Article forthcoming in *Law, Innovation and Technology* 15(2), 2023.

Protecting the Data of African Agricultural Producers: A Review of National Laws, Compliance and Perceptions

Bezawit Beyene Chichaibelu*, Heike Baumüller and Marie Antoinette Matschuck
Center for Development Research, University of Bonn, Bonn, Germany

Abstract

With the rapid spread of digital tools that collect large amounts of data from agricultural producers across Africa, there is a growing need to strike a balance between data protection and use. To inform this debate, this article examines the level of and demand for the protection of data collected from African producers. To this end, the article presents a review of national personal data protection laws in Africa and assesses compliance of digital agricultural service providers with these laws. It also offers a first insight into perceptions on personal data protection among African agricultural producers. The analysis shows that data privacy regulations in Africa have been evolving, but several countries have yet to adopt related legislation. Existing laws generally reflect the basic elements of the 2014 African Union Convention on personal data protection, but often fall short on provisions of particular importance to digital service provision. Compliance with national data privacy laws among digital agricultural service providers is limited, highlighting enforcement challenges. Awareness of data protection issues is low among agricultural producers, as is the ability to control access to their data.

* corresponding author, bchichai@uni-bonn.de

1 Introduction

Digital agricultural solutions[1] are increasingly being used across Africa to offer services to producers, including advisory, marketing and financial services. In 2020, the GSM Association counted 437 such services in Sub-Saharan Africa, primarily offering advice and financial services to their users.[2] Advances in digital devices, such as smartphones, sensors or satellites, connected through the so-called Internet of things and combined with big data analytics are making it possible to collect and analyse large amounts of agricultural data.[3] According to the EU Code of Conduct on Agricultural Data Sharing by Contractual Agreement (2018),[4] agricultural data includes, among others, 'livestock and fish data, land and agronomic data, climate data, machine data, financial data and compliance data' (p.3). This article focuses specifically on farm-related agricultural data (or farm data), i.e. data related to the farmer, the farming site and operations, and commercial transactions related to the farm. These data can be collected by the farmers themselves, by external data collectors or by data collection devices, such as sensors or cameras. Farm data can be used to improve service provision for agricultural producers, for instance through targeted advice for farmers adapted to their specific context.

Concerns have been raised that in the absence of effective data protection frameworks and safeguards, farm data collected by digital service providers could be used by the providers or other third parties for their own benefit without the knowledge and consent and sometimes to the disadvantage of agricultural producers. Lack of data protection may also hinder uptake of digital solutions if producers do not want to entrust the service providers with their data.[5] Thus, to take full advantage of the opportunities offered by digital technologies in agriculture, it will be key to strike a balance between data use and data protection.

The protection of farm data warrants particular attention for a number of reasons. First, farm data protection is a complex issue that stands at the intersection of different regulatory frameworks, i.e. personal data protection laws, contract and competition laws, and intellectual property rights. However, none of these regulatory frameworks currently provide sufficient protection for farm data and many aspects of their application to farm data remains

[1] According to Tsan et al., digital agricultural solutions (or services) can be defined as 'the use of digital technologies, data and business model innovations to transform practices across the agricultural value chain and address bottlenecks in, inter alia, agricultural productivity, postharvest handling, market access, finance and supply chain management'. Michael Tsan, Swetha Totapally, Michael Hailu and Benjamin K Addom, *The Digitalisation of African Agriculture Report 2018-2019* (CTA - Technical Centre for Agricultural and Rural Cooperation 2019)

[2] GSMA, *Digital Agriculture Maps* (GSM Association 2020)

[3] Heike Baumüller and Muhammadou M.O. Kah, 'Going digital: Harnessing the power of emerging technologies for the transformation of Southern African agriculture' in Richard A. Sikora, Eugene R. Terry, Paul L.G. Vlek, and Joyce Chitja (Eds.), *Transforming Agriculture in Southern Africa: Constraints, Technologies, Policies and Processes* (Routledge 2020)

[4] COPA-COGECA and others. *EU code of conduct on agricultural data sharing by contractual agreement* (Copa-Cogeca, CEMA, Fertilizers Europe, CEETTAR, CEJA, ECPA, FEFAC, ESA 2018)

[5] Marie-Agnes Jouanjean, Francesca Casalini, Leanne Wiseman and Emily Gray, *Issues around data governance in the digital transformation of agriculture – the farmers' perspective* (Organisation for Economic Co-operation and Development 2020)

unclear.[6] For instance from a legal perspective, the distinction between personal[7] and non-personal data, and therefore the scope of applicability of personal data protection laws, is particularly difficult to determine in the case of farm data.[8] Second, a legal debate remains to be resolved regarding the most appropriate legal framework to govern collection and use of machine or sensor-generated agricultural data (e.g. data on soil moisture content collected by sensors in the field). Machine or sensor-generated agricultural data are generally considered non-personal data and fall outside of personal data protection laws. Therefore, the access and use rights to data are negotiated between stakeholders in bilateral contracts and fairness of the negotiated claims to the data largely rests on market forces and bargaining power.[9] Third, from an ethical perspective, where digital applications that rely on farm data to provide advice to farmers are being controlled by large companies that also provide the services, technological farm supplies and inputs that farmers need to put the recommendations into practice, there is a risk of anti-competitive practices and manipulation of market outcomes.

African regulators have not yet responded to the specific challenges associated with farm (and agricultural) data protection. There are no regulations for the protection of farm data nor do related regulations e.g. on personal data protection, include specific provisions for agricultural data. In addition to laws and regulations, data licensing agreements and contracts can be used to govern the relationship between agricultural producers, the digital service providers and affiliated companies. However, there are no legal frameworks in Africa that ensures the fairness of the terms of use in data licensing agreements and contracts. To set common standards for agricultural data licensing contracts and address producers' concern in sharing their data, voluntary codes of conduct have recently been introduced in the EU and a few industrialized countries, but it is yet to be seen if these voluntary codes of conduct are having the desired effect.[10] No such codes have been adopted in the African region.

---

[6] Jouanjean (n 5).

[7] Personal data is defined as 'any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity' (AU Convention, Article 1). Related legislation is referred to interchangeably as 'personal data protection law', 'data protection law' or 'data privacy law' in this article.

[8] Can Atik, 'Towards Comprehensive European Agricultural Data Governance: Moving Beyond the "Data Ownership" Debate' [2022] 701–742 (53) IIC - International Review of Intellectual Property and Competition Law < https://doi.org/10.1007/s40319-022-01191-w> accessed 5 September 2022; Mihalis Kritikos, 'Precision agriculture in Europe: Legal, social and ethical considerations' (European Parliamentary Research Service, 2018).

[9] See for example Can Atik and Bertin Martens, 'Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU' [2021] 12(3) JIPITEC 3; Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law.' [2018] 10(1) LIT 40 <https://doi.org/10.1080/17579961.2018.1452176> 11 January 2021.

[10] James Wilgenbusch and others, *Dealing with data privacy and security to support agricultural R&D: Technical practices and operating procedures for responsible agroinformatics data management* (CGIAR Big Data Platform 2020); Jouanjean (n 5); Leanne Wiseman and others, *Review of codes of conduct, voluntary guidelines and principles relevant for farm data sharing* (CTA - Technical Centre for Agricultural and Rural Cooperation 2019); Tsan (n 1).

Thus, the only transparent regulatory framework establishing data protection requirements for agricultural data in Africa, even if not specifically so, are personal data protection regulations.[11] National data privacy laws are increasingly being adopted around the world. They started to emerge in Western Europe in the 1970s and 1980s, followed by Latin America and Eastern Europe in the 1990s and early 2000s, and Asia since 2010.[12] While African countries were relatively late in the adoption of such laws, it is now the region with the fastest expansion in personal data protection laws, partly driven by the entry into force of the European Union's data protection regulation in 2018. As of December 2021, 32 out of 54 African countries had adopted data protection laws and several of the remaining countries were working on related legislation.

The first regional legal instrument on data protection in Africa was developed by the Economic Community of West African States (ECOWAS) in 2010 for its 15 member states.[13] Inspired by the ECOWAS Act, 'The African Union Convention on Cyber Security and Personal Data Protection' (hereafter 'the AU Convention') was adopted at the African Union's Summit in Malabo, Equatorial Guinea in 2014.[14] The ECOWAS Data Protection Act and the AU Convention seek to create a harmonized legal framework for personal data protection at the sub-regional and continental level. Due to the high mobility of data and the cross-border activities of many digital service providers, harmonizing national regulations is particularly needed. Otherwise, the efforts of individual countries to safeguard their citizens' data can be easily undermined when data is transferred to other states with weaker data protection laws.[15]

Although the AU Convention is yet to enter into force, its adoption made Africa only the second region after the European Union to have a region-wide legal instrument for personal data protection.[16] However, contrary to the EU regulations, there are no enforcement mechanisms once the Convention has entered into force and a country can withdraw anytime. Increasing trade integration in Africa through the African Common Free Trade Area (AfCTA), which was officially launched in January 2021, will make harmonization of data protection laws more and more important. Lack of harmonization also poses challenges for multinational organisations and companies operating on the continent.[17] However, the AfCTA does not foresee a similar level of institutional and regulatory

[11] Licensing agreements or contracts that are signed between digital service providers and users are not publicly available to third parties and therefore cannot be studied easily.

[12] Graham Greenleaf and Bertil Cottier, *Comparing African data privacy laws: International, African and regional commitments* (University of New South Wales 2020)

[13] Uchenna Jerome Orji, 'Regionalizing data protection law: A discourse on the status and implementation of the ECOWAS Data Protection Act' [2017] 7(3) IDPL 179 <https://doi.org/10.1093/idpl/ipx013> accessed 02 December 2021.

[14] To complement and further facilitate the implementation of the AU Convention by member states, the AU Commission issued the non-binding 'Personal Data Protection Guidelines for Africa' in 2018 to elaborate on the Conventions' general requirements.

[15] Tiffany Curtiss, 'Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies' (2016) 12(1) WJLTA <https://digitalcommons.law.uw.edu/wjlta/vol12/iss1/5> accessed 06 August 2021.

[16] Greenleaf and Cottier (n 12).

[17] Deloitte, *Privacy is Paramount: Personal Data Protection in Africa* (Deloitte 2017).

harmonization as the EU. With regard to personal data protection, the AfCTA explicitly allows countries to put in place their own laws as long as they don't contravene the AfCTA (Article 15.c.ii). As a result, the main onus of regulating personal data protection remains with the national regulatory bodies unless additional legally binding and enforceable rules are adopted at the pan-African level.

While the importance of regulating personal data use is increasingly being recognized by African governments, it remains unclear to what extent digital agriculture service providers are complying with such legislation. Little is also known about the level of concern among African producers regarding the protection of their data. Research from industrialized countries shows that concerns among farmers regarding data protection are increasing as agriculture becomes more digitalized.[18] In response, some farmers are advocating for greater control over their agriculture data and to address the power disparities and information asymmetries between service providers and farmers.

This article aims to contribute to the existing literature on personal data protection related to farm data by addressing a number of important research gaps. First, it builds on existing reviews of data protection legislation in Africa by adding a systematic comparison with provisions of the AU Convention, relating the level of protection to the level of activity of digital agricultural services providers in the countries, and analysing provisions of particular relevance to digital agriculture in more detail. Second, to assess the effectiveness of the legislation, the article is the first to evaluate compliance of the data privacy policies of digital agricultural service providers in Africa with national legislation. Third, the article is the first to provide initial insights into perceptions among African agricultural producers on data protection and privacy.

The remaining article is structured as follows. Section 2 highlights the key challenges for data governance in smart farming and provides a review of the literature related to personal data protection laws in Africa, compliance of digital agricultural service providers with these laws and perceptions related to data privacy among agricultural producers and users more general. Section 3 outlines the methodology used in this research. Section 4 presents the analysis of African data protection laws and how they compare to the provisions of the AU Convention. Section 5 reviews data privacy policies of digital agricultural services and assesses compliance with national laws. Section 6 reports on the results of a survey among agricultural producers in Benin, Ethiopia and Ghana. The final section integrates the findings from the three previous sections to draw broader conclusions on personal data protection and digital agriculture in Africa, and identifies areas for further research.

[18] Jouanjean (n 5).

2 Literature review

2.1 Literature on governance issues related to the protection of agricultural data

The digital transformation of food and agriculture is increasingly envisioned as a technological solution that could help address a broad range of societal issues, such as achieving global food security, reducing the environmental impact of agriculture, and enhancing the food safety and acceptability through traceability and transparency.[19] The collection of farm data and the applications that result from them could play an important role in this regard. For farmers, actionable insights to support decision making can be obtained by analysing their farm data, helping them to better plan and execute farming activities. For agricultural and food value chains, the availability and flow of agricultural data facilitates efficient transactions, cross-border trade and less-complex custom processes around agricultural products, allowing smallholder farmers and small enterprises to participate in international trade. For governments and policy makers, the ability to access and process aggregated farm data can also be beneficial in designing, implementing and monitoring of agricultural policies, helping them make data-driven decisions and suitable policy choices for farmers, consumers and other players in the food system.[20]

As with many technological changes, the digital transformation of the agri-food sector must address a range of socio-ethical challenges. According to a recent literature review, one such socio-ethical challenge centers on the issue of data privacy, ownership, access, sharing and control.[21] The issue of data privacy, ownership, access, sharing and control of farm data is a complex topic that stands at the intersection of different regulatory frameworks, i.e. personal data protection laws, contract and competition laws, and intellectual property rights. However, none of these regulatory frameworks currently provide sufficient protection for farm data and many aspects of their application to farm data remains unclear.[22] For the purpose of this article, farm data refers to any data related to the farmer, the farming site, the farming operations and commercial transactions related to the farm, collected by the farmers themselves, external data collectors or data collection devices, such as sensors or cameras.

Data privacy is an issue often raised when personal data is collected by intermediaries with powerful analytical tools. However, when it comes to the use of farm data in digital agricultural applications, privacy rights are rarely discussed.[23] To what extent farm data

[19] Simone van der Burg, Marc-Jeroen Bogaardt, Sjaak Wolfert, 'Ethics of smart farming: Current questions and directions for responsible innovation towards the future' [2019] (90–91) NJAS - Wageningen Journal of Life Sciences <https://doi.org/10.1016/j.njas.2019.01.001> accessed 12 February 2020.

[20] Ajit Maru and others, Digital and data-driven agriculture: Harnessing the power of data for smallholders (GFAR, GODAN and CTA 2018); Tsan (n 1); Jouanjeani (n 5).

[21] van der Burg (n 19).

[22] Jouanjean (n 5).

[23] van der Burg (n 19); Andreas Kamilaris, Andreas Kartakoullis, Francesc X. Prenafeta-Boldú, 'A review on the practice of big data analysis in agriculture' [2017] 23–37 (143) Comput. Electron. Agric. <https://doi.org/10.1016/j.compag.2017.09.037> accessed 18 September 2019; Michael Sykuta, 'Big data in agriculture: privacy, property rights and competition in Ag Data Services' [2016] 57–74 (19) Int. Food Agribusiness Manag. Rev. <10.22004/ag.econ.240696> accessed 21 August 2019.

should be classified as personal and therefore fall under personal data protection laws is not clear-cut and may need to be decided on a case-by-case basis depending on the context and purpose of processing.[24]

Moreover, the ownership of data – i.e. who has specific rights to data, including the right to use the data and for what purposes – is at times unclear with regard to non-personal data collected in the context of smart farming. While farmers believe themselves to be the owners of the data collected from their farms, the intermediaries that process farm data own the computed data.[25] Even if agricultural stakeholders generally agree that farmers own the data that is collected on their farms, no specific right corresponding to ownership of data in terms of property over data is included in the laws.[26] This raises the question of how farm data should be governed, i.e. who should control and extract value from the data.

Legal contracts and licensing agreements may be used to bring legal clarity, for instance by specifying the ownership of data covered by the contract. However, such a data ownership provision is not sufficient to protect farmers in terms of the rights they get from it. In addition, the terms and conditions specified in the contracts effectively establish the conditions of the use of the data. Thus, data ownership in itself may not address governance issues relating to access, sharing and use of farm data.[27] Patents and copyright laws also do not provide protection for farmers' data. Patents for instance only cover the invention of a new process or a machine, while copyrights cover original works of authorship. Farm data is not invented by farmers, nor is it a new process or a machine and nor does it qualify as original works of authorship. Farm data, if legally classified as a trade secret, could be protected under the laws governing intellectual property rights and specifically trade secrets. In this case, farmers could then own their data and only allow other parties to use it through licensing agreements that are governed by contract laws. However, this is not yet the case and hence such laws may not yet provide protection for farm data. [28]

From a policy perspective, rather than focusing on the concept of ownership, it might be more practical to focus on the issues that it is meant to address, i.e. to strike a balance in the conditions for sharing, controlling and using farm data.[29] In this regard, regulators can formulate guidelines or standard contractual provisions that should be included in data licensing agreements and contracts, either specifically in agriculture or more broadly. Recently, voluntary codes of conducts have been introduced for the agriculture sector in some countries and regions to set common standards for farm data licensing contracts and improve the governance of agricultural data, for instance in the EU, USA, New Zealand and

[24] Can Atik, 'Towards Comprehensive European Agricultural Data Governance: Moving Beyond the "Data Ownership" Debate' [2022] 701–742 (53) IIC - International Review of Intellectual Property and Competition Law < https://doi.org/10.1007/s40319-022-01191-w> accessed 5 September 2022; Mihalis Kritikos, 'Precision agriculture in Europe: Legal, social and ethical considerations' (European Parliamentary Research Service, 2018).
[25] van der Burg (n 19).
[26] Jouanjeani (n 5).
[27] Jouanjeani (n 5).
[28] Neal Rasmussen, 'From precision agriculture to market manipulation: a new frontier in the legal community' [2016] 489–516 (17) Minn. J. Law Sci. Technol. <https://scholarship.law.umn.edu/mjlst/vol17/iss1/9> accessed 28 September 2022; Kamilaris (n 23); van der Burg (n 19).
[29] Atik (n 24)

Australia. Several other countries are also examining the development of agricultural data codes of practice. However, it is yet to be seen if these voluntary codes of conduct are having the desired effect and if they would be introduced worldwide to protect farmers from the misuse of their data.[30]

In the absence of sound regulatory frameworks that govern the access, sharing, and control of farm data, farmers are concerned about their data being used by agricultural technology providers and intermediaries for other purposes aside from advising them, for instance for anti-competitive practices and manipulation of market outcomes. This is especially critical when large companies not only control smart farming applications and the algorithms underlying them to offer recommendations to farmers, but also provide the services, technological farm supplies and inputs that farmers need to put the recommendations into practice. Such concerns highlight the lack of trust that farmers have for digital service providers and data platforms and farmers' concern over the unfair competitive advantage that large companies have with their privileged insights over farmer's data in a specific country or region.[31]

2.2 Literature on the current state of data protection in Africa

Several authors have analysed national data protection laws in Africa.[32] All studies point to the need for further improvements in the protection of personal data. At the same time, the AU Convention is seen as an opportunity to raise data privacy protection to an adequate level. None of the studies provide a systematic comparison with the provisions of the AU Convention or assess the regulations from the perspective of digital agricultural service provision, as presented in this article. Given the rapid changes in data protection laws in Africa in the past few years, only the most recent studies are reviewed here in more detail.

The International Bar Association provides the most recent and comprehensive review of African data protection laws.[33] The study notes that the African data protection ecosystem is highly influenced by Europe's regulatory approach. Comparing the AU Convention with European regulations, the authors note that the AU Convention was designed along the lines of the EU Data Protection Directive 95/46/EC, which was replaced by the General Data Protection Regulations in 2018. Therefore, the AU Convention may not be a suitable bridge for collaboration with Europe, they conclude. At the national level, the authors find that the African data protection ecosystem is underdeveloped and disparate due to the variety of frameworks and laws in Africa which are at different stages of implementation and cause disagreements around harmonisation, collaboration and cooperation.

[30] Jouanjeani (n 5); van der Burg (n 19); Wilgenbusch (n 10); Wiseman (n 10); Tsan (n 1).
[31] van der Burg (n 19); Kamilaris (n 23); Sykuta (n 23); Neal (n 28).
[32] See for example Deloitte (n **Error! Bookmark not defined.**); Greenleaf and Cottier (n 12); IBA, The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa' (International Bar Association 2021); Mouhamadou Lo, *La protection des données à caractère personnel en Afrique* (Baol editions 2017); Alex Boniface Makulilo, 'Privacy and data protection in Africa: A state of the art' [2012] 2(3) IDPL 163; Cynthia Rich, *A Look at New Trends in 2017: Privacy Laws in Africa and the Near East* (Bureau of National Affairs 2017)
[33] IBA (n 32).

Another recent review of national, regional and continental data protection regulations was carried out by Greenleaf and Cottier.[34] The authors note that the AU Convention was expected to be a driver for data protection in Africa. However, this anticipation could not yet be fulfilled, as the required number of countries for ratifying the Convention has not been met. Nevertheless, the authors caution that the implementation of uniform data protection rules across Africa is a lengthy process, pointing to the 40 years it took the EU member states to enact uniform data privacy laws. The authors predict that the vast majority of African countries will have adopted related legislation by the end of the 2020s.

No research has been carried out to assess the compliance of digital agricultural service providers with national data protection legislation in Africa. Similarly, no research has been done to study African agricultural producers' perception of the need for and adequacy of data protection. The limited research into perceptions of data protection among African users more generally points to growing concerns, but also perceived opportunities. Anecdotal evidence from East Africa suggests that users are increasingly worried that their data may be misused, but very few people are aware of how to ensure online security and privacy.[35] At the same time, however, many said that they interacted more freely via social media than in face-to-face interactions.

One survey among South African internet users found a high level of concern about the protection of personal data among 80 percent of respondents, in particular with regard to data related to their personal identity and financial and health information.[36] In contrast to the study by Kinuthia,[37] for many sharing information online was more problematic than in face-to-face interactions (79 percent and 57 percent of respondents, respectively). Almost two thirds (62 percent) said that they know their privacy rights, but only 37 percent knew how to lodge a complaint. Many do not feel that the organizations collecting and processing personal data adequately implement legal protection requirements.

A study of mobile phone-based health applications in Tanzania concludes that direct users of the technology may trust it more than their clients.[38] Specifically, they find that community health workers felt that smartphone use actually increased data protection compared to paper-based forms while the female clients were more concerned about who has access to these data.

Additional insights relating specifically to agricultural producers can be gained from research into farmers' perception from industrialized countries where extensive data collection and processing is already widespread in the agriculture sector. These finding suggest that farmers are increasingly wary that their data may be used by businesses for

[34] Greenleaf and Cottier (n 12).
[35] Duncan Kinuthia, *Exploring Data Anonymisation and Internet safety in East Africa* (Research ICT Africa 2020)
[36] Adéle Da Veiga, 'An information privacy culture instrument to measure consumer privacy expectations and confidence' (2018) 26(3) ICS 338 <doi.org/10.1108/ICS-03-2018-0036> accessed 20 June 2021.
[37] Kinuthia (n 35).
[38] Kristy M. Hackettab, Mina Kazemic and Daniel W.Sellen, 'Keeping secrets in the cloud: Mobile phones, data security and privacy within the context of pregnancy and childbirth in Tanzania' [2018] 211 SSM 190 <doi.org/10.1016/j.socscimed.2018.06.014> accessed 16 July 2020.

commercial gain without adequate compensation for the data providers.[39] Reporting findings from Australia, see a lack of trust between the farmers as data providers and the third parties that collect, aggregate and share their data at the root of these concerns.[40]

3 Methodology

The data for the analysis in this study was collected in three ways: (1) an analysis of national laws in Africa that regulate the collection and use of personal data, (2) an analysis of data privacy policies of digital agricultural service providers operating in Africa, including an assessment of their adherence to national legislation, and (3) a survey among African agricultural producers to assess perceptions related to data privacy.

3.1 National legislation for data protection

First, the status of adoption of national data protection laws in all African countries was assessed (as of December 2021). The legal texts of national laws were collected for all African countries where such laws have entered into force and the provisions of the laws were analysed. To this end, the provisions of national laws were compared with related provisions set out in the AU Convention which thereby served as the reference point for the analysis. The analysis did not assess compliance with the AU Convention since the Convention has not yet entered into force and several of the laws were already in place upon its adoption. Rather, the Convention was treated as a commonly agreed standard that African countries are expected to aim for in the future. Draft legislation was not included in this analysis.

The focus of the analysis was on provisions that are of direct relevance to users of digital agricultural services, in particular as they related to personal data, i.e. the principles governing the processing of personal data (Article 13 of the AU Convention) as well as the users' rights to their personal data (Articles 16-19, 'Data Subjects' Rights'). Additional provisions of interest relate to Data Protection Authorities (DPAs), cross-border flow of data and automated data processing.

[39] Emma Jakku and others, 'If they don't tell us what they do with it, why would we trust them?" Trust, transparency and benefit-sharing in Smart Farming' [2019] 90-91(1) WJLS 90 <doi.org/10.1016/j.njas.2018.11.002> accessed 11 February 2021; Jouanjean (n 5); Max V. Schönfeld, Reinhard Heil and Laura Bittner, 'Big Data on a Farm—Smart Farming' in T. Hoeren and B. Kolany-Raiser (Eds.), *Big Data in Context: Legal, Social and Technological Insights* (Springer); Simone van der Burg, Leanne Wiseman and Jovana Krkeljas, 'Trust in farm data sharing: Reflections on the EU code of conduct for agricultural data sharing' (2021) 23 EIT <https://doi.org/10.1007/s10676-020-09543-1> accessed 10 September 2021.

[40] Leanne Wiseman, Jay Sandersonb, Airong Zhangc and Emma Jakku, 'Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming' (2019) 90–91WJLS 1 <https://doi.org/10.1016/j.njas.2019.04.007> accessed 05 July 2020.

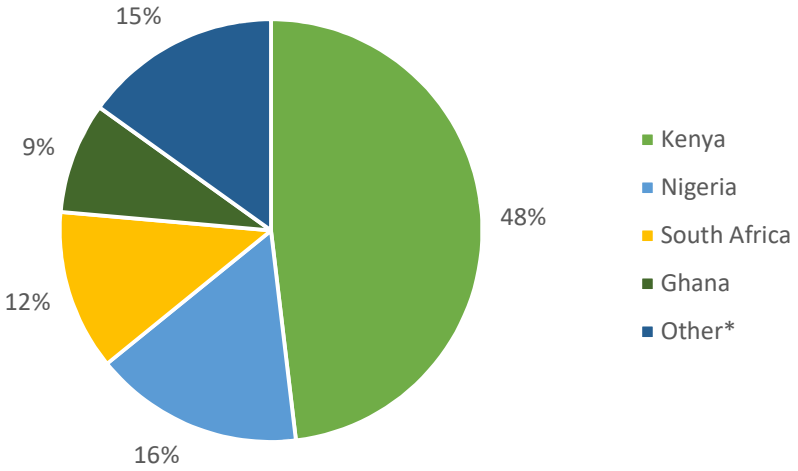
3.2 Data privacy policies of digital agricultural service providers

A list of agricultural digital service providers operating in Africa was compiled using information from the CTA,[41] the GSM Association[42] and web searching. Digital agricultural services were included if

- they provided a service to producers and use digital technologies in their service provision
- they are operating in at least one African country (but not necessarily exclusively in Africa) and are subject to at least one African country's legislation,
- they are operating at the time of the review, and
- they have their own functioning website.

Using these criteria, a list of 106 digital agricultural services was compiled. For these services, the availability of a service-related privacy policy on the providers' websites was documented (as of September 2021). Privacy policies that only apply to visitors of the websites, but not the digital agricultural service offered by the provider, were not included. Where such a policy was available, compliance with the requirements set out in national legislation was assessed. Where service providers operate in more than one African country, their privacy policy was compared with the strictest data protection regulation adopted in the countries of operation. The jurisdiction most commonly used for the purpose of this analysis are Kenya, Nigeria, South Africa and Ghana (**Error! Reference source not found.**).

Figure 1: Jurisdiction for digital service providers used for the analysis



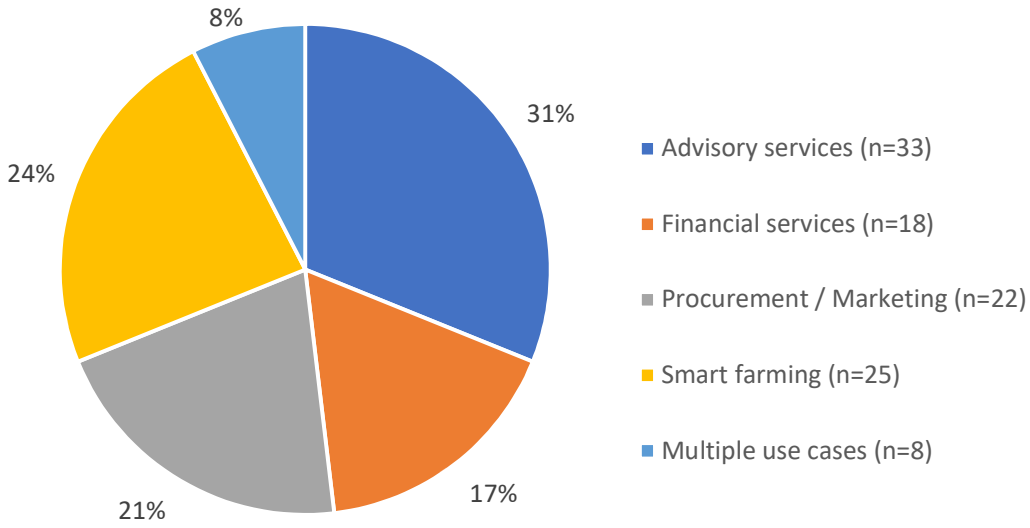
* Burkina Faso, Cameroon, Egypt, Ethiopia, Ivory Coast, Mali, Niger, Senegal, Tanzania, Uganda and Zimbabwe
Source: Authors' own elaboration (as of September 2021).

[41] Tsan (n 1).

[42] GSMA (n 2); GSMA, *AgriTech Deployment Tracker. Mobile for Development* (GSM Association 2021)

The 106 digital agricultural service providers were disaggregated into four primary use cases which were adapted from GSMA:[43] advisory services, financial services, procurement/marketing and smart farming. Where no primary use case could be identified, the service was classified as 'multiple use cases'. The most common primary use case is digital advisory (31 percent of services), followed by smart farming (24 percent), procurement and marketing (21 percent) and financial services (17 percent) (**Error! Reference source not found.**). Eight percent of service provided multiple uses.

Figure 2: Digital agriculture service providers by primary use case



Source: Authors' own elaboration (as of September 2021).

3.3 Producers' data privacy concerns

Data from a survey was analysed to assess to what extent agriculture producers already take measures to protect their data. Data was collected through in-person surveys from 1,915 respondents in Benin (642), Ethiopia (623) and Ghana (650) in October/November 2019. The data collection was part of a larger survey to assess impacts of youth initiatives in the four countries and the respondents were sampled based on their participation in such initiatives plus a control group. To this end, lists of beneficiaries of four youth initiatives in each country were obtained from which the samples were randomly drawn. Non-beneficiaries were interviewed in the same regions using snowball sampling. As a result, the final sample shows a bias towards men (63 percent of the sample) and an uneven distribution across age groups (majority 25-30 year old). It is therefore not necessarily representative of African producers, but nevertheless gives a first insight.

The characteristics of the sample are presented in Table A1 in the Appendix. The respondents were between 15 and 40 years old. Almost one third (29 percent) were engaged in agriculture as their primary occupation (primarily crop farming, but also livestock and agro-forestry), ranging from 23 percent in Ethiopia to 39 percent in Benin. Across the entire sample, 59 percent of respondents use the internet. Among agricultural producers, that share is lower

[43] GSMA (n 2).

at 48 percent. The concern about data privacy was assessed by asking internet users a number of questions about the steps they are taking (or not) to inform themselves of their data protection rights or restrict access to their data. The responses were analysed specifically for agricultural producers and compared to answers of non-producers. Correlation analysis is used to assess the influence of individual characteristics (sex, age, education, occupation) on internet use, the decision to seek information about data protection and control access to personal data.

4 National Privacy and Data Protection Legislations in Africa

This section assesses the current state of the personal data protection in Africa by reviewing existing national data protection laws that influence the ownership, access and use of personal data in Africa. Data protection laws that have been adopted are compared with the provisions of the AU Convention. The analysis focuses on Chapter II-Personal Data Protection of the AU Convention which, among other provisions, sets out basic principles governing the processing of personal data, the rights of users (referred to as 'data subjects' in the AU Convention) to their personal data, details of an institutional framework for the protection of personal data, and obligations placed on entities collecting and processing the data (referred to as 'controllers').

4.1 Status of national data protection legislation adoption

The personal data protection regulatory landscape in Africa has changed considerably over the last few years. As of December 2021, more than half of the African countries (32 of the 54) have enacted data protection laws (Figures 3 and 4 and Source: Authors' own elaboration

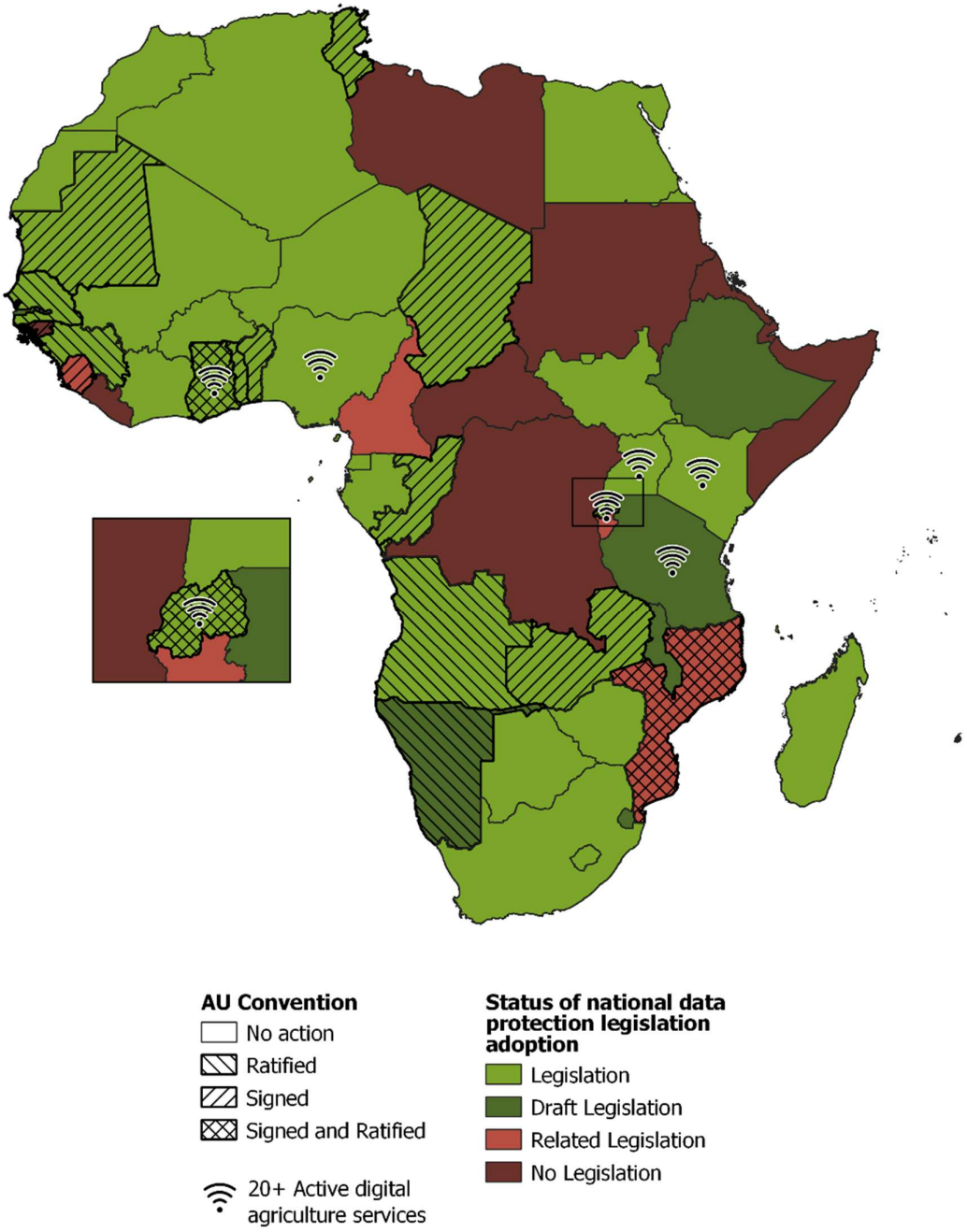
Table A2 in the Appendix), including Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Côte d'Ivoire, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, Republic of the Congo, Rwanda, Sao Tome and Principe, Senegal, South Africa, Togo, Tunisia, Uganda, Zambia and Zimbabwe.[44]

Of the remaining 22 African countries, seven have officially introduced draft laws, including Eswatini, Ethiopia, Gambia, Malawi, Namibia, Seychelles and Tanzania. It is unclear, how many of these regulations are likely to be adopted in the near future. In the Seychelles, for instance, the relevant legislation was enacted already in 2004, but has yet to enter into force (see other country examples below).[45] Four countries have not put forward a draft bill yet, but have related, albeit limited legislation in place (i.e. relevant provisions are included in other legislation), including Burundi, Cameroon, Mozambique and Sierra Leone. Eleven countries do not have any legislation in place, namely Central African Republic, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Guinea-Bissau, Liberia, Libya, Somalia, South Sudan and Sudan.

[44] More detailed information including the title of the key legislations for those countries that have data protection legislation, the draft legislations for those that either have bills proposed for data protection and related legislation for countries that have related legislation to govern privacy and personal data protection; year of law's enactment or recent amendment; and the appointment status and independence of the data protection authority is presented in **Error! Reference source not found.** in the Appendix.

[45] Malcolm Moller, Indra Govind and Jyotika Kaushik, 'Seychelles—Data Protection Overview' (DataGuidance 2021) https://www.dataguidance.com/notes/seychelles-data-protection-overview accessed 5 August 2021.

Figure 3: African Data Protection Legislation Landscape



Source: Authors' own elaboration (as of 23 December 2021). Cartography: Paula Rothenberger.

As of December 2021, eight countries have ratified the AU Convention, namely Angola, Ghana, Guinea (Conakry), Mauritius, Mozambique, Namibia, Rwanda and Senegal, while 14 countries have signed it, including Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome and Principe, Togo, Tunisia and Zambia. The date of the last signature was May 2020. Of those that ratified the AU Convention, only Namibia has not adopted legislation yet (but is in the process of doing so).

Among those that signed the Convention, Comoros, Guinea-Bissau, Mozambique and Sierra Leone do not have a data protection legislation in place.

Comparing countries that have enacted data privacy regulations with prevalence of digital agricultural services shows that most of the countries where such services are more widespread have put personal data protection legislation in place (**Error! Reference source not found.**, **Error! Reference source not found.**). Among the six countries where 20 or more digital services are available, only Tanzania has not yet enacted data protection legislation. Tanzania has been working on a bill since 2013, but the draft has not been released publicly yet.[46] Among the seven countries with 10-19 digital agricultural solutions, data protection legislation is still lacking in Ethiopia and Malawi. Ethiopia already presented a draft data protection law in 2009, but little progress has been made to pass this legislation and in 2020, the government released a new draft, the Personal Data Protection Proclamation.[47] Malawi published a draft Data Protection Bill in 2021. Tanzania, Ethiopia and Malawi have not signed or ratified the AU Convention.

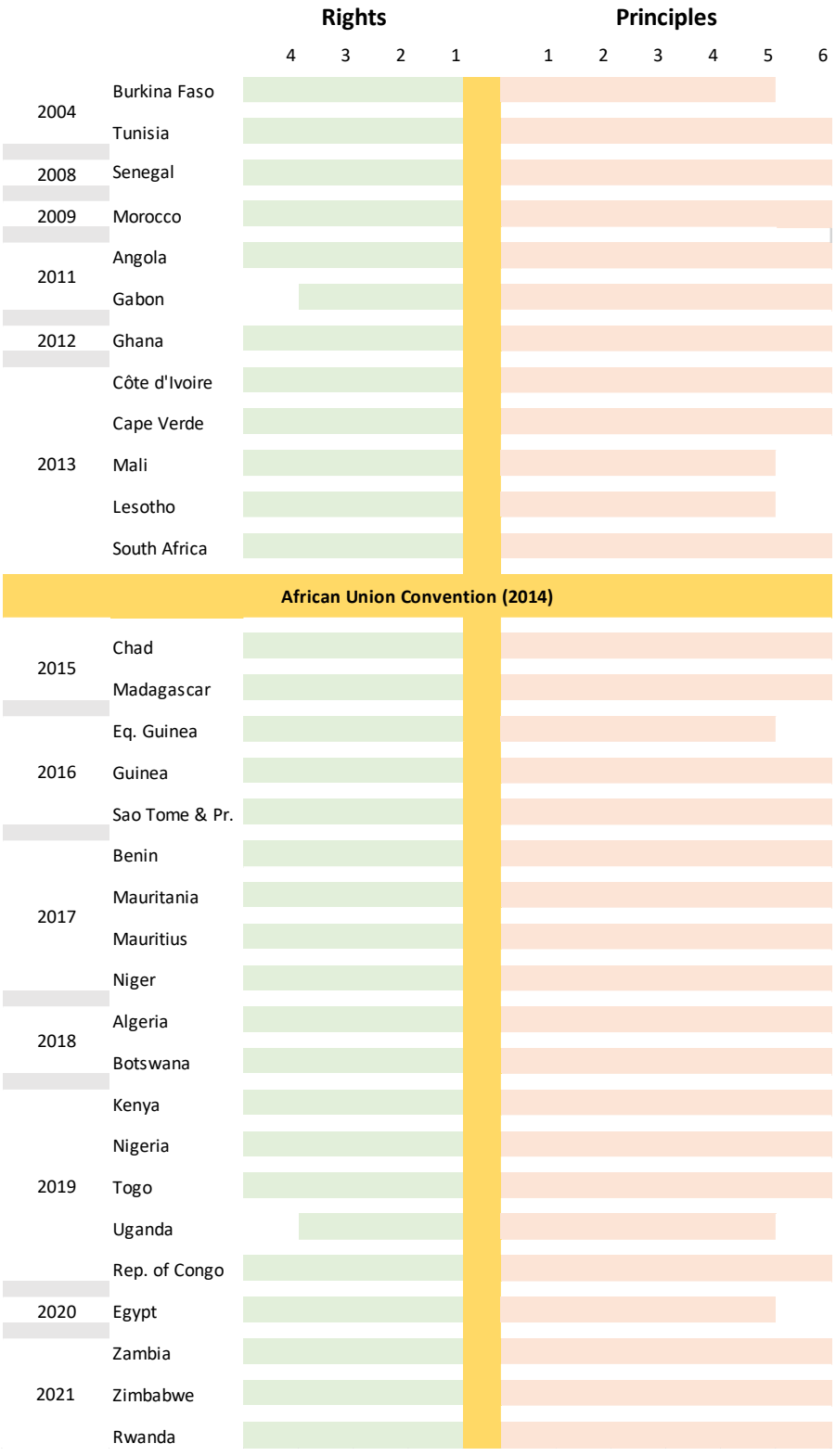
Table 1: Status of legislation and prevalence of digital agricultural services

No. of services	Specific data protection legislation in place	No legislation
20+	Ghana, Kenya, Nigeria, Rwanda, Uganda	Tanzania
10-19	Côte d'Ivoire, Senegal, South Africa, Zambia, Zimbabwe	Ethiopia, Malawi
4-9	Egypt, Madagascar, Mali	Burundi, Cameroon, Mozambique
1-3	Algeria, Angola, Benin, Botswana, Burkina Faso, Chad, Equatorial Guinea, Gabon, Guinea (Conakry), Lesotho, Morocco, Niger, Republic of the Congo, Sao Tome and Principe, Togo, Tunisia	Central African Republic, Democratic Republic of Congo, Djibouti, Eritrea, Eswatini, Gambia, Guinea-Bissau, Liberia, Namibia, Sierra Leone, Somalia, South Sudan, Sudan
no data	Cape Verde, Mauritania, Mauritius	Comoros, Libya, Seychelles

Sources: GSMA (2020) (no. of services, as of Jan. 2020), authors' compilation (status of legislation)

[46] Chris Green, 'Tanzania—Data Protection Overview' (Dataguidance 2021) https://www.dataguidance.com/notes/tanzania-data-protection-overview accessed 26 November 2021.
[47] Hlengiwe Dube and Avani Singh, *Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries* (African Declaration on Internet Rights and Freedoms Coalition 2021).

Figure 4: AU Convention principles and rights reflected in national legislation



Source: Authors' own elaboration. As of 23 December 2021.

4.2 Principles governing the processing of personal data

AU Convention

The African Union Convention outlines a set of **basic principles** governing the processing of personal data (Article 13) which include the Principles of

(1) consent and legitimacy of personal data processing
(2) lawfulness and fairness of personal data processing
(3) purpose, relevance and storage of processed personal data
(4) accuracy of personal data
(5) transparency of the personal data processing
(6) confidentiality and security of personal data.

In addition, the AU Convention established specific principles for the processing of **sensitive data** (Article 14). Specifically, the Convention prohibits 'any data collection and processing revealing racial, ethnic and regional origin, parental filiation, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject'.

National legislation

In the large majority of African countries, national data protection laws include provisions covering the principles set out in the AU Convention (Figure 4). In most cases, they are explicitly listed as principles, while in a few cases they are reflected in the provisions.

Principles 3 (purpose, relevance and storage) and 6 (confidentiality and security) are covered by all regulations. Only a few countries do not include one of the remaining principles:

- Mali is the only country that does not require consent to be obtained from data subjects (Principle 1).
- The regulations of Egypt, Equatorial Guinea and Lesotho do not contain provisions that would require that the collection, recording, processing, storage and transmission of personal data is undertaken lawfully, fairly and non-fraudulently (Principle 2).
- Burkina Faso does not require that data collected to be accurate and, where necessary, kept up to date, and that steps must be taken to ensure that data which are inaccurate or incomplete are erased or rectified (Principle 4). Rather, it puts the onus on data subjects to request corrections to their data if needed.
- Uganda is the only country that does not mandate data controllers to disclose information on personal data (Principle 5).
- The regulations of Côte d'Ivoire, Niger and Nigeria do not contain specific provisions governing the processing of sensitive data even though they all define 'sensitive data' within the legislation.

None of these countries have signed or ratified the AU Convention. In the case of Burkina Faso, Côte d'Ivoire, Lesotho and Mali, the regulations were adopted before the Convention, while Egypt, Equatorial Guinea, Niger, Nigeria and Uganda adopted their legislation afterwards.

4.3 Rights to personal data

AU Convention

The Convention sets out a number of rights of data subjects' to their personal data:

> **Article 16: Right to information** about the entity collecting and processing the data (referred to as the 'data controller'), the purpose of data processing, the data involved, the recipient of the data, their rights to be removed from the file and to access and rectify data, the storage period, and proposed transfers of data to third countries. This information should be provided no later than the time when the data are collected,
>
> **Article 17: Right of access** information upon the user's request to evaluate and object to processing, whether personal data are being collected and processed, the source of the data being processed, the purpose of and data used in processing, the recipient of the data.
>
> **Article 18: Right to object**, on legitimate grounds, to the processing of personal data.
>
> **Article 19: Right of rectification or erasure** of personal data upon demand by the user where such data are inaccurate, incomplete, equivocal or out of date, or whose collection, use, disclosure.

National legislation

Similar to the principles set out in the AU Convention, users' rights to their data are widely reflected in the data protection legislation adopted across Africa (Figure 4). The only exception relates to the right to information which is not included in the Ugandan law (adopted after the AU Convention) and only partially in Gabon (adopted before the AU Convention) where the right of information applies only to health data. In both countries, data subjects can request access to the information but are not automatically provided with the information when their data are collected. Neither country has signed or ratified the Convention.

4.4 Data protection authority

AU Convention

As shown above, the majority of the national laws cover most of the principles and rights set out in the AU Convention. For these and other provisions of the legislation to be effective, they need to be implemented, monitored and enforced. To this end, the AU Convention requires the establishment of a national personal data protection authority (DPA) to ensure that 'the processing of personal data is conducted in accordance with the provisions of this Convention' (Articles 11). The Convention also sets out the envisaged functions of the DPA, including granting authorizations for certain data processing and transfer, entertaining complaints, reporting offenses to the judicial authority and imposing sanctions on data controllers, among others (Article 12).

While each country is free to determine the composition of the national DPA, the AU Convention provides strict guidance on keeping the DPA independent (Article 11). Members of the DPA must not be members of government or be involved in ICT businesses as

executives or shareholders. They should also enjoy full immunity for opinions expressed in connection with their duties and not receive instructions from any other authority.

National legislation

All of the existing data protection laws foresee the establishment of a DPA. Most countries (28) already set out the administrative details. In Equatorial Guinea, Guinea (Conakry) and the Republic of Congo, additional regulations are required before the DPAs can be established, as specified in the law. This has not been done so far even though the laws were already adopted in 2016 (Equatorial Guinea, Guinea Conakry) and 2019 (Republic of Congo). In Rwanda, the rights and obligations of a 'supervisory authority' are set out in the legislation, but the authority is not established and its status is unclear.

Among the 28 countries that have already established DPAs in their legislation, only 18 have appointed DPAs (as of December 2021). In a few cases this gap could be explained by the recency of the legislation (i.e. Egypt and Zambia where the regulations were only adopted in 2020 and 2021 respectively). In the remaining countries (Algeria, Botswana, Lesotho, Madagascar, Mauritania, Niger, Togo and Uganda), the laws were adopted between 2015 and 2019. Without a DPA, the laws cannot be implemented effectively since there is no authority to monitor and enforce the rights.

Moreover, in nine of the 28 countries, the DPA is not independent as stipulated in the AU Convention. Instead, the DPA is placed under the direct authority of a government representative, such the Prime Minister or a Minister (Algeria, Egypt, Nigeria, Uganda and Zambia), can receive ministerial instructions (Botswana, Ghana), or include members that are representatives of ministries (Algeria, Ghana, Tunisia) or are appointed by the King (Morocco). Among these countries, only Ghana, Morocco, Nigeria and Tunisia have so far appointed their DPA. The lack of independence could seriously undermine the level of protection of personal data in case of government interference.

4.5 International data transfer

AU Convention

Many digital service providers operate across countries where data may be collected in one country and processed or used by third parties in another. Such transfers are important e.g. for services that facilitate supply chains management or financial transactions. Regulations that govern the transfer to data across borders is therefore relevant for many providers as well as the users of their services.

The AU Convention sets out restriction on the international transfer of data (Article 14.6). The data controller is in general prohibited from transferring personal data to a non-Member state of the African Union 'unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed'. This prohibition does not apply, however, if the data controller has sought permission to transfer the data from the national DPA.

National legislation

The majority of countries (with the exception of Burkina Faso, Côte d'Ivoire and Tunisia) are less restrictive than the AU Convention when regulating the international transfer of data (

Table A4 in the Appendix). Among the 32 regulations, 27 include exceptions that allow transfer of data to countries without an adequate level of protection. Seventeen countries also allow transfers of data if an adequate level of protection can be assured among the controllers handling the data. The regulation of Ghana does not include any provisions on international data transfers.

In most cases (25), the exceptions are specified in the legislation, e.g. if data subject has given consent and/or the transfer is necessary for certain specified reasons (incl. contract execution, public interest or money transfer or if it takes place within a multilateral agreement). The legislation of Niger leaves the nature of the exceptions open, allowing such transfers by decree of the Council of Ministers. The laws of Uganda and Zimbabwe are special cases. The Ugandan law restricts data transfer to countries without adequate protection in line with the AU Convention, but only with regard to data storage and processing of Uganda-based data processors. The Zimbabwean law exempts data transfer 'to allow tasks covered by the competence of the controller to be carried out' from the restrictions.

As noted above, the AU Convention also provides for exceptions to the prohibition of international data transfer if the transfer has been authorized by the DPA. Of the 27 countries that allow for exceptions, only 9 require such an authorization. Another 12 regulations require the DPA to be notified of transfers. Adding authorization and notification requirements to the law would be an important measure to increase monitoring and compliance.

Another relevant question is who decides the 'adequate level of protection' in the recipient country. In 14 countries, this decision is taken by the DPA. In two countries (Botswanan, Nigeria), the DPA is involved in the decision, but not independently so, thus leaving room for political interference. In Botswana, the decision is taken by the DPA, but the final list of countries is published based on a decision of the Minister. In Nigeria, the Attorney-General is also entitled to decide in addition to the DPA. In Kenya, Mauritius and Rwanda, it is up to the controller to supply proof of adequacy (in Mauritius and Rwanda, authorization of transfers by the DPA is required). In the remaining 13 countries, the law does not specify how the decision is taken, potentially creating legal uncertainty for controllers.

4.6 Automated data processing

AU Convention

Under Article 14.5 of the AU Convention, a person shall not be subject to a decision which produces legal effects based solely on automated processing of data intended to evaluate certain personal aspects. This provision is particularly interesting in the context of digital agricultural services that are increasingly making use of data analytics for decision making, such as the use of mobile phone and other data to assess credit-worthiness of clients, smart contracts that employ blockchains for automatic contract execution, or analysis of weather data to automatically trigger insurance payouts.

National legislation

The majority of countries (20 of 32) prohibit decision-making based solely on automated processing of personal data if it has legal effects, but only 4 countries impose a similar level

of restriction as the AU Convention while the remaining 16 include certain exceptions, most commonly in cases where the processing is required to conclude or implement contracts or if the processing has been authorized by law or the DPA (Table A3 in the Appendix). Some also permit automated decision making if the data subject has given consent and/or has been informed about the processing.

Among the remaining 12 countries that do not explicitly prohibit automated decision-making, four countries allow decision-making based on automated processing, but require data subjects to be informed and/or have the right to object. Seven laws do not include provisions related specifically to automated processing. Uganda is again a special case, putting the onus on data subjects to request from the controller that decisions are not based on automatic processing. Several laws that allow (Madagascar and Nigeria) or do not cover (Botswana, Chad, Egypt and Equatorial Guinea) decision-making based on automated processing were adopted after the AU Convention was finalized.

5 Data Protection Policies of Digital Agricultural Services Providers

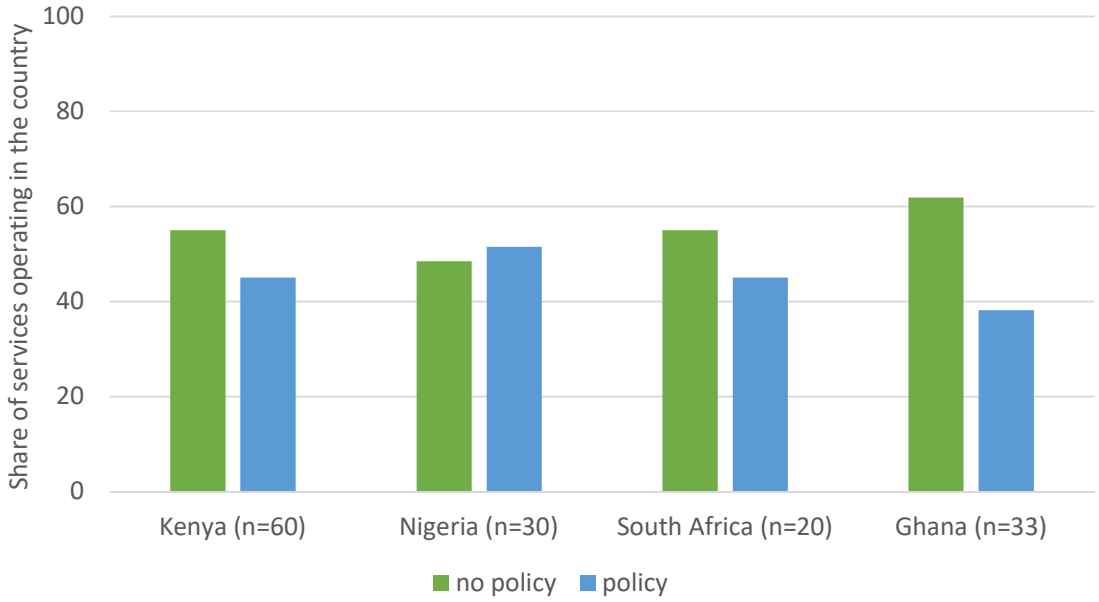
This section presents the results of a review of 106 providers that offer digitally-enabled agricultural services in Africa to assess whether data privacy policies are publicly available on the providers' website, and whether these policies adhere to the requirements of national legislation with regard to (1) the principles governing the processing of personal data and (2) users' rights to their personal data.

The availability and details of the data privacy policies were analyzed in relation to the requirements of national legislation from the relevant jurisdiction. The analysis shows that the large majority of service providers were operating in countries with legislation in place that they were required to comply with (92 percent). Regarding the *Principles* governing the procession of personal data, almost all of the relevant laws cover the six principles of the AU Convention (with the exception of Burkina Faso and Uganda). Regarding users' *rights* to personal data, almost all of the jurisdictions require the protection of the same four rights as the AU Convention (with the exception of Uganda). Given the substantial overlap between the national legislation and the principles and rights set out in the AU Convention, the provisions in the data privacy policies were compared with the provisions in the AU Convention.

5.1 Availability of privacy policies

Out of the 106 service providers, 42 providers (40 percent) publish service-related data privacy policies on their website (as of September 2021). To assess compliance of digital service providers operating in the top four most common relevant jurisdictions (see Section 3.2), the availability of privacy policies of all services operating in that country was assessed. Most services are operating in Kenya (60), followed by Nigeria (33), Ghana (30) and South Africa (20) (Figure 5). The analysis shows that the availability of privacy policies is particularly low in Ghana (with 62 percent of services not providing a policy). The second highest share is found among service providers operating in Kenya and South Africa (55 percent) while 48 percent of the service providers operating in Nigeria do not make a privacy policy available.

Figure 5: Digital services with and without privacy policies by country of operation (share)



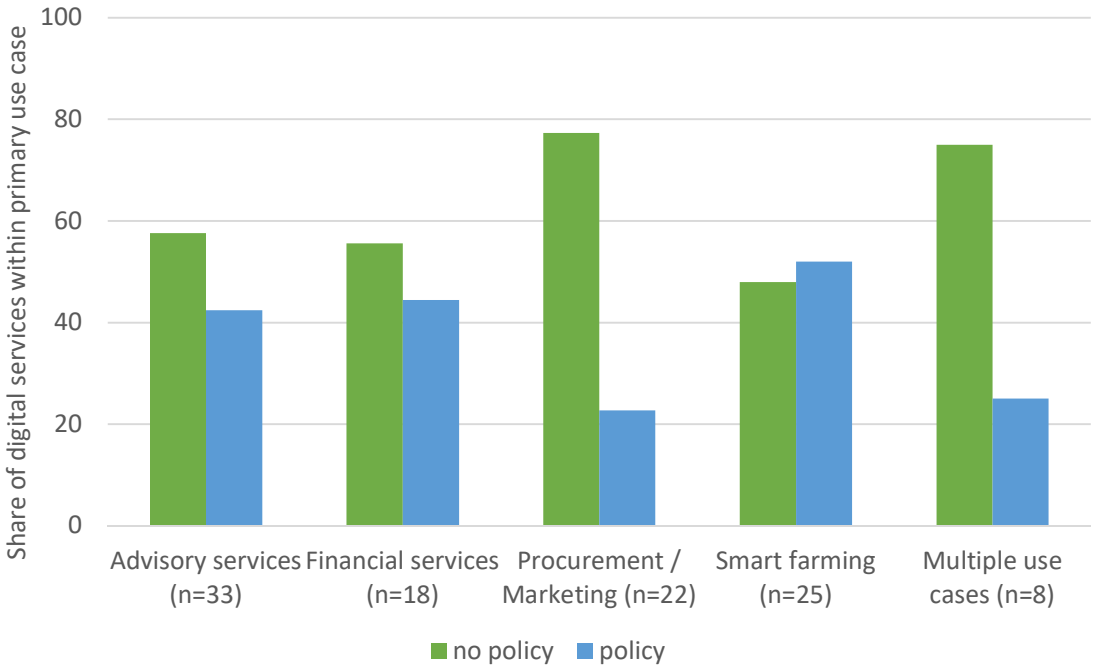
Source: Authors' own elaboration (as of September 2021).

Disaggregating the services by primary use cases also shows that for most use cases, the majority of services within each use case do not provide a policy on their website. This is particularly prevalent among services providing procurement and marketing services as well as services that offer multiple uses. Interestingly, a (small) majority of service providers in smart farming do provide a policy. This may be due to the fact that smart farming services are particularly data intensive and their functionality relies on access to data, including personal data. Thus, the companies depend on their users' willingness to supply the data and would therefore have an incentive to assure data protection.

It was not possible to ascertain whether the 64 service providers for which a data privacy policy could not be found on their websites offer related policies to registered users once they sign up to the services. Nevertheless, it can be said that the privacy policies were not readily available for potential users of the service. An assessment of relevant jurisdictions for these services shows that 92 percent are operating in countries with relevant legislation in place and are therefore required to protect the rights to personal data of their users (exceptions include services with the relevant jurisdiction of Cameroon, Côte d'Ivoire, Ethiopia, Tanzania and Zimbabwe[48]) (Figure 6).

[48] The data protection law of Zimbabwe only came into force in December 2021 and was not yet in place at the time of the analysis.

Figure 6: Digital services with and without privacy policies by primary use case



Source: Authors' own elaboration (as of September 2021).

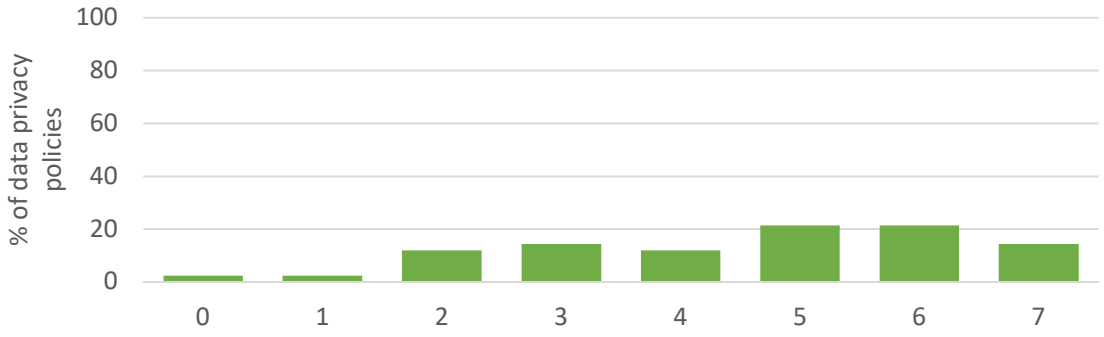
5.2 Principles governing the processing of personal data

The 42 privacy policies were analysed to determine whether the principles of the AU Convention set out in Article 13 are reflected in the policies. For the purpose of this analysis, Principle 3 of the AU Convention was divided into 'purpose', 'relevance' and 'storage' since these topics are usually dealt with separately in the policies. The Principles assessed therefore include:

(1) consent and legitimacy of personal data processing
(2) lawfulness and fairness of personal data processing
(3) purpose and relevance of processed personal data
(4) storage of processed personal data
(5) accuracy of personal data
(6) transparency of the personal data processing
(7) confidentiality and security of personal data

Out of the 42 data privacy policies that are publicly available, most cover five or six of the principles set out in the AU Convention (21 percent each) while 14 percent cover all of the principles (**Error! Reference source not found.**).

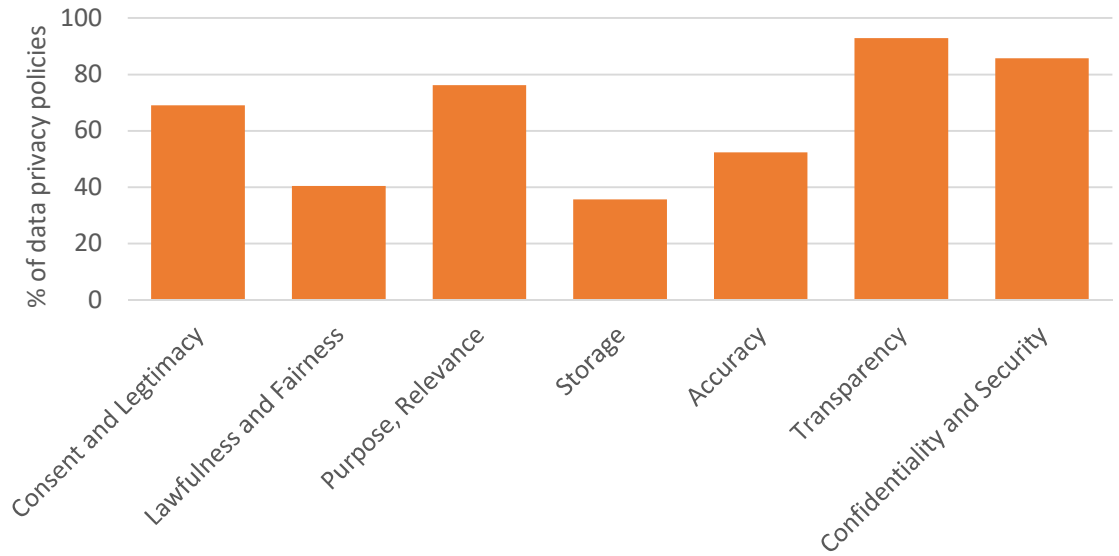
Figure 7: Number of *principles* covered by data privacy policies



Source: Authors' own elaboration (as of September 2021).

Of the seven principles assessed, the principle of *transparency*, which requires organizations to make any information relating to the processing of personal data easily accessible and clear, is most frequently covered by the privacy policies (93 percent of policies), followed by the principle of *confidentiality and security* of personal data processing (86 percent) (**Error! Reference source not found.**). The principle of *consent and legitimacy* of personal data processing and the principle that require data collection and processing to be limited to data adequate and relevant for processing for a specific *purpose*, were also found to be a common principles adhered to by 69 percent and 76 percent of the 42 privacy policies respectively. The principles that were least frequently stated in the privacy policies relate to *accuracy, lawfulness and fairness* of data processing, and *storage* of data (52 percent, 40 percent and 36 percent respectively).

Figure 8: Coverage of core data protection principles by privacy policies of digital agricultural service providers in Africa

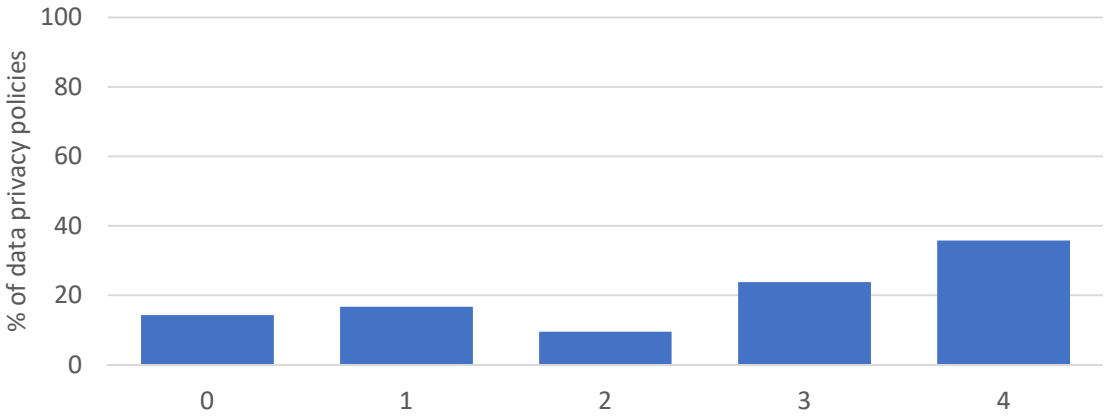


Source: Authors' own elaboration (as of September 2021).

5.3 Rights to personal data

As regards users' rights to their personal data, most of the policies include three or four rights of data subjects established by the AU Convention (24 percent and 36 percent respectively) while 14 percent did not cover any of those rights (**Error! Reference source not found.**).

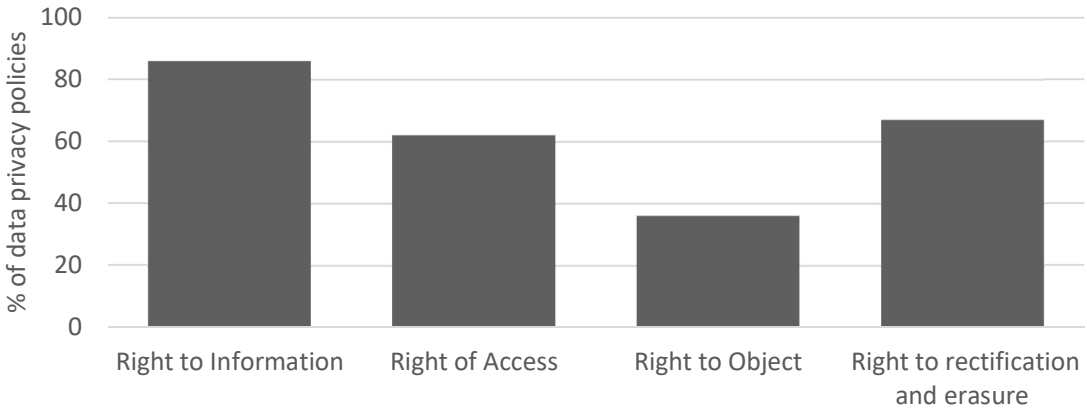
Figure 9: Number of rights covered by the privacy policies



Source: Authors' own elaboration (as of September 2021).

The most common right protected in the policies is the right to obtain *information* regarding the data collected and processed, the purpose of processing the data, and the transfer of data to third parties (86 percent pf the privacy policies; **Error! Reference source not found.**). A closer look at the type of information covered shows, however, that among those policies that include the right to obtain information, only 17 percent refer to all types of information listed in the AU Convention, while the rest only cover some types of information. A sizeable number of the privacy policies also provided users with *access* to their personal data that is collected and processed by the organization and the right to *rectify and erase* the data (62 percent and 67 percent of policies respectively). In contrast, the users' right to *object* to the processing of their data is least frequently covered by the privacy policies (36 percent).

Figure 10: Coverage of rights of data subjects in privacy policies of digital agricultural service providers in Africa



Source: Authors' own elaboration (as of September 2021).

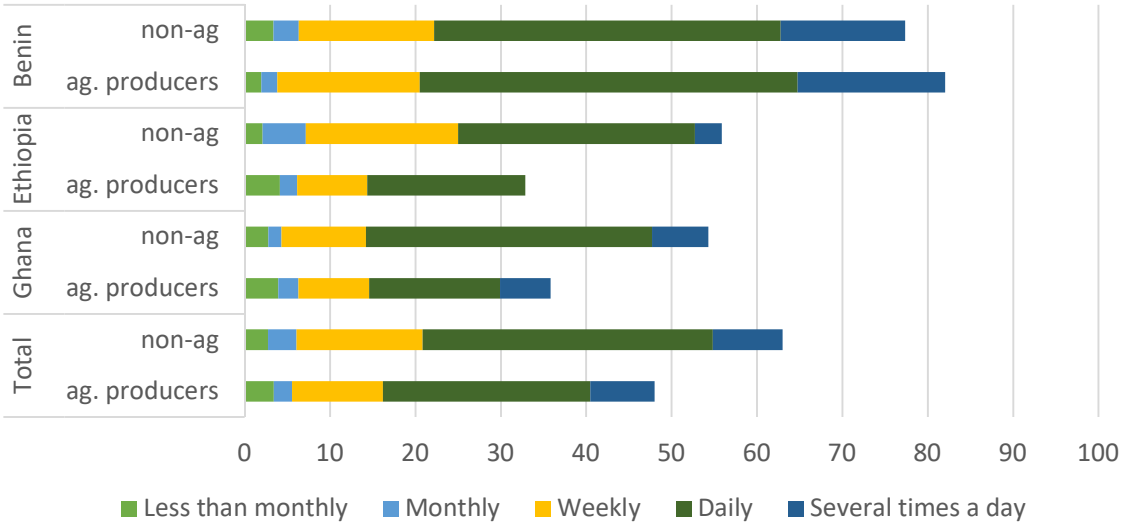
6 Agricultural producers and data protection

This section presents findings from a survey in Ethiopia, Ghana and Benin to assess the level of interest among agricultural producers to obtain information about data protection and the extent to which they are already taking steps to protect their personal data. The majority of data is likely to be shared via internet-based applications. The section therefore begins by assessing prevalence of internet use and characteristics of internet users. The subsequent analysis then focuses specially on internet users who would have access to data privacy policies via apps or websites. Responses of agricultural producers are compared with those of internet users who do not work in agricultural production.

6.1 Internet use

A sizeable share of agricultural producers (48 percent) use the internet, although less than those who do not engage in agriculture as their primary occupation (63 percent) (**Error! Reference source not found.**). Internet use is significantly lower among agricultural producers than among those who do not engage in agriculture (Table A5 in the Annex). Frequency of use is comparable between the two groups, however. Two thirds of agricultural producers use the internet once or several times per day. However, differences can be observed across countries. In Ghana and Ethiopia, internet use is less widespread among agricultural producers (19 and 23 percentage points lower respectively) and less frequent. In contrast, in Benin, the share of internet users (82 percent of agricultural producers) and the frequency of use is higher than non-agricultural users. These differences may be due to the high level of education among agricultural producers, among whom 63 percent have completed tertiary education compared to 46 percent among non-agricultural users. In the other two countries, tertiary education is less prevalent among producers than non-producers.

Figure 11: Frequency of internet use by country and agricultural profession



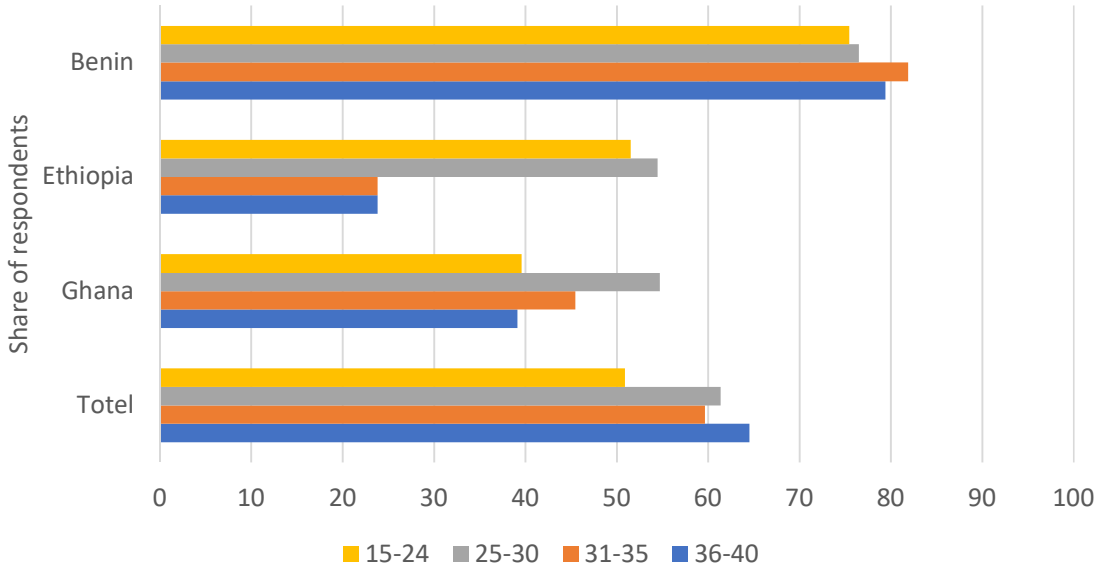
Question: In the last 12 months, how often have you been using the internet?
Source: Authors' own elaboration.

A clear gender bias in internet use can be observed. Among agricultural producers, only 21 percent of women use the internet (compared to 60 percent of men), a considerably smaller share than non-agricultural users among whom 45 percent of women (and 75 percent of men) use the internet. As a result, the sample of female internet users engaged in agriculture is very small (N=36) which does not allow for gender-disaggregated analysis.

The survey responses also show that internet use consistently increases with level of education, from just 1 percent of agricultural producers without any formal education who use the internet (compared to 10 percent among non-agricultural users) to 88 percent of those with tertiary education (86 percent among non-agricultural users). The correlation analysis results also indicate a positive correlation between internet use and education level.

Internet use is particularly low among youth producers (Figure 12). Specifically, Internet use was lowest among 15-24 year old agricultural producers (24 percent), considerably lower that non-agricultural users (57 percent). This could be due to the fact that the share of agricultural producers with tertiary education in this age group is considerable lower (13 percent) than among non-agricultural users (33 percent). For the remaining age brackets, the share of internet users ranged between 51 and 55 percent among agricultural producers (64-68 percent among non-agricultural users), with the highest share observed among the 36-40 year olds.

Figure 12: Share of internet users by age group and country



Source: Authors' own elaboration.

The mobile phone is likely to be the main channel to access the internet, given that 98 percent of agricultural producers who use the internet own a phone, followed by laptops (14 percent). Hardly any agricultural producers own a desktop computer or tablet. Social media are driving internet use; almost all internet users also use social media (99 percent of agricultural producers and non-agricultural users).

6.2 Seeking information about data protection

To find out whether respondents are actively seeking information about the use and security of their personal data, they were asked whether they have read privacy policies before providing personal data and/or have checked whether the sites through which they send personal data are secure (e.g. using https sites, a safety logo or certificate). A third of agricultural producers do one of the two or both (compared to 39 percent of non-agricultural users). Specifically, just over a third of agricultural producers (34 percent) have read privacy policy statements in the last 12 months (compared to 42 percent non-agricultural users) and 22 percent have checked whether website is secure (compared 29 percent non-agricultural users) (**Error! Reference source not found.**). According to the correlation analysis results, agricultural producers are significantly more likely to seek information about the use and security of their personal data than non-agricultural users.

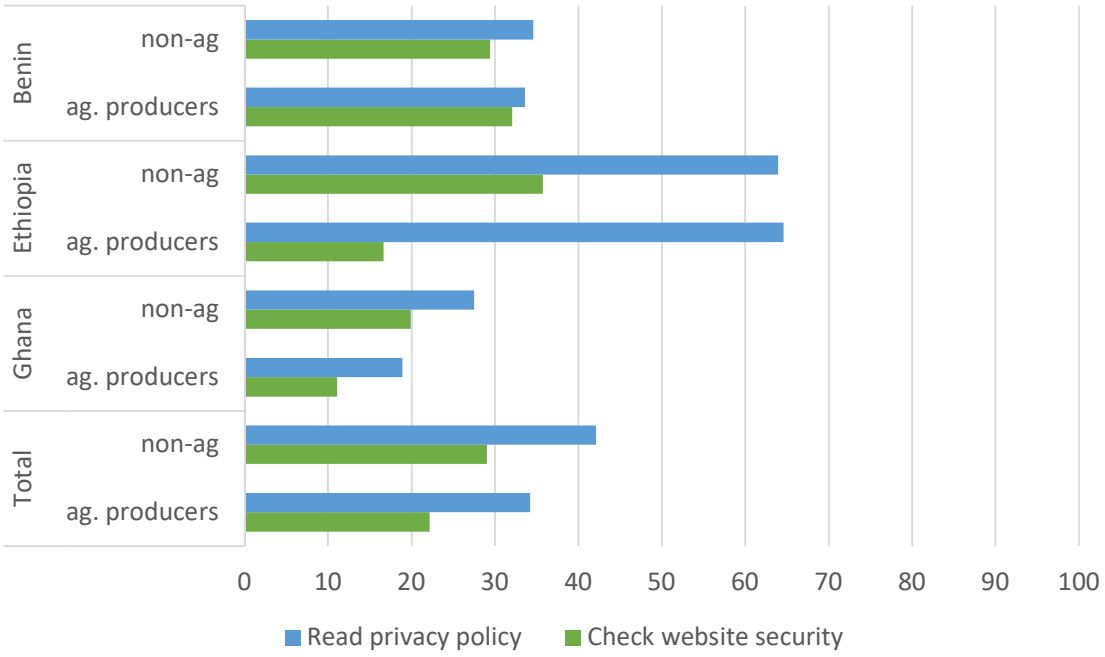
The level of education also significantly influences the likelihood to seek information about data protection (Table A5 in the Annex). Thus, while 28 percent of producers with secondary education seek such information, this share increases to 37 percent among producers with tertiary education.[49] Language constraints are also relevant. The share of respondents who read the policy is particularly low among agricultural producers who cannot read or write in English and French (15 percent). The youth appear more interested in data protection issues; a third of 25-34 year olds seek information compared to 17 percent among 35-40 year olds. [50]

A closer look at the data shows differences between countries (**Error! Reference source not found.**). Interest in data privacy policies was most prevalent in Ethiopia where almost two thirds of surveyed agricultural producers state that they read privacy policies. Just over a third of agricultural producers in Benin and only 19 percent in Ghana say they do so. The share of agricultural producers in Ethiopia who check website security is also higher than in the other countries, but not considerably so.

[49] The sample size of agricultural producers with primary education only was too small to yield meaningful results.

[50] The sample size of agricultural producers aged 15-24 was too small to yield meaningful results.

Figure 13: Internet users who seek information about data protection by country and agricultural profession



Source: Authors' own elaboration.

6.3 Control access to personal data

To assess whether users actively protect their personal data, they were asked whether they had restricted access to information about their geographical location, their profile or content on social networking sites, or personal data for advertising purposes.

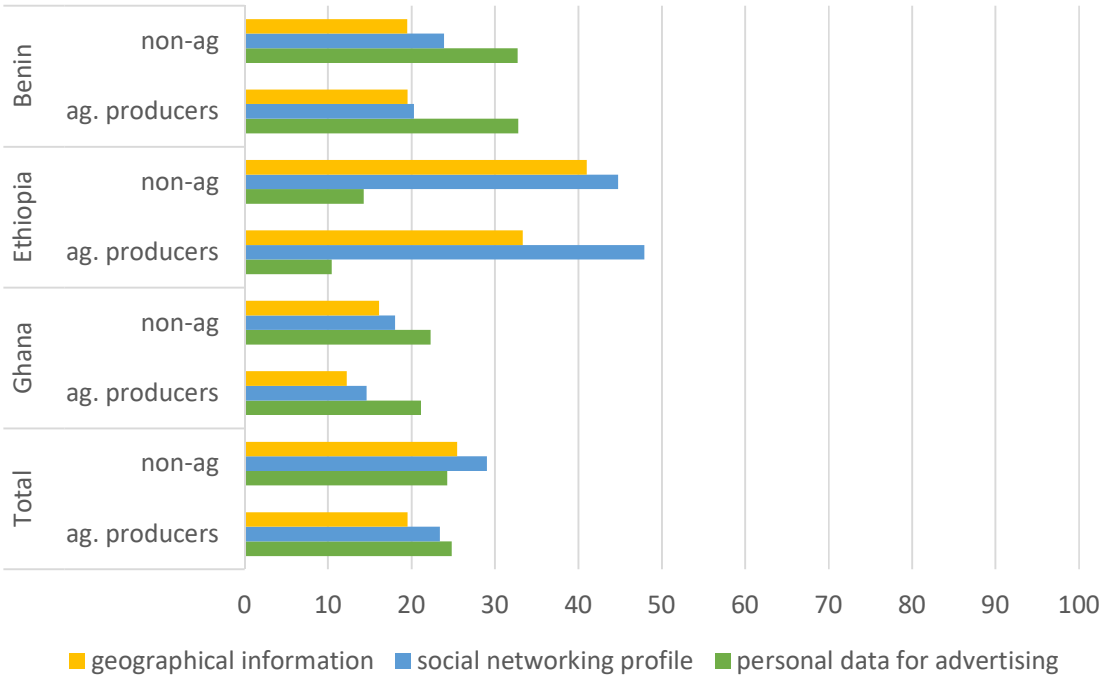
The analysis shows that 39 percent of agricultural producers (44 percent of non-agricultural users) take steps to control access to their personal data (**Error! Reference source not found.**). Almost half of those (49 percent) only restrict access to one type of data, while 31 percent restrict to two and 20 percent restrict to three types of data. The share of agricultural producers who control access to at least one type of information increases with the level of education, from 33 percent with secondary to 45 percent with tertiary education. Younger producers (i.e.) more commonly restrict access to their personal data (39 percent of 25-35 years old) than older producers (28 percent of 36-40 year olds).

Across the entire sample, results are fairly consistent across the three types of personal data and differences between agricultural producers and respondents not engaged in agriculture are not substantial. Around or less than a quarter restricted access to the different kinds of information. Restricting access to social networking profiles or content is most common (23 percent of agricultural producers). The largest difference between agricultural and non-agricultural users are related to geographical information and information shared on social networks.

Differences across countries can again be observed. Mirroring findings from the previous section, the largest share of agricultural producers to take measures to control access is found in Ethiopia (52 percent), followed by Benin (42 percent) and Ghana (28

percent). Countries also differ by the type of data most commonly restricted. While Ethiopian users more frequently restrict access to data on social networks or related to their location, users in Benin (and less prominently so in Ghana) are more concerned about access to personal data for advertising purposes.

Figure 14: Internet users who restrict access to their data by country and agricultural profession



Source: Authors' own elaboration.

7 Discussion and conclusion

While personal data protection legislation is evolving across Africa, 22 countries still do not have dedicated laws in place despite the adoption of a continent-wide Convention in 2014 and the entry into force of EU law in 2018. Even in some of the African countries that have ratified or signed the AU Convention, personal data protection laws are still forthcoming. While in some of these countries, adoption of related laws in only a question of time, others appear to be stalling.

Error! Reference source not found. summarizes the results of the comparison between the provisions of the national laws with equivalent provisions in the AU Convention. Only Côte d'Ivoire is in line with all of the Convention's provisions in the six areas assessed in this article while Uganda is the only country that diverges from the Convention in all areas. The spirit of the AU Convention is widely reflected, with its principles and rights covered by almost all of the laws. Shortcomings are found in the institutional framework needed to monitor and enforce laws which could greatly diminishes their effectiveness. Many countries have not appointed DPAs. Importantly, in several countries the DPA is not independent as set

out in the AU Convention, thus leaving room for political interference. The main gaps in the laws are found with regard to international data transfer and automated processing where the large majority of countries is less stringent than the AU Convention.

Where personal data protection laws exist, compliance with the legislation among digital agricultural service providers is low, highlighting a lack of enforcement. The majority of providers does not make a privacy policy readily available on their website even though they are required by law to provide users with information about data collection, storage and use. Where privacy polices are available, the large majority does not comply with all of the principles or protect all users' rights over their personal data set out in the national legislation. Compliance was highest among providers of smart farming solutions, although only slightly.

In the absence of data protection laws and regulatory frameworks that sufficiently safeguard farm data, the economics of data may further weaken farmers bargaining position. Generally, there is a risk that the so called 'big data divide' – which refers to the divide between the large corporations that decide on the data to be collected, possess the algorithms to process large volume of data and the expertise to interpret them, and those that do not have these capacities – could shift the power distribution within the network of stakeholders around farms. As a result, a few large corporations could end up monopolizing the sector, thereby increasing dependencies by the farmers on their services. Concerns have also been raised that personal and commercially sensitive data collected by corporations about a farm, its inhabitants and activities could be used in price discrimination and manipulation of farmer behaviour and market outcomes for the benefit of the corporations.

Despite these risks, awareness in data privacy issues among agricultural producers appears limited. Across the three countries studied, only about a third of producers surveyed actively seek information by reading the privacy policy. A slightly larger share, but still the minority is taking steps to protect their personal data. Younger people and producers with a higher level of education appear to be more aware of data protection issues and better able to control access to their data. English and French language barriers are another important constraint. This suggests that the low shares may be due to a lack of knowledge and skills rather than primarily a lack of interest. Therefore, farmers may not be demanding the protection of their data not because they are not concerned about sharing their data but rather due to their lack of awareness of the need for data protection.

Table 2: Summary of the comparison between national data protection laws and the AU Convention

Country	DPA appointed	Independent DPA	Principles covered	Rights covered	Restrictions on int. data transfer	Restrictions on automated processing
Algeria			x	x	x	
Angola	x	x	x	x	X	
Benin	x	x	x	x	X	
Botswana			x	x		
Burkina Faso	x	x		x	X	
Cape Verde	x	x	x	x		
Chad	x	x	x	x		
Côte d'Ivoire	x	x	x	x	X	x
Egypt				x	X	
Equ. Guinea				x	X	
Gabon	x	x	x			
Ghana	x		x	x		
Guinea (Con.)			x	x	X	x
Kenya	x	x	x	x		
Lesotho		x		x		
Madagascar		x	x	x		
Mali	x	x		x		
Mauritania		x	x	x		x
Mauritius	x	x	x	x		
Morocco	x		x	x		
Niger		x	x	x	x	x
Nigeria	x		x	x		
R. of Congo			x	x		
Rwanda			x	x	x	
Sao Tome & Pr.	x	x	x	x		
Senegal	x	x	x	x		
South Africa	x	x	x	x		
Togo		x	x	x		
Tunisia	x		x	x	x	
Uganda						
Zambia			x	x		
Zimbabwe	x	x	x	x		
Total	18	19	26	30	11	4

Note: 'x' means that the national laws are in line with the provisions of the AU Convention. It is important to note that the summary only shows the results for a selected number of provisions related to specific topics, not the entire laws.

Source: Authors' own elaboration (as of 23 December 2021).

The case of Ghana exemplifies the triple challenges related to legal protection, enforcement and awareness. Ghana is one of the leading countries for digital agricultural services in Africa. The country was one of the early adopters of data protection legislation (2012) and one of the few that has signed and ratified the AU Convention. However, the current law does not follow the AU Convention in several respects, including less restrictive provisions on automated processing of data and none on international data transfers. The latter two provisions would not have been as relevant at the time of adoption when digital technologies were less advanced, highlighting the need to continuously updating data protection laws in light of rapid technological changes. Thus, revisions of the Ghanaian law are needed to bring it in line with the AU Convention and adapt it to the new digital realities. Enforcement of the law is also a concern. Among the leading countries for digital agricultural solutions, Ghana has the highest share of providers that do not comply with national data protection legislation. The independence of the DPA is also not assured, potentially weakening its enforcement capabilities. At the same time, producers from Ghana appear least interested in data privacy issues among the three countries surveyed, in particular compared to Ethiopian producers where personal data protection legislation is yet to be adopted. Ghanaian producers may trust providers more with their data because of the legislation in place that they have to comply with, while in Ethiopia, data protection is the responsibility of the individual provider. Given the low compliance among digital service providers, producers should be encouraged to check the available data protection measures even where regulations are in place.

This article has a number of limitations that point to areas for future research. Due to the biased sample, the survey data offers only a preliminary insight into producers' perceptions of data protection issues. More in-depth analyses would be needed to better understand awareness of and interest in personal data protection as well as obstacles that prevent producers from taking measures to control access to their data. In addition, the article does not address the question of how to ensure that producers benefit from the use of their personal data by third parties. Further research into innovative ways to compensate producers for the use of their personal data would be required to address this question.

Finally, the article assesses only personal data protection legislation as a means to protect producers' data. The question arises whether such laws are sufficient to protect all types of farm-level data.[51] With the growth of the Internet of Things and big data analytics, the use of devices for data collection will become increasingly common, e.g. where digital agricultural service providers use soil or moisture sensors, GPS or satellites to collect producer-related data. There is a need to clarify the legal scope with regard to different types of agricultural data to ensure that measures are in place to protect producers' data, including through additional data protection tools regulated through national legislation where needed.

[51] Jouanjean (n 5).

8 Appendix

Table A1: Characteristics of the sample (%)

	TOTAL		GHANA		ETHIOPIA		BENIN	
	ag. producers N=557 (29%)	**non-ag** N=1345 (71%)	**ag. producers** N=255 (25%)	**non-ag** N=395 (75%)	**ag. producers** N=146 (23%)	**non-ag** N=477 (77%)	**ag. producers** N=156 (39%)	**non-ag** N=473 (61%)
Sex								
male	69	60	59	45	74	66	80	67
female	31	40	41	55	26	34	20	33
Age								
15-24	17	27	15	26	36	45	2	10
25-30	39	40	33	35	50	48	39	35
31-35	35	22	45	32	10	4	43	31
36-40	9	11	8	7	5	3	16	23
Education								
None	14	6	24	16	11	2	1	1
Primary	13	11	10	6	28	18	4	8
Secondary	43	44	23	25	34	29	8	16
Tertiary	29	38	15	27	16	39	63	46
Other	1	1	0	2	5	3	0	0
Internet use								
user	48	63	36	54	33	56	82	77
non-user	52	37	64	46	67	44	18	23

Source: Authors' own elaboration

Table A2: Legal provisions on data protection authorities

Country	Law(s) enacted / amended	Establish DPA	DPA Appointment Status	Independence of DPA
Algeria	2018	Established	Not appointed	no
Angola	2011, 2016	Established	Appointed	yes
Benin	2017	Established	Appointed	yes
Botswana	2018	Established	Not appointed	no
Burkina Faso	2004	Established	Appointed	yes
Cape Verde	adopted 2001, amended 2013, 2021	Established	Appointed	yes
Chad	2015	Established	Appointed	yes
Côte d'Ivoire	2013	Established	Appointed	yes
Egypt	2020	Established	Not appointed	no
Equatorial Guinea	2016	To be established by another regulation	Not appointed	unknown
Gabon	2011	Established	Appointed	yes
Ghana	2012	Established	Appointed	no
Guinea (Conakry)	2016	To be established by another regulation	Not appointed	unknown
Kenya	2019	Established	Appointed	yes
Lesotho	2011 (2013 entry into force)	Established	Not appointed	yes
Madagascar	2015	Established	Not appointed	yes
Mali	2013	Established	Appointed	yes
Mauritania	2017	Established	Not appointed	yes
Mauritius	2017	Established	Appointed	yes
Morocco	2009, 2011	Established	Appointed	no
Niger	adopted 2017, amended 2019, 2020	Established	Not appointed	yes
Nigeria	2019	Established	Appointed	no
Republic of the Congo	2019	To be established by another regulation	Not appointed	unknown
Rwanda	2021	Not established (status unclear)	Not appointed	unknown
Sao Tome and Principe	2016	Established	Appointed	yes
Senegal	2008 (2014 entry into force)	Established	Appointed	yes
South Africa	2013 (2020 entry into force)	Established	Appointed	yes
Togo	2019	Established	Not appointed	yes
Tunisia	2004	Established	Appointed	no
Uganda	2009, 2019, 2021	Established	Not appointed	no
Zambia	2009, 2021	Established	Not appointed	no
Zimbabwe	2021	Established	Appointed	yes

Source: Authors' own elaboration (as of 23 December 2021).

Table A3: Provisions related to decision-making based solely on automated processing

Country	Level of restriction	Articles	if required for contract implementation	if allowed under regulations	if authorized by DPA	additional exceptions
Algeria	Prohibited with exceptions	Article 11	x			
Angola	Prohibited with exceptions	Article 29	x		X	
Benin	Prohibited with exceptions	Article 401	x	x		
Botswana	Not covered					
Burkina Faso	Not covered					
Cape Verde	Prohibited with exceptions	Article 14	x		X	
Chad	Not covered					
Côte d'Ivoire	Prohibited	Article 25				
Egypt	Not covered					
Equatorial Guinea	Not covered					
Gabon	Prohibited with exceptions	Article 50	x			
Ghana	Allowed	Article 41	x			x
Guinea (Conakry)	Prohibited	Article 27				
Kenya	Prohibited with exceptions	Article 35	x	x		
Lesotho	Prohibited with exceptions	Article 51	x			x
Madagascar	Allowed	Article 23				
Mali	Not covered					
Mauritania	Prohibited	Article 19				
Mauritius	Prohibited with exceptions	Article 38				x
Morocco	Not covered					
Niger	Prohibited	Article 23 (Loi 2017-28)				
Nigeria	Allowed	Article 2.13.6				
Republic of the Congo	Prohibited with exceptions	Article 13	x			
Rwanda	Prohibited with exceptions	Article 21	x	x		x
Sao Tome and Principe	Prohibited with exceptions	Article 13	x	x		
Senegal	Prohibited with exceptions	Article 48	x			
South Africa	Prohibited with exceptions	Article 70	x	x		
Togo	Prohibited with exceptions	Art. 27	x			
Tunisia	Allowed	Article 37				
Uganda	Prohibited upon request	Article 27 (2019 Act), Article 28 (2021 Reg.)				
Zambia	Prohibited with exceptions	Article 62	x	x		x
Zimbabwe	Prohibited with exceptions	Article 25		x		x

Source: Authors' own elaboration (as of 23 December 2021).

Table A4: Provisions related to the international transfer of personal data

Country	Level of restriction	Articles	Exceptions to prohibition		Transfer if adequate level of protection among controllers	DPA authorization required	DPA notification required	Approval of countries
Algeria	Restricted with exceptions	Chapitre 4	x	(specified)		x		DPA
Angola	Restricted with exceptions	Article 33-34	x	(specified)		x		DPA
Benin	Restricted with exceptions	Article 391-392	x	(specified)	x	x		DPA
Botswana	Restricted with exceptions	Articles 48-49	x	(specified)	x		x	DPA (but Minister decides country list to be published)
Burkina Faso	Restricted	Article 24					x	
Cape Verde	Restricted with exceptions	Articles 19-20	x	(specified)	x		x	DPA
Chad	Restricted with exceptions	Chapter VII	x	(specified)	x		x	
Côte d'Ivoire	Restricted	Article 26				x		
Egypt	Restricted with exceptions	Chapter 7	x	(specified)	x	x		
Equatorial Guinea	Restricted with exceptions	Chapter III	x	(specified)		x		DPA
Gabon	Restricted with exceptions	Articles 94-96	x	(specified)	x			DPA
Ghana	not covered							
Guinea (Conakry)	Restricted with exceptions	Article 28	x	(specified)		x		DPA
Kenya	Restricted with exceptions	Articles 48-49	x	(specified)	x			controller must supply proof, DPA can suspend or place conditions on transfer
Lesotho	Restricted with exceptions	Article 52, 53	x	(specified)			x	
Madagascar	Restricted with exceptions	Article 20	x	(specified)	x		x	

Mali	Restricted with exceptions	Article 11			x			DPA
Mauritania	Restricted with exceptions	Section 3	x	(specified)	x			DPA
Mauritius	Restricted with exceptions	Article 36	x	(specified)	x		x	controller must supply proof, DPA can suspend or place conditions on transfer
Morocco	Restricted with exceptions	Articles 46-50	x	(specified)	x		x	DPA
Niger	Restricted with exceptions	Article 24 (Loi 2017-28)	x			x		
Nigeria	Restricted with exceptions	Sections 14-15	x	(specified)				DPA or HAGF
Republic of the Congo	Restricted with exceptions	Section 3	x	(specified)	x		x	DPA
Rwanda	Restricted with exceptions	Article 48	x	(specified)	x	x		supervisory authority
Sao Tome and Principe	Restricted with exceptions	Chapter V	x	(specified)	x			DPA
Senegal	Restricted with exceptions	Article 49-51	x	(specified)	x		x	
South Africa	Restricted with exceptions	Article 72	x	(specified)	x			
Togo	Restricted with exceptions	Articles 28-29	x	(specified)	x		x	DPA
Tunisia	Restricted	Articles 50-52					x	DPA
Uganda	Partially restricted	Section 19	x	(included by default, not as exceptions)				
Zambia	Restricted with exceptions	Articles 71	x	(specified)				
Zimbabwe	Restricted with exceptions	Article 28		(specified)	x			

Source: Authors' own elaboration (as of 23 December 2021).

Table A5: Correlation of individual characteristics with internet use, seeking information about data protection and controlling access to personal data

Variable	No. of obs. (1916)	Full sample (%)	Internet use		Chi² Test	Seeking info about data protection		Chi² Test	Controlling access to personal data		Chi² Test
			User (%)	Non-User (%)		Seeker (%)	Non-seeker (%)		Controller (%)	Non- Controller (%)	
Sex											
Male	1202	63	70	30	181.1***	40	60	9.9***	46	54	6.8***
Female	714	37	39	61		30	70		37	63	
Age											
15-24	462	24	51	49	16.9***	47	53	16.1***	51	49	7.1*
25-30	758	39	61	39		39	61		43	57	
31-35	493	26	60	40		34	66		40	60	
36-40	203	11	65	35		27	73		40	60	
Education											
None	156	8	6	94	508.2***	33	67	18.9***	33	67	15.8***
Primary	218	11	24	76		31	69		31	69	
Secondary	835	44	56	44		32	68		39	61	
Tertiary	678	35	86	14		44	56		48	52	
Other	28	2	36	64		20	80		20	80	
Occupation											
Agricultural	557	71	48	52	36.3***	33	67	3.4*	39	61	2.0
Non-agricultural	1345	29	63	37		39	61		44	56	

Source: Authors' own elaboration