Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108

Santa Slokenberga*

Key Points

- Convention 108 is the first international data protection treaty. Upon entry into force of the Protocol modernizing the convention in the near future, Convention 108 will become Convention 108+ and will gain the potential to become a global standard-setter in the field of data protection.
- Even though Convention 108 and Convention 108+ have close ties with the European Union, Convention 108+ can be expected to have different impacts in regard to adequacy assessments in different national legal orders, and hence varying potential to contribute to building data transfer avenues for biobank research.
- An adequacy decision is not a decision on the adequacy of the data protection regime *stricto sensu* but, in fact, requires the adequacy of the legal system in the respective country to be in place and its capability to uphold the fundamental right to privacy as a key pillar of a democratic legal system where a data subject has adequate seclusion not only from other individuals but also from the state.
- In order to enable sustainable collaborative research, in addition to raising the data protection bar and strengthening biobanking in Cape Verde, Mauritius, Morocco, Senegal, and Tunisia, the efforts should go further and strengthen democracy, human rights, and rule of law.

Biobanking, data sharing, and states of interest

Biobanking is a privacy-intrusive activity. With advances in biobanking and its associated science, the intensity and depth of privacy intrusions are increasing. These intrusions can occur in a number of ways, which can be largely divided into the following three groups: first, through the sample and data collection, and in particular, the approach that is being used for participant recruitment, types of specimen, and how they are obtained; secondly, through data processing during research; and thirdly, during data and sample sharing. The latter two steps have in particular advanced in the last decades. Now, not only is it common for the sample annotation and storage location to have been digitalized[1] but also for various software solutions to have been operationalized in order to support biobanks in administrative and research practices.[2] Relatively recently virtual biobanks have also become common,[3] which allows for easier and faster data exchange. Finally, data depositing in compliance with, inter alia, data

* Santa Slokenberga, Lund University, Lund, Sweden. Email: santa.slokenberga@jur.lu.se

1 See Hocine Bendou and others, 'Baobab Laboratory Information Management System: Development of an Open-Source Laboratory Information Management System for Biobanking' (2017) 15 Biopreservation and Biobanking 116.

2 Yvonne G De Souza and John S Greenspan, 'Biobanking Past, Present and Future: Responsibilities and Benefits' (2013) 27 AIDS 303. Heimo Müller and others, 'From the Evaluation of Existing Solutions to an All-Inclusive Package for Biobanks' (2017) 7 Health and Technology 89.

3 Babette LR Reijs and others, 'The Central Biobank and Virtual Biobank of BIOMARKAPD: A Resource for Studies on Neurodegenerative Diseases' (2015) 6 Frontiers in Neurology 216.

sharing and open science requirements has also given rise to considerable privacy-related questions.[4]

Data and sample sharing is key pre-requisite for biomedical advances. Just as a sufficient amount and a high enough quality of biospecimen and data have the potential to accelerate translational research and clinical discoveries, their lack can stall research and limit scientific advances.[5] Sharing concerns exist both in research collaborations between actors within the European Union (EU), in which Biobanking and BioMolecular Resources Research Infrastructure-European Research Infrastructure Consortium European Court of Human Rights General Data Protection Regulation (BMRI-ERIC) has a prominent role to play,[6] as well as between EU countries and third countries, for example, states in Africa, in which several considerable biobank capacity-building initiatives have taken place, or international organizations such as IARC BioBank, which is among the largest, most varied, and richest collections of samples in the world.[7]

In addition to the potential to further scientific advances, which is in the EU's interest,[8] data and sample sharing by EU countries with third countries can contribute to establishing ethical research practices. Specifically in regard to states in Africa, it includes a contribution to local capacity building through which the ethical duties to advance science can be furthered and solid grounds for the eradication of unethical research practices set. For this to happen, it is essential that two-way data sharing is enabled. Not only should researchers working for the infrastructures in the EU be able to import data from the third countries, and in particular, states within Africa, but they should also be able to transfer data from these infrastructures to research facilities in Africa.[9] After all, a pre-requisite for sustainable collaborations is data transfer avenues, and the EU, and specifically its data protection regime, has a particular role to play in this.

For the EU Member States, data protection requirements are predominantly defined through the GDPR.[10] However, they are also governed by other external sovereignty commitments, for example, through Convention 108 and general privacy protection provisions found in international human rights instruments such as the Universal Declaration of Human Rights (UDHR),[11] International Covenant on Civil and Political Rights (ICCPR),[12] and European Convention for the Protection of Human Rights (ECHR).[13] As will be elaborated later, recently Convention 108 has been revised and the EU has given authorization to its Member States to accede to it. Without doubt, the EU data protection regime is the strictest and most comprehensive across the globe. This high standard is to be granted to data subjects in biobank research when data are being processed in the EU, regardless of whether the data originate from EU data subjects, as well as, for example, when the EU data subjects' data are being transferred to third countries or international organizations. This standard has been externalized through territorial clauses and data transfer provisions set forth in the GDPR.[14] Chapter V GDPR provides for three alternative data sharing avenues (adequacy, appropriate safeguards, and derogations in specific situations). Although appropriate safeguards and derogations can be used for data transfer purposes, previously it was argued that adequacy is the most suitable means for large-scale data and sample sharing,[15] as well as sustainable collaboration and capacity building.[16]

Up to the present (March 2020), the European Commission has adopted 13 adequacy decisions, of which two are partial decisions (regarding Canada and the USA).[17] Additionally, negotiations with South

4 See Deborah Mascalzoni and others, 'Are Requirements to Deposit Data in Research Repositories Compatible with the European Union's General Data Protection Regulation?' (2019) 170 Annals of Internal Medicine 332.

5 Jenna van Draanen and others, 'Assessing Researcher Needs for a Virtual Biobank' (2017) 15 Biopreservation and Biobanking 203.

6 Generally on BBMRI-ERIC, see Jane Reichel and others, 'ERIC: A New Governance Tool for Biobanking' (2014) 22 European Journal of Human Genetics 1055.

7 'ARC Biobank' <https://ibb.iarc.fr> last accessed 2 August 2019.

8 See further Santa Slokenberga, 'Setting the Foundations: Individual Rights, Public Interest, Scientific Research and Biobanking' in Santa Slokenbega, Olga Tzortzatou and Jane Reichel (eds), GDPR and biobanking. Individual rights, public interest and research regulation across Europe (Springer 2020 forthcoming).

9 Santa Slokenberga and others, 'EU Data Transfer Rules and African Legal Realities: Is Data Exchange for Biobank Research Realistic?' (2019) 9(1) International Data Privacy Law 30.

10 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) (2016) OJ L119/1.

11 UDHR (adopted 10 December 1948) UNGA Res 217 A(III).

12 ICCPR (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

13 ECHR and Fundamental Freedoms, as amended by Protocols Nos 11 and 14, 4 November 1950, ETS 5.

14 For challenges relating to extra-territorial application of GDPR, see Benjamin Greze, 'The Extra-territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9(2) International Data Privacy Law 109.

15 Jennifer Stoddart, Benny Chan and Yann Joly, 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research' (2016) 44 The Journal of Law, Medicine & Ethics 143.

16 Slokenberga and others (n 9).

17 Others are Andorra, Argentina, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. See Commission, 'Adequacy Decisions' < https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> last accessed 5 March 2020.

Korea are in progress and additional adequacy procedures are envisaged.[18] None of these decisions has been adopted with respect to countries in Africa. Nevertheless, several states in Africa, both in North Africa and the sub-Saharan region, are signatories to Convention 108. Tunisia has already signed the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Protocol). This will lead to a commitment to comply with the data protection framework of Convention 108+ (a consolidated text of Convention 108 as amended by the Protocol). Other African states that are signatories to Convention 108 can be expected to accede to the Protocol in the near future. Convention 108, as well as foreseeably Convention 108+, not only has a particular importance in the national legal orders of the EU Member States but also for the EU itself, especially concerning adequacy assessment. Therefore, the potential for Convention 108+ to be a means to further adequacy assessment emerges, which could then become the basis for building sustainable data transfer avenues and the development of scientific research. Could Convention 108+ be a tool through which gaps between the data protection standards in the EU Member States and third countries, notably, those in Africa, be overcome?

In light of the foregoing, this contribution examines how, if at all, accession to Convention 108+ can help in reaching an adequacy decision and thus contribute to building sustainable data transfer avenues and facilitate research collaboration in the area of biobanking. It begins by reviewing the ties between the EU and the Council of Europe in the area of data protection. Then, it moves on to scrutinizing the EU adequacy requirements under the GDPR, and thereafter to analysing the extent that Convention 108+ could contribute to furthering an adequacy decision. In this regard, particular focus is placed on African countries that have acceded to Convention 108. It argues that although it can positively contribute to furthering the data protection standard in the respective third countries and international organizations that are or will become its parties, accession to the convention in itself is not sufficient. An adequacy decision is not a decision on the adequacy of the data protection regime *stricto sensu*. It requires adequacy of the legal system in the respective country to be in place and for it to have the capability to uphold the fundamental right to privacy as a key pillar of a democratic legal system where the transparency of a data subject enjoys adequate seclusion not only from other individuals but also from the state, which is far beyond the scope of Convention 108+. Therefore, in addition to raising the data protection bar and furthering biobanking capacity, the necessity to strengthen democratic values, human rights, and rule of law emerges.

Ties between the EU and Council of Europe in the area of data protection

Although the Council of Europe was a pioneer regional legal order in Europe in the way it engaged with the question of data protection, in the last decade its contribution to the field seems to have been somewhat overshadowed by developments in the area of data protection in the EU. However, one could argue that this is merely an illusion. The Council of Europe has not only revised its key treaty in the area of data protection, namely Convention 108, but also a number of other instruments relevant to the area, including recommendations on medical data protection[19] and in the field of biobanking,[20] thus strengthening the general data protection regime and also requirements applicable to scientific research.

Convention 108 has a particular relationship with the EU. This is because the EU data protection regime has its roots in Convention 108. Moreover, all Member States of the EU are parties to Convention 108, and hence through accession to the convention have exercised their external sovereignty in the area in which the EU has also asserted itself by pushing an internal market policy.[21] In these circumstances, already from the very early days of the EU data protection regime it has been in the interests of the EU not to arrive at a situation where the EU Member States are required to comply with conflicting obligations.

One could muse over the reasons for the EU's interest in the modernization of Convention 108. Although the answer is relatively complex and is beyond the scope of this article, by way of illustration a few reasons can be noted. Support for Convention 108 and Convention 108+ and eventual EU accession comes at a relatively low cost and with considerable gains. Unlike accession to the ECHR, accession to Convention 108+ does not bring significant threats to the autonomy of the EU legal

18 Commission, 'Data protection rules as a trust-enabler in the EU and beyond - taking stock' (Communication) COM (2019) 374 final.

19 Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data.

20 Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin.

21 Bruno De Witte, 'Non-market Values in Internal Market Legislation' in Niamh Nic Shuibhne (ed), *Regulating the Internal Market* (Edward Elgar Publishing, Cornwall 2006) 61–86.

order.[22] In terms of status, the Convention Committee that will function under Convention 108+ is comparable to the European Data Protection Board and not the Court of Justice of the European Union (CJEU). However, among the benefits that the EU can gain are the extension of EU-approved standards to other members of the Council of Europe that are not Member States of the EU, as well as non-Council of Europe Member States and international organizations, which is something that the EU would find difficult to achieve alone. Additionally, it is a means of strengthening the Council of Europe, a co-habitant of an overlapping European legal space, and of politically strengthening the region. These reasons also contribute to explaining the role of Convention 108 in the GDPR and are somewhat in line with the long since observed role of mixed agreements as a technique to manage the EU's external relations.[23]

From the EU perspective, the impact of Convention 108+ can be expected to be felt at least in two different situations: first, vis-à-vis the EU Member States; secondly, vis-à-vis the third countries. The impact vis-à-vis the EU Member States can be explained by gaining a brief insight into the mixed agreements. The concept of a mixed agreement requires that the Member States and/or the EU are parties to a certain agreement. Generally, mixed agreements can be concluded when the EU lacks competence to conclude an agreement unilaterally (namely, when the scope of an agreement exceeds the limits of the EU's exclusive powers) or for political purposes the Member States may be asked to join the agreement.[24] Conventions 108 and 108+, both being data protection treaties, fall within the domain of shared competence between the EU and its Member States. All EU Member States are parties to Convention 108 and, except for Denmark, Malta, Romania, and Slovakia, they have all signed the Protocol.[25] Furthermore, the EU has given an authorization to its Member States to proceed with the ratification of the Protocol.[26] Once the EU itself has acceded to Convention 108+, following Article 216.2 TFEU, it will be an integral part of EU law[27] and will be binding upon the EU institutions and the Member States as an EU law.[28] It has well been established in case law that 'in ensuring compliance with commitments arising from an agreement concluded by the [Union] institutions, the Member States fulfil, within the [Union] system, an obligation in relation to the [Union], which has assumed responsibility for the due performance of the agreement'.[29] This means that once the EU accedes to Convention 108+, in so far as EU competence in the area of data protection stretches, the direct relationship between Convention 108+ and the EU Member States ceases to exist. The relationship will remain direct only in so far as a particular question is not a competence of the EU, which explains the importance of aligning Convention 108+ with the GDPR.

Vis-à-vis the third countries, one particular point is essential to emphasize. Article 45(2) GDPR already assigns a particular role to Convention 108 in adequacy assessment, which is only reasonable. If Convention 108 was a basis for developing the Data Protection Directive, then it could be expected that states that have acceded to Convention 108 will have similar elements in their data protection legal frameworks to those in the EU Data Protection Directive. This would also be similar to the GDPR and Convention 108+. If, as discussed further on, the Protocol has been drafted to include core elements of the GDPR, then it can be expected that states that have acceded to the Protocol and become parties to Convention 108+ will have similar elements in their data protection legal frameworks to those in the EU GDPR.

As elaborated in the next section, the GDPR affords a particular role to Convention 108 but not to Convention 108+. Recital 105 states that

> [a]part from the international commitments the third country or international organisation has entered into, the Commission should take account of obligations arising from the third country's or international organisation's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as

22 Compare with the intended EU accession to the ECHR. See Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms, Opinion 2/13, [2014] electronic Reports of Cases (EU:C:2014:2454).

23 Generally on mixed agreements see, for example, Joni Heliskoski, *Mixed Agreements as a Technique for Organizing the International Relations of the European Community and Its Member States* (Martinus Nijhoff Publishers, The Hague 2001).

24 Geert De Baere, *Constitutional Principles of EU External Relations* (OUP, Oxford 2008) 235.

25 Details of Treaty No 223, 'Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223> last accessed 9 December 2019.

26 European Parliament legislative resolution of 12 March 2019 on the draft Council decision authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (10923/2018 – C8-0440/2018 – 2018/0238(NLE)).

27 Case 181-73 *R & V Haegeman v Belgian State* [1974] ECR-00449 (ECLI:EU:C:1974:41) para 5.

28 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/01, art 216.2.

29 Case C-293/03 *My* [2004] ECR I-12013 (ECLI:EU:C:2004:821) para 26.

> the implementation of such obligations. In particular, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol should be taken into account. The Commission should consult the Board when assessing the level of protection in third countries or international organisations.

The importance of Convention 108 was emphasized in a similar way in WP 254. While a likely reason for the omission of Convention 108+ is rather clear, namely that the Protocol was opened for signature on 10 October 2018, more than two years after the adoption of the GDPR, what is less clear is whether and to what extent, given the substantive differences between Conventions 108 and 108+, the former is sufficient in meeting the EU data protection requirements required by the adequacy assessment. This question will be scrutinized in the next section of this article.

Adequacy in context

The place and role of an adequacy mechanism under the GDPR

Under Chapter V GDPR, adequacy is one of the three avenues through which data transfers to third countries or international organizations may take place. The other avenues are appropriate safeguards and derogations applicable in specific situations, among which of particular relevance to the area of biobanking are important reasons of public interest.[30]

An adequacy decision means that the Commission has found that either the third country, a territory, or one or more specified sectors within that third country, or the international organization in question, ensures an adequate level of protection.[31] Existence of an adequacy decision entails the free flow of personal data between the EU and the respective international organization or third country as far as the adequacy decision applies.[32] This free flow, however, is not without limits. First, the Commission holds the authority to decide on adequacy (Article 45(1)), recognizing that a territory or a sector or sectors within the third country or an international organization ensures an adequate level of protection of personal data.[33] However, that very same implementing act shall provide for a mechanism for a periodic review at least every four years and pay due regard to all relevant developments in the third country or international organization.[34] Additionally, the Commission is under the duty to carry out an ongoing monitoring of developments in the third country or international organization that could affect the functioning of the adopted adequacy decisions and, where necessary, repeal, amend, or suspend the respective decision.[35] Moreover, following the *Schrems* case, the Member States are placed in the role of a watchdog of the data transfers based on adequacy decisions and can bring a case to the CJEU if necessary.[36]

For biobankers and researchers, an adequacy decision is a means of building sustainable collaborations and data transfer routes as it offers considerable stability. Of course, in the absence of an adequacy decision other transfer routes are possible although each comes with its limitations.[37] For example, standard contractual clauses generally impose a considerable responsibility on the sender, which is something a biobank or another institution engaging in research might not be willing to assume. Binding corporate rules require the existence of a structure between the sending and recipient organizations, which is something that does not often exist in a research context. Finally, transfers relating to important reasons of public interest generally require that research (and transfers in that regard) are regarded as a public interest nationally or under the EU law.[38] In the event of a transfer based on an adequacy decision, the transfers are relatively straightforward with few obligations placed on the biobanker acting in the capacity of a data exporter. However, although no further authorizations or other formalities are needed,[39] it could be reasonably expected that the biobanker makes sure that the adequacy decision has not been repealed or suspended by the European Commission or invalidated by the CJEU.

For the EU, an adequacy mechanism can be seen as a tool through which to expand international trade and cooperation.[40] Internally, it is a means through which 'legal certainty and uniformity throughout the Union' are provided as regards the respective third country or international organization.[41] Thus far, however, the adequacy mechanism has had a relatively slow uptake. It was established under the Data Protection Directive in

30 GDPR, art 49(1)(d).
31 Ibid, art 45(1).
32 Ibid, art 45(1).
33 Ibid, art 45(3).
34 Ibid, art 45(3). Further rules regarding the implementing act are set forth in this provision.
35 GDPR, art 45(4).
36 Case C-362/14 *Schrems* [2015] electronic Reports of Cases (ECLI:EU:C:2015:650) paras 37–66.
37 Slokenberga and others (n 9).
38 GDPR, Recital 112.
39 Ibid, Recital 103.
40 Ibid, Recital 101.
41 Ibid, Recital 103.

1995 and to date the Commission has arrived at 11 full and two partial adequacy decisions,[42] which on average is one decision a year. Furthermore, talks with South Korea are at an advanced stage.[43] If successful, this could be the first adopted adequacy decision under the GDPR. However, this small number of decisions is the tip of the iceberg in regard to work that has been done in assessing third countries. As Makulilo has highlighted, the European Commission has outsourced studies to review the state of art of data protection in the countries considered for adequacy but these reports have not been made public.[44] Moreover, data about the actual number of countries interested in an adequacy decision are also lacking.

Adequacy decision

An adequacy decision means that the overall level of data protection in the respective third country or international organization wholly or in a specific sector ensures *essentially equivalent* protection to that offered within the EU.[45] Essential equivalence could be argued to entail that substantive rules and procedures are in place to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when data are freely transferred to the third country.[46]

Unlike the Data Protection Directive,[47] the GDPR outlines more specifically the key rules for assessing adequacy. However, as the wording of Article 45(2) GDPR suggests, the list is not exhaustive and other factors could be considered. The requirements set forth in Article 45(2) can be divided into three groups: substantive and procedural rules; oversight; and international commitments. Each will be considered in greater detail. However, at the outset one should be mindful that these criteria in themselves are surrounded by a degree of ambiguity and the GDPR itself is not particularly forthcoming with guidance for their interpretation. Likewise, the actions of the European Commission—by not making available the analysis relating to work done in regard to unsuccessful adequacy assessments—has hardly helped. Therefore, WP 254 Adequacy Referential, which repealed WP 12, (adopted by Article 29 Working Party and is endorsed by the European Data Protection Board with Endorsement 1/2008) is of importance as a source to navigate the EU law requirements relevant for assessing adequacy in third countries and international organizations. Yet, these tools in themselves can neither replace nor provide sufficient understanding of the unpublished detailed rules and procedures for adequacy assessment that are presumably at the disposal of the European Commission.

Adequacy requirements

Substantive and procedural rules

Article 45(2)(a) GDPR requires the Commission to take into account a long list of requirements:

> the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.

The rule of law and respect for human rights and fundamental freedoms are fundamentals of the EU and held up as common values of all EU Member States. While for assessing human rights and fundamental freedoms EU primary law, namely, the CFREU and the importance of the ECHR in the EU legal order is of help,[48] this is not the case with the content of the rule of law. Even though the Treaties refer to the rule of law, it has neither been defined nor exhaustively explained by the CJEU. In doctrine this principle has appeared in multiple forms, and they 'may comprise the lawfulness of public administration, legal security, legal certainty, and protection of legitimate expectations, non-retroactive effect of penal laws, and the principle of

42 Commission (n 17).

43 Commissioner Jurová's intervention at the event 'The General Data Protection Regulation One Year On: Taking Stock in the EU and Beyond' <http://europa.eu/rapid/press-release_SPEECH-19-2999_en.htm> last accessed 2 August 2019.

44 Alex Boniface Makulilo, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3 International Data Privacy Law 42.

45 GDPR, Recital 104.

46 Ibid, art 44; Article 29 Working Party, 'Working document on Adequacy Referential' (wp254rev.01, 6 February 2018), ch 1.

47 A mechanism that was needed to be 'rationalized'. See Paul Roth, '"Adequate Level of Data Protection" in Third Countries Post-Schrems and under the General Data Protection Regulation' (2017) 25 Journal of Law, Information & Science 49. See also Peter Johan Hustinx, 'Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive' (24 July 1998) European Commission, Working Paper No DG XV D/5025/98 WP 12, ch 6.

48 See Article 29 Working Party (n 46) ch 1; Consolidated version of the Treaty on European Union, 13 December 2007, 2008/C 115/01, art 6.

proportionality'.[49] In case law, it has been found that the expression of rule of law includes such dimensions as the principle of legality,[50] legal certainty, particularly, that the law is clear and precise and that its application be foreseeable for all interested parties,[51] as well as compliance with the law.[52] Additionally, measures against the misuse of power are of importance, including that 'individuals have the right to challenge before the courts the legality of any decision or other national measure concerning the application to them of an EU act'.[53] Furthermore, in the context of the EU it includes that the 'institutions are subject to review of the conformity of their acts with the treaties and the general principles of law'.[54]

Article 45(2) requires the Commission to consider 'both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation'. In this regard, WP 29 has pointed out that '[a]ttention must also be paid to the legal framework for the access of public authorities to personal data.'[55] WP 237, the Essential Guarantees document, pins down the following European essential guarantees: first, that processing should be based on clear, precise, and accessible rules; secondly, that the principles of necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated; thirdly, that an independent oversight mechanism should exist; and fourthly, that effective remedies need to be available to the individual.[56] These requirements are in line with the EU take on data protection as a tool for upholding democracy. Whether and to what extent there is flexibility in this area may be clarified in the *Schrems II* case,[57] Part II of the saga involving Facebook data transfers and Mr Maximillian Schrems.

Article 45(2)(a) requires considering the 'data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred'. Furthermore, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred should be ensured.

It has been well established that the general provisions regarding privacy and data protection imposed on third countries are not sufficient in meeting the EU law requirements.[58] Specific and enforceable provisions that address 'concrete needs for practically relevant aspects of the right to data protection must be included in the third country's or international organisation's legal framework'.[59] However, even this guidance does not in itself explain what these needs are and how specific the provisions should be. These requirements are further delineated in WP 254 which states that '[a] third country's or international organisation's system must contain a number of basic content and procedural/enforcement data protection principles and mechanisms.'[60] These have been categorized in three groups: content principles; additional content principles; and principles applicable in particular situations.

The group content principles cover the following. The first is concepts. It is expected that basic data protection concepts and/or principles are set forth in the national law. Although these should exist, 'they do not have to mirror the GDPR terminology but should reflect and be consistent with the concepts enshrined in the European data protection law'. The second is grounds for lawful and fair processing for legitimate purposes. In this regard, 'legitimate bases, under which personal data may be lawfully, fairly and legitimately

49 Rdolf Geiger, 'Article 2 [Common Values]' in Rudolf Geiger, Daniel-Erasmus Khan and Markus Kotzur (eds), *European Union Treaties* (C.H. Beck/Hart, Munich / Oxford 2015) 15–17.

50 See, for example, Case 294/83 *Les Verts v Parliament*, [1986] Reports of Cases 01339 (ECLI:EU:C:1986:166) para 23; Case C-496/99 P *Commission v CAS Succhi di Frutta* [2004] Reports of Cases I-03801, para 63.

51 C-585/13 P *Europäisch-Iranische Handelsbank v Council* [2015] electronic Reports of Cases (ECLI:EU:C:2015:145), para 93.

52 Joined Cases 212 to 217/80 *Meridionale Industria Salumi and Others* [1981] Reports of Cases 02735 (ECLI:EU:C:1981:270) para 10.

53 Case C-619/18 *Commission v Poland (Indépendance de la Cour suprême)* [2019] (ECLI:EU:C:2019:615) para 46 (not yet published).

54 Case C-355/04 P *Segi and Others v Council* [2007] Reports of Cases I-01657 (ECLI:EU:C:2007:116) para. 51.

55 Article 29 Working Party (n 46) 4.

56 Article 29 Working Party, 'Working Document 01/2016 on the Justification of Interferences with the Fundamental Rights to Privacy and Data Protection Through Surveillance Measures When Transferring Personal Data (European Essential Guarantees)' (13 April 2016) WP 237, 6.

57 CJEU, Case C-311/18 *Reference for a Preliminary Ruling from the High Court (Ireland) Made on 9 May 2018 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* <http://curia.europa.eu/juris/document/document.jsf?text=&docid=204046&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=5320248> last accessed 2 August 2019. As one may infer from the opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, these requirements apply in so far as the scope of GDPR is triggered by activity in question. See Opinion of Advocate General Saugmandsgaard Øe delivered on 19 December 2019, Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (2019) (ECLI:EU:C:2019:1145) paras 201–230.

58 Article 29 Working Party (n 46) 4.

59 Ibid.

60 Ibid 5.

processed, should be set out in a sufficiently clear manner'.[61] The third is the purpose limitation principle. The fourth is the data quality and proportionality principle.[62] The fifth is the data retention principle.[63] The sixth is the security and confidentiality principle.[64] The seventh is the transparency principle, which requires that individuals be informed of all the main elements of the processing of their personal data in a clear, easily accessible, concise, transparent, and intelligible form.[65] However, it is acceptable that some exceptions to this right for information in particular circumstances can exist, for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings, or other important objectives of general public interest as is the case with Article 23 of the GDPR.[66] The eighth is the right of access, rectification, erasure, and objection, which could in some situations be restricted.[67] The ninth is restrictions on onward transfers. This means that onward transfers should not be permitted unless the recipient affords an adequate level of protection of personal data in the respective country or international organization. In the event of transfer, '[t]he initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing.'[68]

The additional content principles are expected to be applied to specific types of processing. WP 254 points at three situations. First, regarding the protection of special categories of personal data and requiring special safeguards when these data are processed. In that regard, the categories addressed in Articles 9 and 10 GDPR are of particular importance.[69] Secondly, in case it is permissible to process personal data for the purposes of direct marketing, the data subject shall be given a right to object to such a processing free of charge at any time.[70] Thirdly, where automated decision-making and profiling occurs, it 'can take place only under certain conditions established in the third country legal framework'. In such a case, the law should provide for necessary safeguards to the data subject.[71]

Oversight

An independent supervisory authority is a key element of the fundamental right to data protection as set forth in Article 8 CFREU. As derived from Article 45(2)(b) GDPR, in assessing adequacy not only the existence of this authority is crucial but also that it is effective in monitoring and enforcing data protection requirements.[72] Effectiveness could be furthered not only through equipping the authority with adequate resources but also through operationalizing the principle of accountability[73] and raising awareness among data controllers and those processing personal data on their behalf of their obligations, tasks and responsibilities, and among data subjects of their rights and the means of exercising them. Additionally, as emphasized in WP 254, sanctions and other compliance mechanisms could play an important role in ensuring respect for the data protection rules.[74] Furthermore, the data protection system must provide support to individual data subjects in the exercise of their rights as well as offer appropriate redress mechanisms. This requirement strongly relates to the effective enforcement of the data subject's rights in regard to which an independent investigation of complaints and punishment of violations is of particular importance.[75]

International commitments

Finally, as derived from Article 45(2)(c) GDPR, account should be taken of 'the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data'. In this regard, Recital 105 guides the Commission on the international commitments the third country or international organization has entered into, the obligations arising from participation in multilateral or regional systems, in particular in relation to

61 Ibid.
62 Ibid.
63 Ibid.
64 Ibid.
65 Ibid 6.
66 Ibid.
67 Ibid.
68 Ibid.
69 Ibid.
70 Ibid 7.
71 Ibid.
72 Art 45(2)(b) GDPR requires account to be taken of the 'existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States'.
73 Article 29 Working Party (n 46) 7 and 8.
74 Ibid 7.
75 Ibid 8.

the protection of personal data, as well as the implementation of such obligations. As previously noted, in this regard Convention 108 is of importance.[76] However, given the significant changes that the Protocol introduces in bringing Convention 108 in line with the GDPR and the high requirements set forth in Article 45(2) GDPR, it is rather unlikely that Convention 108 alone will be sufficient in meeting the respective requirements. However, it may well be possible for a state that has not acceded to the Protocol but has revised its internal legal system to meet the adequacy requirements.

Adequacy requirements and Convention 108+

Through the Protocol, upon its entry into force,[77] Convention 108 will become Convention 108+. The slight change to the short title of the convention in fact represents considerable revisions undertaken by the Council of Europe with a view to responding to the challenges that advances in technology have brought and to ensure effective enforcement of its requirements. The amendments[78] inter alia have reshaped the preamble of the convention through anchoring data protection rules in human dignity[79] and reaffirmed the previously existing aspiration for securing the protection of the human rights and fundamental freedoms of every individual.[80] They also emphasize that the right to data protection shall be reconciled with other human rights and fundamental freedoms,[81] acknowledge the importance of access to public documents,[82] and stress the importance of promoting at the global level the fundamental values of respect for privacy and protection of personal data[83] and the need for cooperation between the parties of the convention.[84] In that way, the preamble introduces the convention as an ambitious data protection tool with aspirations for a global impact.

Substantively, key novelties include the following. The objective and purpose of the convention have been clarified (Article 1) by placing emphasis on the protection of every individual with regard to processing of their personal data. The amendments bring changes in the definitions of the convention (Article 2), inter alia reshaping the focus from 'automatic processing' to 'processing' of personal data. They also introduce the concepts of 'recipient' and 'processor'. Furthermore, through the amendments (Article 3), the scope of application of the convention is clarified so that the contracting parties are deprived of the possibility of excluding certain types of processing from the scope of application of the convention. Now, the convention can be rendered inapplicable only 'to data processing carried out by an individual in the course of purely personal or household activities'.

The amendments add nuance to and strengthen the duties of the contracting parties (Article 4) by requiring them to take measures in their 'law' (previously 'domestic law') by the time of ratification or accession and to commit themselves to permitting and engaging in the evaluation of the effectiveness of these national measures. They also clarify and expand the rules relating to the legitimacy of data processing and quality of data (Article 5), including aligning the article with those data protection principles set forth in the GDPR. Notably, however, the principle of accountability is not enshrined by Article 5 but by the 'additional obligations' included in Article 10. Additionally, this provision includes rules relating to the legal basis for the processing of personal data. Furthermore, the amendments reaffirm the importance of a specific approach to special categories of personal data and set out conditions under which they can be processed (Article 6). In alignment with the GDPR, the convention now contains several new categories, including those of biometric data and genetic data, the latter of which is crucial to ensure a high level of data protection in biobanking.

The amended convention reaffirms the data security requirement (Article 7) and in alignment with the GDPR, it requires that its signatories adopt provisions that oblige controllers to notify the competent authority regarding 'those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects'. It expressly delineates the content of the principle of transparency (Article 8), which strongly relates to the data subject's right to information under Articles 13 and 14 of the GDPR and largely contains similar obligations and freedoms to the controllers. The previous 'additional safeguards for the data subject'

76 GDPR, Recital 105.

77 See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 223, art 37.1.

78 See a full comparison between the texts, 'Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108)' <https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958> last accessed 2 August 2019.

79 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 223, Preamble, para 3.

80 Ibid, Preamble, para 2. Compare with Convention 108 (n 78) Preamble, para 2.

81 ETS 223 (n 79) Preamble, para 4.

82 Ibid, Preamble, para 5.

83 Ibid, Preamble, para 6.

84 Ibid, Preamble, para 7.

have now become 'rights of the data subject' (Article 9). This provision now contains rights that in essence correspond to those enshrined in Chapter III of the GDPR. Additionally, this provision includes a right to remedy, which is a fundamental component of the GDPR that is located in Chapter VIII of the regulation.

The principle of accountability, along with such fundamental elements found in Chapter IV of the GDPR as general obligations of the controller and processor, data security, and impact assessment requirements, now have a place in Article 10 of Convention 108+. The amendments also include revisions of the exceptions and restrictions, which inter alia expand the list of situations when the provisions of the convention can be restricted, and set out the notion of 'general public interest', which in many ways is operationalized similarly to the 'general public interest' under Article 23 of the GDPR (Article 11). Rules relating to sanctions and remedies now place an emphasis on 'judicial and non-judicial' means and apply to the violation of provisions of the convention as opposed to one chapter of the convention as previously (Article 12). In exactly the same way as previously, the convention enables contracting parties to grant 'a wider measure of protection' than that which is set by the convention, thus affirming its *de minimis* character (Article 13).

The rules relating to the transborder flow of personal data (Article 14) apply to transfers within the constellation created by the treaty signatories, as well as between the signatories of the convention and third parties. The convention slightly rephrases the principle of free movement of data among the signatories and defines limitations to free movement when there is 'a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention', as well as if so required by another international organization to which a signatory is a member. In regard to third countries, it sets out the requirement that 'an appropriate level of protection based on the provisions of this Convention is secured', and provides for two alternative avenues through which this appropriate level of protection can be secured: first, 'the law of that State or international organisation', including international treaties; secondly, 'ad hoc or approved standardised safeguards [which are delineated in Article 15] provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing'. In the same way as the GDPR, it also allows transfers in exceptional situations. Unlike Article 49 GDPR, Article 15 of the convention (similar to Article 2 of the Additional Protocol of Convention 108)[85] does not seem to be phrased in terms of a last resort when the appropriate level requirement is not met. Instead, it is presented as an alternative data transfer legal avenue. These requirements to a considerable degree resemble Article 49 GDPR and include such essential provisions in the context of scientific research as 'important public interest' if so provided by national law (in comparison, the wording of Article 49 is 'important reasons of public interest'). Finally, it introduces the principle of exporter's responsibility, mandating provision of information to the supervisory authority and requiring that the person who transfers personal data 'demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests', and when necessary, the authority may 'prohibit such transfers, suspend them or subject them to conditions'.

For effective operationalization of the provisions of the convention, the role of the supervisory authorities has been strengthened and the catalogue of their powers that was previously listed in Article 1 of the additional protocol to Convention 108 has now been expanded (Article 15). The exercise of these powers, however, is limited in scope as it expressly excludes acting in regard to 'processing carried out by bodies when acting in their judicial capacity'. The supervisory authorities are competent to approve the standardized safeguards and have the authority to deal with data subject requests and complaints (including providing assistance as regulated under Article 18) unless it may refuse them (Article 20), declare violations of the convention, and impose sanctions. The decisions taken by supervisory authorities 'may be subject to appeal through the courts'. The authorities are also required to promote awareness of privacy and pay due regard to the protection of the rights of the vulnerable. In exercising their tasks, 'complete independence and impartiality' is required, and neither should they 'seek nor accept instructions'.

In regard to enabling the supervisory authorities to fulfil their tasks, the signatories are required to ensure that the competent authorities have the necessary resources. The members and staff of the authority are required to be bound by confidentiality, and the authority is required to be transparent about its activities by means of preparing and publishing a periodical report on the issue. The parties are under an obligation to cooperate and mutually assist to implement the convention, as well as to inform the Secretary General of the

85 Chart of Signatures and Ratifications of Treaty 181, 'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows' ETS 181 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=Eum0VGYi> last accessed 2 August 2019.

Council of Europe of the competent national supervisory authority or authorities (Article 16). The supervisory authorities shall form a network and 'co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers' (Article 17). In order to limit the risks of misuse of information, purpose specification vis-à-vis the supervisory authorities is an *expressis verbis* obligation of the convention, as is their ability to make a request on behalf of a data subject (Article 19). Furthermore, actions of the supervisory authorities in fulfilling their tasks shall be free of charge. In regard to other details of co-operation and procedures, the parties concerned should agree on the practicalities (Article 21).

Finally, the Consultative Committee of Convention 108 becomes the Convention Committee and its role and powers are strengthened inter alia by assigning to it assessment and monitoring powers and specific duties in the case of data transfers (Articles 22–24). Similar to Convention 108, under Convention 108+ neither an enforcement body such as the ECtHR is envisaged, nor is any interpretive authority assigned to the ECtHR. However, another similarity is that, in so far as a matter concerns privacy and a signatory of the ECHR, it is likely to be framed in terms of privacy and so have the potential to be brought before the ECtHR.

It is more than obvious that Convention 108+ bears considerable similarities to the GDPR, which could be said to relate to what the Commission itself has labelled the 'significant contribution from the Commission' in modernizing the convention.[86] However, there are differences between the two instruments. For example, Convention 108+ does not exclude matters of national security; the GDPR is more precise and stringent on the detail, whereas Convention 108+ leaves some room for its signatories to determine how it will be operationalized. While vis-à-vis the EU Member States it will be operationalized through the GDPR, third countries will decide this for themselves. There is a risk, albeit minimized through the Convention 108+ provisions,[87] that the operationalization provisions are considered too weak to ensure effective implementation of Convention 108+.

Adequacy and data protection insights in Cape Verde, Mauritius, Morocco, Senegal, and Tunisia, Conventions 108 and 108+

In the absence of transparency on the part of the Commission in how various adequacy criteria interplay, as well as the varying discretion allowed to different third countries,[88] it is impossible to conduct a comprehensive adequacy exercise. However, this does not prevent highlighting some areas of concern that those states in Africa that are parties to Convention 108 and are expected to become parties to Convention 108+ could face on their path towards adequacy.

First of all, even though Cape Verde, Mauritius, Morocco, Senegal, and Tunisia have acceded to Convention 108[89] (and its Protocol),[90] and Tunisia is the first of these states to sign the Protocol,[91] there are considerable differences in the data protection standard and how that has been operationalized in these countries. For example, data protection laws have been adopted at different times, in some instances leading to an outdated regulatory framework or one that has already been scrutinized vis-à-vis adequacy and found to be inadequate. For example, the Data Protection Act of Cape Verde is from 2001,[92] the Mauritius Data Protection Act from 2017,[93] and the law of Morocco from 2009 (Law n° 09-08 of 18 February 2009 and its Implementation Decree n° 2-09-165 of 21 May 2009).[94] These did not meet the adequacy requirements.[95]

86 Commission (n 18) 11.

87 Art 4.2 of Convention 108+ states '[t]hese measures shall be taken by each Party and shall have come into force by the time of ratification or of accession to this Convention.'

88 See Stoddart, Chan and Joly (n 15).

89 Chart of Signatures and Ratifications of Treaty 108, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=FFPPsnwj> last accessed 2 August 2019.

90 Chart of Signatures and Ratifications of Treaty 181 (n 85).

91 Chart of Signatures and Ratifications of Treaty 223, 'Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures?p_auth=FFPPsnwj> last accessed 2 August 2019.

92 The Republic of Cape Verde, Data Protection Act, Law 133/V/2001 of 22 January <http://www.cnpd.cv/leis/DATA%20PROTECTION%20Law%20133.pdf> last accessed 2 August 2019. For detailed insights in the Act at the time of adoption, see João Luis Traça and Bernardo Embry, 'An Overview of the Legal Regime for Data Protection in Cape Verde' (2011) 1(4) International Data Privacy Law 249.

93 Mauritius, The Data Protection Act 2017, Act No 20 of 2017 <http://mauritiusassembly.govmu.org/English/acts/Documents/2017/act2017.pdf> last accessed 2 August 2019.

94 Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel <https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf> accessed 2 August 2019. Décret N° 2-09-165 du 25 joumada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel <https://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf> last accessed 2 August 2019.

95 See Makulilo (n 44).

Senegal's law is from 2008,[96] and Tunisia has had a Data Protection Act since 2004,[97] which also did not meet the adequacy requirements.[98] Even though in 2018 a new bill was drafted with a view to taking a step closer to the GDPR provisions, this bill has not yet been passed into law.[99] In contrast, even though the Data Protection Act of Cape Verde is from 2001, the Act contains a number of similarities with the GDPR, and the Mauritius Data Protection Act of 2017 bears considerable similarities regarding data protection requirements with the GDPR.

The five states of interest have assumed some regional commitments that are of relevance to the area of data protection. Cape Verde and Senegal are members of the Economic Community of West African States (ECOWAS) has a Supplementary Act A/SA.1/01/10 on Personal Data Protection from 2010. This act requires its Member States to enact legislation for the regulation of personal data 'collection, processing, transmission, storage and use', and is directly applicable in the ECOWAS Member States.[100] Substantively, it is strongly influenced by the Data Protection Directive,[101] and hence national laws that follow the Supplementary Act bear similarities with the previous EU data protection framework. At the same time, considerable differences emerge between the data protection frameworks of Senegal and Cape Verde. On the other hand, states such as Mauritius, Morocco, and Tunisia do not have comparable external data protection obligations. Furthermore, the overall situation regarding surveillance is of importance as is awareness of the privacy rights, which appear to have been a challenge in some states. For example, previously in the literature it was highlighted that in Morocco[102] and Senegal,[103] surveillance was a concern, and in Tunisia, censorship existed.[104] Likewise, in different states awareness of privacy rights has differed. While awareness has been reported in Senegal,[105] scholars have noted that 'citizens are not yet fully aware of the full scope of their own sense of privacy' in Cape Verde.[106]

Lastly, some comments need to be made on the question of democracy, rule of law, and human rights. In this regard, a number of differences and complexities emerge. Even though the African Union is established to further the protection of human rights in the area, and Cape Verde, Mauritius, Senegal, and Tunisia are parties to it, Morocco withdrew in 1985.[107] Furthermore, only Mauritius, Senegal, and Tunisia have acceded to the Protocol and have agreed to the review of the Court,[108] and hence only they can be held accountable by a judicial body for the non-observation of the human rights standard in their national legal orders. Internally and externally, the African states of interest have different democracy incentives, and here the trade relations with the EU have some role to play. In states that follow a monist tradition, international commitments can be seen as a considerable step in strengthening human rights, as is the case of Senegal, for example.[109] In Tunisia[110] and Morocco,[111] democratization features have emerged through trade despite the authoritarian regimes that exist in the states.[112] This can be contrasted with, for example, Cape Verde,[113]

96 Senegal, Data Protection Act (Law 2008-12, 25 January 2008) and Decree on the Application of the Data Protection Act (2008-721, 30 June 2008).

97 Loi organique numéro 63 en date du 27 juillet 2004 portant sur la protection des données à caractère personnel <http://www.inpdp.nat.tn/ressources/loi_2004.pdf> last accessed 2 August 2019.

98 See Alex B Makulilo, 'Data Protection in North Africa: Tunisia and Morocco' in Alex B Makulilo (ed), *African Data Privacy Laws* (Springer International Publishing, Cham 2016).

99 INPDP <http://www.inpdp.nat.tn/textes.xhtml> last accessed 9 December 2019.

100 Supplementary Act A1SA.1f01f10 on Personal Data Protection within ECOWAS, art 48. Lukman Adebisi Abdulrauf and Abdulrazaq Adelodun Daibu, 'New Technologies and the Right to Privacy in Nigeria: Evaluating the Tension Between Traditional and Modern Conceptions' (2016) 7 Journal Home 123.

101 Graham Greenleaf , 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108' (2012) 2 International Data Privacy Law 68, 81.

102 Makulilo (n 98).

103 Patricia Boshe, 'Protection of Personal Data in Senegal' in Alex B Makulilo (ed), *African Data Privacy Laws* (Springer International Publishing, Cham 2016).

104 Makulilo (n 98) 30.

105 Boshe (n 103) 261.

106 João Luís Traça and Pedro Marques Gaspar, 'Data Protection in Cape Verde: An Analysis of the State of the Art' in Alex B Makulilo (ed), *African Data Privacy Laws* (Springer International Publishing 2016) 250.

107 'List of Countries Which Have Signed, Ratified/Acceded to the African Charter on Human and People's Rights' <https://au.int/sites/default/files/treaties/36390-sl-african_charter_on_human_and_peoples_rights_2.pdf> last accessed 2 August 2019.

108 'List of Countries Which Have Signed, Ratified/Acceded to the Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights' <https://au.int/sites/default/files/treaties/36393-sl-protocol_to_the_african_charter_on_human_and_peoplesrights_on_the_estab.pdf> last accessed 2 August 2019.

109 Boshe (n 103) 264.

110 See Makulilo (n 98) 30.

111 See Vera Van Hüllen, 'Europeanisation Through Cooperation? EU Democracy Promotion in Morocco and Tunisia' (2012) 35 West European Politics 117; Makulilo, ibid 35–38.

112 Jonathan N.C. Hill, 'Authoritarian Resilience and Regime Cohesion in Morocco after the Arab Spring' (2019) 55 Middle Eastern Studies 276; Merouan Mekouar, 'Police Collapse in Authoritarian Regimes: Lessons from Tunisia' (2017) 40 Studies in Conflict & Terrorism 857.

113 Bruce Baker, 'Cape Verde: The Most Democratic Nation in Africa?' (2006) 44(4) The Journal of Modern African Studies 493.

Mauritius,[114] and Senegal where a democratic style of governance exists.[115]

Concluding analysis

The overall aim of this contribution is to examine to what extent, if at all, Convention 108+ could help in achieving an adequacy level in third countries and thus serve as a basis for building sustainable data transfer avenues and facilitate research collaboration in the area of biobanking.

As the analysis shows, the EU has a considerable interest in Convention 108+ and in this convention being in line with EU law. It also shares the same interest the Council of Europe has expressly acknowledged, namely, to globalize Convention 108+ and increase global alignment of the data protection standard. Whether and to what extent this can be done remains to be seen. Although it could bring a number of benefits, it would also bring challenges. These challenges relate to the stringency of the requirements set forth in Convention 108+ and the limited leeway for the signatories, and could be interpreted as the loss of regulatory autonomy on the part of the respective third countries that are considering accession.

It has been argued that an adequacy assessment is not about data protection *stricto sensu* but data protection *lato sensu*. It covers not only the detailed requirements of personal data protection, including what is protected and how this protection is ensured, but also the overall legal system in which this data protection framework functions. Therefore, although Convention 108+ has considerable similarities with the GDPR and contains key elements as outlined in WP 254, it is in itself insufficient to lead a third country or international organization to adequacy. This convention not only needs to be effectively operationalized but also operationalized in an environment that is capable of effectively upholding a fundamental right to personal data protection. First, this should be done nationally. Secondly, it is desirable that it is also done regionally if that is possible.

In this regard, a distinction can be drawn between the third countries that are members of the Council of Europe and those that are not. Within the Council of Europe, rule of law and human rights have been of a particular importance. All Council of Europe Member States are signatories to the ECHR, and these states have assumed a commitment to ensure the protection of human rights in their legal orders. Ultimately, it is the ECtHR that can hold states responsible in case the protection has not been ensured in a particular case. Furthermore, thus far the ECHR has shown considerable engagement in accommodating data protection rules under Article 8 ECHR, which protects privacy. This can be contrasted with the approach possible under the Banjul Charter, which in itself does not contain a privacy provision. In 2014, the African Union adopted the Convention on Cybersecurity and Personal Data Protection. However, this convention is not in force yet.[116] Furthermore, only Mauritius and Senegal have taken steps to ratify the convention, Tunisia has signed it, whereas neither Cape Verde nor Morocco has done so.[117] Arguably, this difference also emerged in the recent communication from the Commission regarding data protection rules, where the Commission foresaw adequacy expansion within the European region as well as some other areas but did not mention Africa.[118] Nonetheless, the African Union is among the organizations with which the Commission intends to step up its dialogue in the area of data protection,[119] thus implicitly indicating at the importance of the regional legal orders in furthering data protection as a right and mechanism to uphold this right.

Upholding data protection is not only a question of human rights and specific data protection provisions. It is also an issue of democracy. Democracy of the respective countries, as far as their external commitments are concerned, could be further developed. For example, among the states of interest to this article, the African Charter on Democracy, Elections and Governance is relevant for strengthening the rule of law, but it has only been signed by Cape Verde, Mauritius, Senegal, and Tunisia and not ratified. Morocco has not even signed the treaty.[120] Hence, the regional potential to strengthen democracy has not been fully utilized.

114 Sheila Bunwaree, 'The Democratic Deficits of Mauritius—Development and Justice Threatened' in Said Adejumobi (ed), *National Democratic Reforms in Africa: Changes and Challenges* (Palgrave Macmillan, New York 2015).

115 Ashley M Fent, 'Dreams of Eco-dictatorship: Senegalese Democracy in the Age of Environmental Crisis' (2018) 40 Ufahamu: A Journal of African Studies 109.

116 'List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection' <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> last accessed 2 August 2019.

117 'List of Countries Which Have Signed, Ratified/Acceded to the African Charter on Democracy, Elections and Governance' <https://au.int/sites/default/files/treaties/36384-sl-AFRICAN%20CHARTER%20ON%20DEMOCRACY%2C%20ELECTIONS%20AND%20GOVERNANCE.PDF> accessed 2 August 2019.

118 Commission (n 18).

119 Ibid 11.

120 African Charter on Democracy, Elections and Governance, 'List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection' <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf> last accessed 2 August 2019.

If doubts exist about the state's capability to uphold the fundamental right to privacy as a key pillar of a democratic legal system where transparency of a data subject enjoys a solid state of separateness not only from other individuals but also from the state, it could be rather difficult to grant the EU data subjects those rights as set forth in the GDPR in the third country. To overcome this challenge, the efforts then, in addition to raising the data protection bar and strengthening biobanking in Cape Verde, Mauritius, Morocco, Senegal, and Tunisia, should go further and strengthen democracy, human rights, and rule of law. Another question is whether and to what extent these states would be willing to accept such activities and how effective they could be. Convention 108+ will only be capable of serving as a means to strengthen data protection but not of filling in the remaining gaps. At the same time, for the European Commission the ambiguity regarding the interplay of different adequacy criteria will remain an excellent veil behind which it can hide the actual reasons for not granting adequacy to those states that might have difficulties in having a system in place that is capable of upholding a fundamental right to data protection. On a different note, if scientific research and capacity building is a true EU interest, one might need to start discussing the need for partial adequacy in some areas of scientific research, at least in the fields heavily regulated by soft law, such as biobanking.

doi:10.1093/idpl/ipaa006
Advance Access Publication 27 May 2020