of personal data unless specific national criteria are not met. In the short term, however, the GDPR requires a specific compensatory measure on a case by case basis in order to allow transfer of data. These compensatory measures depend on the involvement of administrative and judicial actors in the countries involved which, as pointed out above, is challenging, and could therefore significantly affect collaboration.

Capacity-building in biobanking is not a one-way road. It is a collaborative relationship that requires activities on both sides from the sending and receiving country. It requires a genuine interest and mutual hard work towards pursuing this interest. Failure to acknowledge this and take actions in that regard could risk watering down the capacity building activities to aid in biobanking only. Although aid in itself could bring benefits, it would not resolve such concerns as the isolation of African researchers from joint work towards scientific advances and would not eradicate such easy shortcuts as parachuting. Thus, considerable responsibility is placed in the hands of the legislatures in the countries of concern, both the EU and in the African states—and notably in Kenya, Nigeria, and Uganda—to set foundations for ending research and research integrity-harming practices. South Africa and Nigeria, however, have taken a big step towards building routes for genuine biobank capacity-building in the country and collaboration in that regard.

doi:10.1093/idpl/ipy010

202 Henrik Wenander, 'A Toolbox For Administrative Law Cooperation Beyond The State' in Anna-Sara Lind and Jane Reichel (eds), *Administrative Law Beyond the State – a Nordic Perspective* Liber (Martinus Nijhoff Publishers, 2013).