KONRAD ADENAUER STIFTUNG

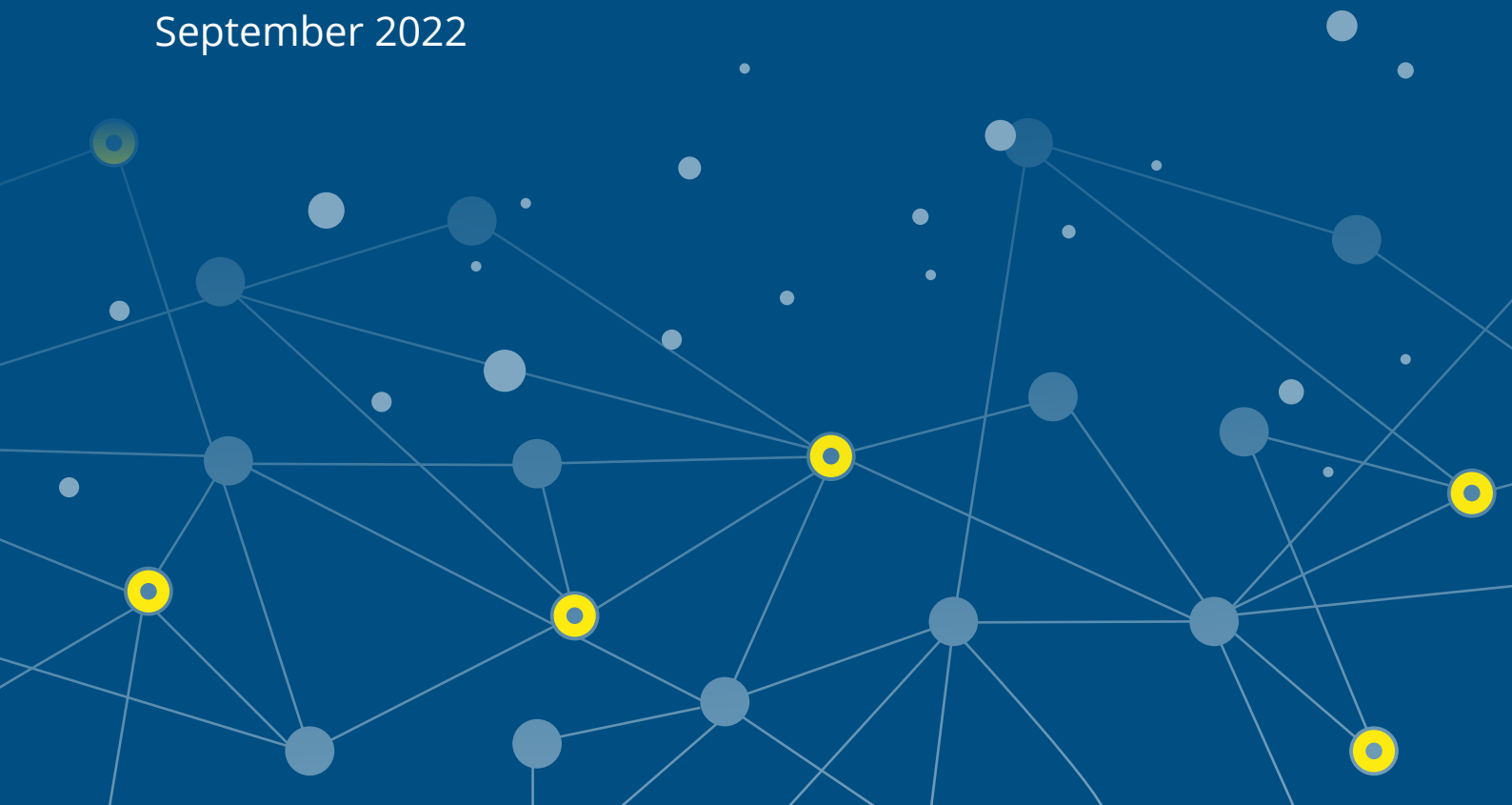
RULE OF LAW PROGRAMME
MIDDLE EAST AND NORTH AFRICA

Data Protection Laws in Northern Africa

Regulatory Approaches, Key Principles, Selected Documents

Dr. Patricia Boshe
Prof. Moritz Henneman

September 2022



KONRAD ADENAUER STIFTUNG
RULE OF LAW PROGRAMME
MIDDLE EAST AND NORTH AFRICA

Data Protection Laws in Northern Africa

– Regulatory Approaches, Key Principles, Selected Documents –

Dr. Patricia Boshe
and
Prof. Dr. Moritz Hennemann

September 2022

Foreword

"Data is the new gold!"; and much like gold, once discovered, there is a rush – to collect and use it, for marketing, trade, national security and defense, surveillance, and other manifold reasons, by both the public and private sector. While being useful, processes of data collection, processing and storing also pose a serious threat to basic human rights and freedoms. Data subjects are under an ever-growing risk of having their data misused, accounts hacked, and personal information unwillingly being turned against themselves. How can legislation protect the data of individuals in times of "mass social media", "big data", "legal tech" and "artificial intelligence"? How can legislation remain flexible and up to speed during the ever so quick developments of data technology?

Data protection regulations are growing worldwide in number and complexity. In Africa, until August 2022, 34 out of 55 countries had comprehensive data protection laws, 8 countries had bills and 24 countries had data protection authorities, with more to be expected. While their enforcement is often limited, the legal frameworks for data protection are slowly but surely being put in place. This also applies to the North African countries. While Libya and Sudan have yet to develop respective data protection regulations, Algeria, Egypt, Mauritania, Morocco and Tunisia all passed comprehensive data protection laws. These five laws share a similar approach and can also be compared to the EU General Data Protection Regulation (GDPR), as the framework offers similar basic standards and data protection values. However, many differences remain, also between the North African countries themselves, each having to consider their national legislative frameworks and requirements.

How have these countries designed their data protection laws, what does the 'law in the books' lay out? Which commonalities and differences can be identified, where do loopholes (continue to) exist?

As the Konrad-Adenauer-Stiftung Rule of Law Programme Middle East & North Africa (KAS), it was of paramount importance to us to have this thorough comparative study carried out in order to also be able to tackle the regional legal aspects of data protection implementation.

On behalf of the KAS, I would like to thank our authors, Prof. Dr. Moritz Hennemann and Dr. Patricia Boshe, for all their thorough and tireless efforts in researching and writing this study. It is sure to be a groundwork of more valuable research and findings on data protection laws in North Africa in the future.

Beirut, September 2022

Philipp Bremer

Director of the Konrad-Adenauer-Stiftung Rule of Law Programme Middle East & North Africa

Preface by the authors

This report provides an in-depth overview of the current state and trends of data protection regulation of seven North African countries – namely Algeria, Egypt, Mauritania, Morocco, Libya, Sudan, and Tunisia. The study tackles regulatory approaches, key principles, and selected instruments. The analysis was limited from the start to a textual analysis of the data protection laws including constitutional law (the "law in the books").

In detail, we have also engaged with the development and status of regional and sub-regional data protection frameworks in Africa. Political as well as international influences on the development (or the lack of) of data protection laws in North Africa were also considered. For countries with comprehensive data protection laws (i.e. Algeria, Egypt, Mauritania, Morocco, and Tunisia), the comparative assessment also looked into the scope of alignment and of divergence with the EU General Data Protection Regulation.

First and foremost, we thank the Konrad-Adenauer-Stiftung Rule of Law Programme for the possibility to conduct this study. The study was written mainly during the first half of 2022, although we have also integrated references to later developments (especially, but not only, the AU Data Policy Framework). Maximilian Heldt conducted research for and made small contributions to it (especially with regard to the respective political developments). We are extremely grateful for his thorough assistance.

Passau, September 2022

Dr. Patricia Boshe

Prof. Dr. Moritz Hennemann

Executive Summary

This report provides an in-depth overview of the current state and trends of data protection regulation of seven North African countries – namely Algeria, Egypt, Mauritania, Morocco, Libya, Sudan, and Tunisia. The study tackles regulatory approaches, key principles, and selected instruments of the aforementioned states. In detail, we have engaged with the development and status of regional and sub-regional data protection frameworks in Africa. Political as well as international influences on the development (or the lack of) of data protection laws in North Africa were also considered. For countries with comprehensive data protection laws (i.e. Algeria, Egypt, Mauritania, Morocco, and Tunisia), the comparative assessment also looked into the scope of alignment and of divergence with the EU General Data Protection Regulation (GDPR). The analysis was limited to a textual analysis of the data protection laws including constitutional law (the "law in the books").

Other than Egypt, the data protection laws in four countries analysed in this report were adopted before the GDPR. Given their similarities to the EU data protection framework, it is safe to assume that the laws in the four countries were influenced by the 1995 EU Data Protection Directive which was replaced by the GDPR. This being the case, there is a need to revisit these laws to determine their robustness in light of the current technological and legal development(s) beyond the region.

In Libya and in Sudan, no reforms in the data protection field have happened in the period when other African countries were reforming. The main reason is that the two countries are prone to internal civil and political unrest. Nevertheless, given the political and economic pressure on the need to protect personal data, it is possible to see reforms in a very near future. Given the involvement of the EU in the area and the extra-territorial application of the GDPR, it is possible that any reform would follow the suit of the other North African countries with an adoption of a law / establishment of a data protection framework similar to the EU data protection framework (despite – arguably – shortcomings of the EU legislation in substance).

Our analysis shows that data protection laws in Algeria, Egypt, Mauritania, Morocco, and Tunisia are based on common approaches. The laws in the five countries resemble the GDPR rather closely. The laws adopted (more or less similar) the basic standards and data protection values similar to those found in the GPDR as well as – partly – in the 1995 EU Directive. This is for example the case with regard to the scope of protection (i.e. omnibus laws that apply to private and public institutions).

Nevertheless, divergences exist – such as compulsory registration of the data controllers, the omission of the 'transparency principles', or the judge's power to give consent on behalf of a minor in Tunisia and Algeria. These divergences might underline local needs and legal culture in general.

In addition, and especially, a transfer of data subject rights to heirs is an aspect that is not explicitly present in the EU data protection framework – neither in the GDPR (which leaves this question to the EU member states) nor in the previous Directive. In Algeria, Mauritania, and Tunisia, family members of a deceased person can 'inherit' and enforce data protection rights of the deceased. This aspect can potentially be considered as an important fragment of African approaches to data protection enforcement and legal culture.

Also, despite sharing the same core data principles and similar enforcement frameworks, we do see enforcement challenges across the region (and beyond). Private enforcement also seems to be limited.

Lastly, none of the five countries have received an EU adequacy decision, despite the similarities in the legal content of their laws to that of the GDPR. It is clear from Article 45(2) GDPR that a country – if it wants a respective decision – needs to go beyond approximating the GDPR (or any other data protection legal framework). The adequacy assessment of a data protection framework looks beyond the mere legal text.

Finally, the report stresses the need to promote cooperation between data protection authorities. As a first step, a deeper cooperation between DPAs and legislators in the development and enforcement of data protection laws could be an option to proceed.

Any created harmonised legal framework across the region should also bear the compatibility of such a framework with other regional and international data protection frameworks in mind. The recently adopted African Union Data Policy Framework whose objective is to create a policy framework to support 'a consolidated data environment and harmonised digital data governance systems' may be just the right step towards resolving these disparities.

This will potentially enhance harmonious implementation of the laws across the region. This in turn will also ensure the sharing of the best practice among the authorities, promote mutual trust, and support a trusted free flow of data across borders – thereby also contributing to the growth of the data economy in North Africa and beyond.

Table of Contents

Table of Statutes and Conventions

African Union

African Commission on Human and Peoples' Rights, The African Union Data Policy Framework, EX.CL/Dec.1144 X endorsed in February 2022, Addis Ababa.

African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, adopted on the 65th Ordinary Session of 10 November 2019 in Banjul, Gambia.

African Commission on Human and Peoples' Rights, Convention on Cyberspace Security and Protection of Personal Data, adopted on the 23rd Ordinary Session of the Assembly of 27th June 2014, Malabo.

Organisation of African Union, African Charter on the Rights and Welfare of the Child, CAB/LEG/24.9/49, entered into force on 11 July 1999, Addis Ababa.
Organisation of African Union, African Charter on Human and Peoples' Rights OAU Doc. CAB/LEG/24.9/49, entered into force on 29 Nov. 1999, Banjul.

Algeria

Loi n° 18-07 du 25 Ramadhan 1439 Correspondant au 10 Juin 2018 Relative à la Protection des Personnes Physiques dans le Traitement des Données à Caractère Personnel.

Loi n° 15-12 du 28 Ramadhan 1436 Correspondant au 15 Juillet 2015 Relative à la Protection de l'Enfant.

Décret Présidentiel n° 22-187 du 17 Chaoual 1443 Correspondant au 18 Mai 2022 Portant Nomination du Président et des Membres de l'Autorité Nationale de Protection des Données à Caractère Personnel.

Egypt

Consumer Protection Law, Law No. 181 of year 2018.

Personal Data Protection Law, Law No. 151 of 2020.

The Media and Journalism Law and Decree No. 418 of 2020, 16 February 2020.

East African Community

UNCTAD / EAC, Draft EAC Legal Framework for Cyber Laws – Phase I, November 2008.

Economic Community of Central African States (ECCAS)

Data Protection Model Law / Directive No. 07/08-UEAC-133-CM-18.

Economic Community of West African States (ECOWAS)

ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection, Abuja 16.2.2010.

European Union

Proposal of the Data Act by the EU Commission, COM (2022), 68 final.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Mauritania

Ordonnance n° 2006-015 du 12 Juillet 2006 Portant Institution d'une Commission Nationale des Droits de l'Homme.

Loi n°2016-006 Portant loi d'Orientation sur la Société Mauritanienne de l'Information.

Loi n°2016-007 sur la Cybercriminalité.

Loi n° 2017-020 sur la Protection des Données à Caractère Personnel.

Loi n°2018-022 sur les Transactions Électroniques.

Libya

Telecommunication Law, Law No. (22) of 1378 FDP (2010 AD).

Morocco

Loi n° 09-08 Relative à la Protection des Personnes Physiques à L'égard du Traitement des Données à Caractère Personnel.

Southern African Development Community (SADC).

SADC Data Protection Model Law of 2012.

Sudan

Miscellaneous Amendments (Repeal or amend the provisions restricting freedoms) Law No.12 of 2020.

The Law of the Commission for the Reform of the Legal and Justice System, Law No. (13) of 2020.
Telecommunication Act of 2001.

The Child Act of 2010.

Tunisia

Loi Organique Numéro 63 en Date du 27 Juillet 2004 Portant sur la Protection des Données à Caractère Personnel.

United Nations

UN General Assembly, Universal Declaration of Human Rights, A/RES/217, UN-Doc. 217/A-(III) of March (1948).

UN General Assembly, International Covenant on Civil and Political Rights, U.N.T.S. Vol. 999, 171 (1966).

UN Commission on Human Rights, Convention on the Rights of the Child, E/CN.4/RES/1990/74 of March 1990, Geneva).

Abbreviations

ACHR - The Arab Charter on Human Rights
ACRWC - African Charter on the Rights and Welfare of the Child
AFAPDP - L'Association Francophone des Autorités de Protection des Données Personnelles
AMU - Arab Maghreb Union
APDP - L'Autorité de Protection des Données à caractère Personnel
AU - African Union
CACF - China-Africa Consultative Forum
CBL - Central Bank of Libya
CCTV - Closed Circuit Television
CDR - Constitutional Democratic Rally
CEMAC - Economic and Monetary Community of Central Africa
CEN-SAD - The Community of Sahel-Saharan States
CIL - Commission de l'Informatique et des Libertés
CLTG - Civilian-Led Transitional Government
CNDP - Commission Nationale de Protection des Données Personnelles
CoE - Council of Europe
CRC - Convention on the Rights of the Child
DCFTA - Deep and Comprehensive Free Trade Area
DCFTA - Deep and Comprehensive Free Trade Area
DPA - Data Protection Authority
ECCAS - Economic Community of Central African States.
ESCWA - United Nations Economic and Social Commission for Western Asia
EU - European Union
EURO-MED – European and Mediterranean Agreement
FREDI - Forschungsstelle für Rechtsfragen der Digitalisierung
GDPR - The General Data Protection Regulation
GNU - Government of National Unity
HAPDP - Haute Autorité De La Protection Des Données À Caractère Personnel
HoR - Libyan House of Representatives
ICCPR - International Covenant on Civil and Political Rights
ICT- Information and Communications Technology
IGAD - The Intergovernmental Authority on Development
IGAD - The Intergovernmental Authority on Development
INPDP - l'Instance Nationale de Protection des Données à Caractère
L'ANSICE - Agence Nationale de Sécurité Informatique et de Certification Électronique
LNA - Libyan National Army
LPDF - Libyan Political Dialogue Forum
MENA - The Middle East and North Africa region
NADPA-RAPDP - Network of African Data Protection Authorities/Réseau Africain des Autorités de Protection des Données Personnelles
NISSA - National Information Security and Safety Authority
OECD - The Organisation for Economic Co-operation and Development
RECs – Regional Economic Community
TMC - Transitional Military Council (in Libya)
TMC - Transitional Military Council (in Sudan)
UDHR - Universal Declaration of Human Rights
UNITAMS - The United Nations Integrated Transition Assistance Mission in Sudan
UNITAMS - United Nations Integrated Transition Assistance Mission in Sudan

1 Introduction

This report analyses data protection laws – their status and future prospects – of North African countries, namely Algeria, Egypt, Libya, Mauritania, Morocco, Sudan, and Tunisia.[1] The following brief overview of the state of data protection laws in Africa paves the way to the analysis. The overview is based upon the general observation that data protection regulation in Africa is growing. At the time of writing the report (August 2022), 34 countries out of 55 countries have comprehensive data protection laws, 8 countries have bills and 24 countries have data protection authorities (DPAs)[2]. Enforcement of these laws is often limited mainly because of financial and institutional challenges.[3]

1.1 Data Protection at African Union / Regional Economic Communities Level

At the continental level, three instruments provide frameworks for data protection: (1) the Convention on Cyber Security and Personal Data Protection (Malabo Convention)[4], (2) the African Declaration on Internet Rights and Freedoms[5], and (3) the Declaration of Principles on Freedom of Expression and Access to Information in Africa[6]. The Malabo Convention (chapter 2) and the Declaration of Principles on Freedom of Expression and Access to Information (principles 40-42) provide a common data protection framework. The African Declaration on Internet Rights and Freedoms provides a framework for the protection of personal data on the internet.

Data protection principles provided in the two Declarations mentioned above are similar with those in the EU General Data Protection Regulation (GDPR)[7].[8] These being

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimisation;
- data accuracy;

[1] The study is based upon pre-published research projects of the authors, cf. Hennemann/Boshe/von Meding, Datenschutzrechtsordnungen in Afrika – Grundlagen, Rechtsentwicklung und Fortentwicklungspotenziale, ZfDR 2021, 193; Boshe/Hennemann/von Meding, African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward, GPLR 3 (2022), 56 (English version); FREDI, Global Data Law Maps: Africa and Malabo Convention (2022).

[2] Zimbabwe is added to the list of countries with Data Protection Laws; and Algeria, Botswana, Uganda, Mauritania, Nigeria, Tunisia and Zimbabwe as countries with newly established Data Protection Authorities; cf. for details Boshe/Hennemann/von Meding, African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward, GPLR 3 (2022), 56 (60); FREDI, Global Data Law Maps: Africa (2022).

[3] Ilori, Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions.

[4] Adopted by the 23rd Ordinary Session of the Assembly of the Union, Malabo, 27th June 2014.

[5] Adopted by the African Commission on Human and Peoples' Rights (ACHPR), 2016.

[6] Adopted by the 65th Ordinary Session of the Africa Union Commission held from 21 October to 10 November 2019, Banjul, The Gambia.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

[8] See Article 42 of the Declaration of Principles on Freedom of Expression and Access to Information, and pp. 21-23 of the African Declaration on Internet Rights and Freedoms.

- storage limitation;
- integrity and confidentiality;
- accountability.

The Malabo Convention is, however, missing one leading principle, the accountability principle.

Among the three frameworks, it is only the Declaration of Principles on Freedom of Expression and Access to Information that has a binding force.[9] The Malabo Convection is yet to come into force due to lack of a sufficient number of ratifications by member states.[10] Furthermore, at the time of writing this report, the African Union had issued a tender for the review of the Malabo Convention.[11]

In addition to national and continental frameworks for data protection, four regional data protection frameworks exist. These include the SADC Model Law[12], ECOWAS supplementary Act[13], EAC Framework for Cyberlaws[14], and ECCAS / CEMAC Model Law[15]. The four frameworks are established within respective Regional Economic Communities (RECs). The ECOWAS is the only binding data protection framework.[16] SADC, ECCAS / CEMAC Model Laws are soft laws with no binding force to member states. The EAC Framework is a set of recommendations – also with no binding force to member states.[17]

The Malabo Convention and the RECs frameworks for the protection of personal data are generally influenced by interregional frameworks, especially EU data protection frameworks (the former EU Data Protection Directive[18] and the current GDPR) as well as the Council of Europe Data Protection Convention 108 and 108+.[19] As early as 2001, a study by the European Parliament revealed that the EU support in Africa is focusing on 'regulamentary issues' as opposed to ICT infrastructure development as in the case

[9] The Declaration was adopted to modify and re-enforce article 9 of the African Charter on Human and Peoples' Rights (ACHPR). All African countries are party to and bound by the ACHPR. This gives the Declaration a binding force.

[10] According to Article 26 of Malabo Convention, to come into force, at least 15 AU member states must ratify (sign and deposit the instrument with the AU Commission) the Convention. As of August 2022, only 14 countries had ratified the Convention.

[11] Consultancy Services to Review the Malabo Convention on Cyber security and Personal Data Protection and Recommend Possible Amendments to Articles, Tender issued by the African Union on 17 June 2022.

[12] SADC Data Protection Model Law of 2012.

[13] ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection, Abuja 16.2.2010.

[14] UNCTAD / EAC, Draft EAC Legal Framework for Cyber Laws – Phase I November 2008.

[15] ECCAS adopted it as a Model Law, while CEMAC released Draft Directives on Cybersecurity, Directive No. 07/08-UEAC-133-CM-18. Cf. Boshe/Hennemann/von Meding, supra n. 1 at pp. 13-14 et seq.

[16] The ECOWAS Act is annexed to and forms an integral part of the ECOWAS Treaty. See article. 48. Consequently, a violation of the ECOWAS Act by member states can be enforced by the ECOWAS Court of Justice.

[17] Cf. Boshe/Hennemann/von Meding, supra n. 1 at p. 66 et seq.

[18] Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

[19] See Makulilo "One size fits all": Does Europe Impose its Data Protection Regime on Africa?' Datenschutz und Datensicherheit 37 (2013); Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, 24 Stan. Tech. L. Rev. (2021) 389 (407); Daigle, Data Protection Laws in Africa: A Pan-African Survey and Noted Trends, Journal of International Commerce and Economics, (2021), p. 2; Finley et al., 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).

of support offered to Latin America, Asia, and the Mediterranean countries.[20] This support in Africa includes financial support[21] as well as capacity building programmes.[22] The above mentioned study suggests that African countries 'look upon the EU as a model' in developing information society.[23] The claim is that the 'European vision of the Information Society is more likely closer than the American one, particularly as regards Asian and African culture'.[24]

The fact that Africa relies heavily on 'borrowed' data protection framework is also stated by the African Union Data Policy Framework (hereinafter 'the Framework').[25] The Framework was adopted in February 2022 with a vision of 'creating a consolidated data environment and harmonised digital data governance systems to enable the free and secure flow of data across the continent.'[26] Noting that data regulation in Africa heavily relies on imported standards, it suggests the need for coordinated action by Africans to change this narrative and place Africa in a position of a 'policy standard maker'.[27]

1.1 Development on the National Level in Africa

Africa has witnessed an unprecedented growth in data protection regulation since the coming of the GDPR. In 2016, when the GDPR was adopted, 17 out of 54 African countries had data protection laws[28]. This was 15 years after the first African country[29] adopted a comprehensive data protection law. By August 2022, 34 African countries had data protection laws[30] and 8 had bills or draft bills[31] in place. The laws adopted and amended / revised after the adoption of the GDPR in 2016 'align closely with the regulatory standards of GDPR'.[32] Among other things, this growth is assumed to result from the prospect of

[20] European Parliament - Directorate General for Research, Developing Countries and the ICT Revolution, March 2001:

[21] Ibid.

[22] Ibid, p. 37.

[23] European Parliament - Directorate General for Research, supra n. 20 at p. 38 et seq.

[24] Ibid, p. 39.

[25] The Framework was endorsed by the Executive Council of the AU in Decision EX/CL/Dec. 1144(XL) in February 2022.

[26] See the Framework on the foreword, pp. 3, 5, 13, 18 and 35-40.

[27] Ibid, p. 17.

[28] Cape Verde (2001, amended in 2013 and in 2021), Seychelles (2003), Burkina Faso (2004, under revision), Mauritius (2004, amended in 2017), Tunisia (2004, under revision), Senegal (2008, under revision), Benin (2009, amended in 2017), Morocco (2009, under revision), Angola (2011), Gabon (2011), Lesotho (2011), Ghana (2012), Ivory Coast (2013), Mali (2013, amended in 2017), South Africa (2013), Madagascar (2014), Chad (2015). Cf. Boshe/Hennemann/von Meding, supra n. 1 at p. 60.

[29] Cape Verde is the first African country to adopt data protection law in 2001, the Data Protection Law (No. 133/V/2001); cf. Boshe/Hennemann/von Meding, ibid.

[30] In addition to the above list (cf footnote 28) other countries with data protection laws are Equatorial Guinea (2016), São Tomé and Principe (2016), Guinea (Conakry) (2016). Mauritania (2017), Niger (2017), Algeria (2018), Botswana (2018), Nigeria (Data Protection Regulation 2019), Uganda (2019), Kenya (2019), Congo-Brazzaville (Republic of Congo) (2019), Togo (2019), Egypt (2020), Rwanda (2021), Zambia (2021), Zimbabwe (2021) and the Kingdom of Swaziland (Eswatini) (2022).

[31] Comoros (2014), Ethiopia (2009), Malawi (2021), Namibia (2020), Nigeria (2020) (the Bill is in addition to the current Data Protection Regulation), South Sudan (2021),), and Tanzania (2021). (See Boshe/Hennemann/von Meding, supra n. 1.

[32] Daigle, supra n. 19 at p. 8 et seq.

an adequacy decision (Article 45 GDPR) as well as from Article 3 of the GDPR.[33] Adequacy decisions are pronouncements made by the European Commission recognizing a country, a region, territory, or an organisation outside Europe as providing equivalent level of protection to personal data as the European data protection framework does; this means that personal data from EU countries can be transferred to such a country / territory / international organisation without special restrictions or further safeguards. According to the latter, the GDPR especially applies to all persons targeting the EU market (Article 3(2)(a) GDPR). Data protection scholar Justin Bryant believes that Article 3(2)(a) GDPR has intensified the pressure on third countries to 'either adopt or approximate EU standards.'[34]

Nevertheless, despite EU influence on data protection in Africa, data protection policies vary significantly across the continent.[35] Also, the adoption / approximation of the GDPR in African countries has not (yet) led to an adequacy decision (Article 45 GDPR) from the EU.

1.2 The Situation in Northern Africa

North African states' membership to RECs overlaps between two RECs. Algeria, Libya, Mauritania, Morocco, and Tunisia are members of the Arab Maghreb Union (AMU). Mauritania, Morocco, Tunisia together with Egypt and Sudan are also members of the Community of Sahel-Saharan States (CEN-SAD). The two RECs have no data protection frameworks. In addition, Algeria, Egypt, Libya, Morocco and Tunisia are part of the Middle East and North Africa (MENA) region. There is no specific data protection framework for the MENA region either. A research commissioned by the World Bank describes digital regulation in MENA as underdeveloped and outdated; only a few countries have advanced digital regulations.[36] Regardless, the research noted the existence of comprehensive and up-to-date regulatory frameworks in Morocco and Tunisia.[37]

A notable initiative towards a harmonised data protection framework involving North African countries is driven by the United Nations Economic and Social Commission for Western Asia (ESCWA). The purpose of the initiative is to promote the enactment of, as well as, to enhance and harmonise ICT laws by member states. Members of the ESCWA include Algeria, Egypt, Libya, Morocco, Sudan, and Tunisia. In 2007, ESCWA started a cyber legislation initiative[38], and in 2012, it released cyber law directives. Among these

[33] Cf. Hennemann, Wettbewerb der Datenschutzrechtsordnungen – zur Rezeption der Datenschutz-Grundverordnung, RabelsZ 84 (2020) 864.

[34] Bryant, supra n. 19.

[35] Daigle, supra n. 19.

[36] Jaller/Molinuevo, Digital Trade in MENA Regulatory Readiness Assessment – Policy Research Working Paper, March 2020, p.2.

[37] Ibid.

[38] The project was named, 'the Regional Harmonization of Cyber Legislation to Promote the Knowledge Society in the Arab World'. Cf. UN-ESCWA, The ESCWA Cyber Legislation Digest, 2013.

directives is a directive on personal data protection. The ESCWA Directive 4 "The Processing and Protection of Personal Data" provides for a model data protection framework for member states. The Directive emulates the 1995 EU Directive[39] and the OECD Guidelines[40].

Economically, North Africa is Europe's biggest trade partner. It is 'separated' from the rest of Africa through the European Neighborhood Policy and the EURO-MED Agreements[41]. North Africa provides half of all Africa's trade with Europe.[42] The partnership, however, does not create a concrete framework for the protection of personal data. But, within the EURO-MED Agreements, respective parties are required to take necessary measures to protect personal data. In this respect, the Agreement suggests for the approximation of data protection laws of specific North African countries to the EU laws in order to support trade exchange.[43] The Agreement with Morocco includes an Annex with fundamental principles applicable to data protection and rights of a data subject. These resemble the principles enshrined in the 1995 Data Protection Directive and the GDPR.[44] The Agreement also contains a provision on assisting Morocco to approximate EU laws to support free trade.[45] Similar provisions are provided in the Egypt - Euro-Mediterranean Association Agreement[46] and the Tunisia - Euro-Mediterranean Association Agreement[47]. Libya is yet to conclude a similar Agreement with the EU.[48] Mauritania and Sudan have no such agreement with the EU.

In 2020, the EU released a renewed partnership with the EU southern neighbours, which include North African countries.[49] According to the renewed Agreement, '[t]he EU will continue to engage with partner countries to ensure a high level of protection of the fundamental rights to privacy and data protection

[39] The ESCWA Cyber Legislation Digest, 2013.

[40] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). See also Fatafta/Samaro, Exposed and Exploited: Data Protection in the Middle East and North Africa, January 2021, pp. 4-5.

[41] These are series of agreements between Europe and neighbouring countries at the Mediterranean coast. Through the EURO-MED agreements, North Africa and Europe created a free trade area allowing free movement of goods between them.

[42] Dieye, Assessing Trade Relations Between Africa and Europe in Abimbola/Aggad (Eds), Towards a Policy fit for Purpose between Africa and Europe, APRI – 2021, pp. 17-18.

[43] See Article 2, 6 56 of the Algeria - Euro-Mediterranean Association Agreement.

[44] In additional to the Annex, Articles 10 (1) (2), 14 of the Agreement also requires Morocco to adhere to confidentiality of data shared.

[45] Ibid, Article 52.

[46] Article 48 on approximation of laws and Articles 10 and 13 requiring equivalent data protection to any information shared.

[47] Article 52 on approximation of laws and Articles 10, 14 and the Annex contain data protection principles and data subject rights.

[48] Negotiations started in 2008 but were suspended in 2011 due to political unrest.

[49] European Commission, Renewed partnership with the Southern Neighbourhood: A new Agenda for the Mediterranean, SWD (2021) 23 final, p. 6.

and promote further convergence with EU and international data protection standards, facilitating commercial exchanges and law enforcement cooperation.'[50] The EU promises to provide financial support to 'countries that show ambition in implementing (…) shared values.'[51]

The EU is not the only foreign partner to North African countries. In 2000, China initiated the first of a series of strategic meetings, namely, China-Africa Consultative Forum (CACF) to discuss African policy.[52] During the meeting held in Beijing, participants adopted the Beijing Declaration and the Program for China-Africa Cooperation in Economic and Social Development.[53] The second meeting was held in 2003, in Addis Abeba, and was attended by 44 African delegations. During the meeting, China cancelled 1.3 billion USD debt owed by 31 African countries. The debt cancellation was done as a sign of good will and a start of a new relationship between China and Africa.

In 2016, China released an Arab Policy Paper outlining its commitment to improve the relationship between China and North African countries.[54] According to the Arab Policy Paper, one of the areas in which the China-Arab cooperation is to be strengthened is the exchange between the legislature of the National People's Congress of China and the legislatures of Arab states.[55] According to a report by ERA, '[i]n 2005 alone, China sent twice as many cabinet level officials to Africa as did the United States or France.'[56]

In addition, China also vowed to ensure the two sides sign an agreement to create a free trade zone between China and North African countries[57] and a China-Arab technology transfer.[58] China's influence on data protection regulation in North Africa is not yet visible. However, it slowly leads to a competition to the EU's sustainability trade policy in North Africa. According to Lons et al., China is emerging as an important development partner in the region and its 'economic importance to the region has the potential to outweigh that of the US and Europe'.[59] Nevertheless, data protection reforms may not be a priority in the China-Arab cooperation as it is in the case of the EU. Consequently, the influence of the EU data protection framework in Africa may still prevail regardless of China's presence and influence in trade.

[50] Ibid.

[51] Ibid.

[52] Shinn, China's Approach to East, North and the Horn of Africa, China's Global Influence: Objectives and Strategies, a Testimony before the U. S.-China Economic and Security Review Commission, July 21, 2005, p. 4.

[53] Ibid.

[54] China's Arab Policy Paper, Xinhua, January 14, 2016.

[55] See Article 1.3 of the China's Arab Policy Paper.

[56] Executive Research Associates (Pty) Ltd, China in Africa: A Strategic Overview, October 2009, p. 9.

[57] Ibid, Articles 2.3 and 2.4

[58] Ibid, Article 3.3.

[59] Lons et al, China's Great Game in the Middle East, Policy Brief commissioned by the European Council on Foreign Relations, October 2019, p. 7.

2 Methodology

Scope, objectives, and structure of the study are outlined by way of an introduction. This study used qualitative research methods to analyse legal texts and other related sources of literature. A parallel comparative analysis was conducted between data protection laws of North African countries on the one hand, and between data protection laws of North African countries and the GDPR on the other. The process of the analysis was broken down into two major stages. First, relevant laws and literature were researched, identified and perused. This was followed by a comparative analysis with the GDPR and with the relevant laws of each individual country to the other.

2.1 The Study and its Scope

This study is a descriptive desk study. As mentioned above, it involves the legal analysis of data protection statutes of North African countries (the "law in the books") and related literature. It also involves comparative aspects in which both contents and contexts of national statutes are analysed, also in relationship with the GDPR. Eventually, the study identifies commonalities as well as divergences between the North African data protection laws and the GDPR. Resulting from the analysis, this study presents a summary of the content-related and contextual resemblances between the North African data protection laws. Finally, the study intends to identify patterns in the development of data protection laws in North Africa, looking at the influence of regional and international regulations, socio-economic, and political influences. This study did neither conduct any empirical research nor an exhaustive comparative analysis of the laws, policies, and their actual implementation. Indeed, the analysis is focussed on selected subject-matters to enable the identification of relevant resemblances and divergences.

2.2 Objectives

The study provides a legal overview of data protection laws in North Africa countries. It may lay a groundwork for an interdisciplinary in-depth study on "North African Data Protection Laws in Action", an empirical study on actual enforcement of data protection laws, the perception of data protection laws, alternative mechanisms of dispute resolution regarding data protection issues, stakeholder interests, etc. The study may also be used as an advisory basis for events concerning this legal field, i.e. measures of implementation or for further discussion.

2.3 Structure

In its core, the study presents seven country reports of North African countries (Algeria, Egypt, Mauretania, Morocco, Tunisia, Libya, and Sudan). These country reports formed the basis of a comparative analysis of the countries' data protection legal frameworks as well as general (overarching) observations thereof. In the end, the study sets out key takeaways and suggests recommendations with regards to the North African region – and puts the current state of data protection law in the aforementioned countries into a broader context.

3 Country reports

This chapter presents country reports on the state of the data protection laws of Algeria, Egypt, Mauritania, Morocco, Tunisia, Libya, and Sudan.

3.1 Algeria

Despite decades of political unrest and terrorism, the People's Democratic Republic of Algeria was able to adopt a comprehensive data protection law in 2018. The following section reviews the framework of the right to privacy and data protection in Algeria; more specifically, the 2018 Law and the status of its implementation since its promulgation.

3.1.1 Political Context of Data Protection

The preamble of the Algerian Constitution declares Algeria as 'an integral part of the Great Arab Maghreb and an Arab, Mediterranean and African country'. It also expresses Algeria's commitment to 'full respect for the goals and organising principles of human rights' treaties including the Universal Declaration of Human Rights (hereinafter: UDHR), the International Covenant on Civil and Political Rights (hereinafter: ICCPR), the African Charter on Human and Peoples' Rights (hereinafter: Banjul Charter), and the Arab Charter on Human Rights (hereinafter: ACHR).[60]

In relation to data protection, Article 47 of the Constitution specifically stipulates the right to data protection stating, '[t]he protection of individuals when handling personal data shall be a fundamental right'. Additionally, the Constitution entails the right to confidentiality of correspondence and private communications in all their forms, and guarantees the inviolability of dwelling houses[61]. To enforce the right to data protection, the Constitution gives citizens the right to access, acquire, and transmit information, documents and statistics. Further, it clarifies that a specific law shall be adopted to determine the modalities for exercising the right to data protection.[62] An aspect worth noting is the fact that the right to data protection under Article 47 is given to 'every person', while the right to access, acquire and transmit information under Article 55 is limited to 'citizens'.

Algeria's legal development and reform initiatives have been considerably impeded by civil unrest and violence, notably by the 'black decade of violence' that took place between the early 1990s to the early 2000s.[63] During this period, human rights implementation, let alone measures of data protection, could not be a priority.

[60] Constitution of the Republic of Algeria, 2020, Preamble

[61] Article 48.

[62] Article 55 of the aforementioned Constitution.

[63] Dupret/Hounet, Anthropological Perspectives on Law and Property in Algeria. Law and Property in Algeria: An Anthropological Perspective in Hounet, (ed), Brill, 2018.

3.1.2 Development of and Influence on Data Protection Regulation

In the early 2000's, Algeria undertook socio-economic reforms to transition to a free-market economy. These reforms included the modernisation and liberalisation of the ICT policies.[64] The purpose of the reforms was to align Algeria with international practice and support its participation in the information society. Consequently, it was necessary for Algeria to reform its legal framework, since the existed framework did not support the use of new technology.[65] Specifically, privacy, security (including payment systems), and confidentiality of information were identified as some of the issues that needed to be addressed in the reforms.[66]

In 2005, the Ministry of Post, Information Technology and Communications received assistance from the Internews Network Global Internet Policy Initiative (GIPI)[67] towards policy and regulatory development to liberalise ICT infrastructure.[68] Liberalisation of the ICT sector had improved Algeria's ICT market competition and growth in the roll-out and use of ICTs. On the downside of this development, the risk of cybercrimes and data insecurity increased.[69] Combined with the country's pressure to evolve its economy through the use of ICTs, a legal framework to regulate associated risks had become fundamental. The country also recognised the use of ICTs to improve its foreign trade and its international competitiveness through exports. To accomplish this, it needed to establish public trust in the use of ICTs, and therefore undertook to reform data protection laws.[70]

In addition, Algeria signed the Euro-Mediterranean Association Agreement in 2005.[71] The Agreement entails support of the European Union to help Algeria restructure its economy and technological modernisation. Section 2 of the Agreement makes it a requirement for parties to respect democratic principles and fundamental human rights, and to have those principles lead internal and international policies of the parties. The Agreement also creates a free trade zone between the EU and Algeria.[72] Section 45 of the Agreement imposes an obligation for parties to take necessary measures to ensure the protection of personal data in order to facilitate the free flow of data between parties. Basically, these provisions of the Agreement are aimed at aligning relevant Algerian laws, particularly laws affecting free trade and free

[64] APC/Hivos, Global Information Society Watch, 2009, p. 83.

[65] Ibid, p. 98.

[66] Ibid, p. 94.

[67] GIPI is a United States-funded project to assist Algeria on digital policy and regulatory processes.

[68] Ibid.

[69] In 2014, a report titled, 'IT Threat Evolution Q1 2014' compiled global IT threats and identified Algeria as the highest in Africa cyber security incidents.

[70] World Bank, Report on the Foundation for the Development of Information and Communications Technologies in Algeria, 2003, p. 66.

[71] Accord Euro-Mediterraneen Etablissant une Association entre la Republique Algerienne Democratique et Populaire d'une Part, et, la Communaute Europeenne et ses etats Membres, d'autre Part.

[72] Section 6 of the Agreement.

movement of information.[73] They also envision cooperation between Algeria and the EU in harmonising consumer protection systems.[74]

Other than the EU, Algeria received assistance from the government of South Korea through the Knowledge Sharing Program Project (KSP).[75] In 2012, the KSP assisted the Ministry of Prospective and Statistics to draft the Algeria National Vision 2030. The latter, as a strategy to improve international trade in the country, emphasized on the need of the Algerian government to develop and implement suitable policies.[76]

In the process of developing suitable policies, the country adopted a data protection law: the *Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel*[77] in 2018. It remains to be seen if Algeria will ultimately also support the regional framework for data protection and sign the Malabo Convention.

3.1.3 Nature and Scope of the Law: Loi n° 18-07 Relative à la Protection des Personnes Physiques dans le Traitement des Données à Caractère Personnel

Loi n° 18-07 Relative à la Protection des Personnes Physiques dans le Traitement des Données à Caractère Personnel (hereinafter "the Law") was published in the Official Gazette in July 2018, as the first comprehensive data protection law in Algeria. Per Article 1 of the Law, the purpose of the Law is to establish rules for the protection of personal data. Article 2 clarifies the underlying principle for the protection of personal data, stating that the processing of personal data must respect human dignity, privacy, and civil liberties. According to Articles 70 and 71, the Law is applicable alongside the penal law of Algeria.

Similarly to the GDPR, the Law applies to any processing of personal data, whether by natural or legal persons, be it automated or not. The Law applies equally to public or private entities.[78] Unlike the GDPR, the Law does not have extraterritorial application. Geographically, it applies to the processing of personal data if the data controller is based in Algeria or if the means of processing data are located in Algeria. In the latter case, data controllers must notify the Data Protection Authority (DPA) and designate a representative in Algeria for purposes of accountability.[79]

With regards to the material scope, the Law does not apply to the processing of personal data in a purely domestic context, by national security agencies, for purposes related to criminal justice enforcement and

[73] Section 56 of the Agreement:

[74] Section 65 of the aforementioned Agreement.

[75] KSP was launched in 2004 by the Ministry of Strategy and Finance and the Korea Development Institute. The aim of the project is to share experience and knowledge with other countries in policy matters. The project also helps partner countries to navigate policy development challenges and assist them in the process of developing policies. See Ministry of Strategy and Finance/Republic of Korea, Establishment of Algeria's National Vision 2030, 2013, p.5

[76] Ibid at pp. 160-162 et seq.

[77] Translated as, 'The Law No. 18-07 dated 10 June 2018 Relating to the Protection of Individuals in the Processing of Personal Data.'

[78] Article 4.

[79] Article 4.

for judicial activities.[80] The Law does not exempt the processing of personal data for journalistic, literature, or scientific purposes or by Non-Governmental Organisations (NGOs) processing data of its members.

Basic concepts such as 'personal data', 'data subject', 'data controller', 'data processor' (the Law uses the term *Sous-traitant*), 'sensitive data', and 'consent' have similar connotations as in the GDPR.[81] The Law further categorises data into sensitive and non-sensitive data[82], taking over the GDPR's categorisation.

3.1.4 General Principles and Conditions for the Processing of Personal Data

The Law sets up the basis for the processing of personal data, which can only take place once declared[83] to the DPA or authorised by the DPA[84] (these requirements are not set forth in the GDPR[85]). In both cases, the prerequisite for the processing of personal data is either the data subject's express consent or another legal basis for processing of personal data as provided by the Law.[86] For the processing of a child's[87] personal data, the Law requires the consent of a parent or a legal guardian of the child. The Law further empowers a competent judge to give their consent for the processing of data relating to a child. To secure the interest of the child, the judge may provide his consent, overriding the parents' or guardian's withheld consent.[88]

A legal basis for the processing of personal data include instances where the processing of personal data is necessary (in the absence of the consent of the data subject). This includes when the processing of personal data is necessary to allow the data controller to meet his legal obligations, for purposes of executing contractual obligations to which data subject is a party, to safeguard vital interests of a data subject, and discharging of official duties or pursue legitimate interests by a data controller or a third party.[89]

---

[80] Article 6.

[81] Article 3.

[82] Article 3.

[83] According to Article 13, a declaration is a statement filed with the DPA ensuring the DPA that the processing is carried out in accordance with the law. In this case, a single declaration filed with the DPA is sufficient for multiple data processing as long as the processing are done by the same controller and involves same or related purposes. The decision allowing the processing activities to take place is communicated within 10 days of filling the declaration.

[84] All processing activities likely to infringe on individual rights and freedoms require DPA authorisation. Once an application for an authorisation to process personal data is filed, the DPA assesses the situation and decides, within two months, on whether or not to issue the authorisation. In the expire of two months, if the DPA has not communicate / issue authorisation, it means that the application is rejected. It is worth noting that processing authorisation can be withdrawn by the DPA if the processing undermines national security or is contrary to morality and good customs. See Articles 12, 17, 20 and 48.

[85] Although the GDPR requires neither a declaration nor an authorisation from the DPA prior to the processing of personal data, Article 36 (5) permits member states to enact such requirements in their national laws.

[86] Article 7. A legal basis for the processing of personal data – other than consent – is given when the Law allows the processing of personal data (under specified circumstances). Normally, this is the case if the processing of personal data is necessary for inter alia reasons of national security or criminal justice etc.

[87] The word used in the law (and the GDPR) is 'a child'. The GDPR refers to 16 years (for purposes of consent). In the Algerian law, there is no definition of a child. The law makes a cross reference to another law on child protection, i.e. law n° 15-12 of 28 Ramadhan 1436 corresponding to July 15, 2015 relating to child protection, in which Article 2 defines a child as a person under 18 years.

[88] Article 8 of the aforementioned Law.

[89] Article 7.

This scope is similar to the one provided for under Article 6 of the GDPR as legal basis for the processing of personal data.

Once the basis for the processing of personal data is established, the data controller must adhere to seven data protection principles. The seven principles stipulated in the Law are equivalent to the principles in the GDPR. However, the first principle 'lawfulness, fairness and transparency' has excluded 'transparency'.[90] Other principles, including purpose limitation, data minimisation, data accuracy, storage limitation, integrity and confidentiality[91], and accountability[92] are equally provided for in the Law.

3.1.5 Selected Data Subject's Rights

The Law gives data subjects the right to be informed of the existence of their data (information right)[93], to have access to such data[94], to request correction, erasure, and object or block all or specific data processing activities[95]. In case the basis for the processing of personal data is the data subject's consent, the data subject has the right to withdraw such consent at any time.[96] Data subjects have the right to be notified of any data breaches involving their personal data. However, this right may be disregarded if the DPA finds that appropriate data protection measures to counteract the breach have been implemented by the data controller / processor.[97]

The Law prohibits direct marketing (unsolicited advertisements). An exception is when direct marketing is through an email, and contact information (email address) was freely given by the data subject during a sale or the provision of similar services. In this case, the data subject's right to withdraw their consent must be communicated to the data subject.[98] Similarly, the Law prohibits the processing of personal data that leads to automated decision making. Particularly, when such decision involves an assessment of a person's behaviour or aspect of their personality. In such cases, data subject's involvement in the decision-making process is expected.[99]

The rights mentioned above resemble those provided for in the GDPR. However, the Law does not stipulate the right to data portability which is granted under Article 20 of the GDPR.

[90] Article 9(a).

[91] Article 9 (b) – (e).

[92] Article 9 and 38.

[93] Article 32.

[94] Article 34.

[95] Articles 35 and 36.

[96] Article7.

[97] Article 43.

[98] Article 37.

[99] Article 11.

3.1.6 Implementation Status

According to Article 75 of the Law, it is to come into force one year after the installation of an Algerian data protection authority. In 11 August 2022, the President and members of the DPA were sworn in. The establishment and appointment of the members of the DPA were both decided upon under the Presidential Decree to establish the DPA.[100] As per Article 75 of the Law, it means, the Law will officially come into force in mid-2023. The respective DPA is established as an independent administrative authority, with legal personality and financial autonomy. This authority is created under the office of the President of the Republic of Algeria.[101]

The Law provides for administrative and judicial penalties for breaches of the Law. Once in force, the DPA will have the mandate to issue administrative sanctions against data controllers in breach of their obligations. The sanctions range from issuing a warning, a notice of breach, temporary or permanent withdrawal of the declaration or authorisation, to prescribing a fine.[102]

Data subjects could also seek judicial remedies in either civil or criminal courts – depending on the nature of the claim. In terms of civil remedies, a court of competent authority may order precautionary measures tending to put an end to a breach of the Law or may grant compensation for the breach.[103] Criminal courts can adjudicate offences emanating from the Law and have the sanctioning power to order the payment of a fine or even imprisonment of the wrong-doer.[104] Imprisonment is not foreseen as one of the penalties for failure to abide to the law under the GDPR.

Although the Law does not have extraterritorial application, Article 53 gives criminal courts the power to hear offences committed outside of the Republic of Algeria. This jurisdiction is limited to Algerian citizens in foreign countries or a company / firm established under the laws of Algeria. Criminal courts are also competent to hear offences in accordance with the rules of jurisdiction provided for in Article 588 of the Code of Criminal Procedure.[105]

3.1.7 Conclusion

The 2018 Data Protection Law not only protects personal data, but also re-enforces Articles 47 and 55 of the Constitution of the Republic of Algeria. The right to personal data protection under Article 47 of the Constitution required an enactment of a law to provide for mechanisms for individuals to exercise their rights such as the right to access their personal data. By establishing a comprehensive framework for personal data protection, the Law provides for such a mechanism. Save for a few omissions (such as the lack of derogation for the processing of personal data for journalistic purposes), the Law creates a frame-

[100] Presidential Decree 22-187 of 17 Chaoual 1443 corresponding to 18 May 2022 (*Décret présidentiel n° 22-187 du 17 Chaoual 1443 correspondant au 18 mai 2022 portant nomination du président et des membres de l'autorité nationale de protection des données à caractère personnel*).

[101] Article 22.

[102] Article 46.

[103] Article 52.

[104] See Article 53 and Chapter 3 in general.

[105] Article 53.

work of basic rights and conditions for processing of personal data found in most international instruments. Since the establishment of the DPA took place recently, and the Law is yet to come into force, the actual protection of personal data or the efficiency of the DPA is to be seen.

3.2 Egypt

Before the year 2020, the Arab Republic of Egypt had neither a comprehensive law for the protection of privacy and personal data nor a record in the implementation of such rights. The following section reviews Egypt's data protection law that was adopted in 2020.

3.2.1 Political Context of Data Protection

The right to privacy has been part of the Egyptian Constitution since Egypt's first Constitution of 1923.[106] The current Constitution of 2014[107] provides for a right to privacy[108] and security of information spaces[109]. Under Article 57 of the Constitution, the right to privacy stipulates a guarantee to private life and inviolability of households. Article 57 guarantees confidentiality of all forms of communications and further prohibits illegal access, interception, assessment, confiscation or monitoring of citizens communications.[110] Per Article 57, only 'citizens' fall under the personal scope of protection of the right to privacy.

Article 58 prohibits the invasion of privacy of households. The prohibition extends to entering, searching, monitoring or wiretapping households without causal judicial warrant, or in cases of dangerous situations, or if a call for help is made. Unlike Article 57, this Article does not expressly limit the personal scope of protections to only Egyptian citizens.

The constitutional right to privacy is incorporated in several laws, including the Penal Code[111] (which imposes criminal sanctions for unlawful collection of images or recordings of individuals in private places), the Civil Code[112], the Cyber Security Law[113] (under which service providers have the obligation to ensure

[106] The 1923 Constitution provided for the privacy of domicile / home (Article 8) and privacy of communications under Article 11. The Article states, 'No secrecy of letters, telegraphs and telephone communications may be divulged unless in conditions set forth by the law.'

[107] The Constitution of Egypt of 2014.

[108] Articles 57 and 58.

[109] Article 31.

[110] These guarantees can be waived by causal judicial order, for a limited period of time, and in cases specified by the law (see Article 57).

[111] No. 58/1937, Article 309 bis.

[112] No. 131/1948, Article 163.

[113] No. 175 of 2018.

the privacy of data they process), the Telecommunications Law[114] (which penalises access to telecommunication), and the E-signature Law[115]. In 2020, Egypt adopted a law to enforce the right to privacy of victims of sexual harassment and violence.[116] However, the actual implementation of the right to privacy is stalling.

Egypt continues to receive financial and material assistance to support human rights reforms and their application. For example, in 2020, the European Instrument for Democracy and Human Rights issued more than EUR 80 million to support over 40 projects to support human rights reforms.[117]

3.2.2 Development of and Influence on Data Protection Regulation

Egypt has considerably reformed and developed its legal and regulatory framework for media, data, and consumer protection in the last decade.[118] On January 12th 2016, the Egyptian Ministry of Communications and Information Technology, presented to the High Committee for Legislative Reform, a 'Cybersecurity and Information Crime Law' as part of its legislative agenda.[119] According to a report written by Mohamed Hemdani, the Ministry's memo accompanying the draft Law cited 'cyber security' as the main reason to urge the adoption of the Law at that specific time. Another reason was 'the increased value of electronic commerce in Egypt.'[120] The latter necessitate strengthening Egypt's legal and regulatory framework to support digital economy.[121]

Following the Minister's legislative reform proposal, in 2018, the country adopted the Cyber and Information Technology Crimes Law[122] and the Consumer Protection Law[123] followed by the Data Protection Law (قانون 151 لسنة 2020 لحماية البيانات الشخصيَّة;) (hereinafter "the Law")[124] and the Media and Journalism Law[125]. The reforms were Government's overall efforts to 'maintain data safety' in order to support and promote digital economy.[126]

Another reason that might have contributed to reforms in Egypt is its 'fraternity' to the League of Arab States and the United Nations Economic and Social Commission for Western Asia (ESCWA). The Arab

[114] No. 10/2003.

[115] No. 15/2004.

[116] European Commission, EU Annual Report on Human Rights and Democracy in the World: 2020 Country Updates. p. 39.

[117] European Commission, supra n. 116, p. 40.

[118] See further Badawy, T. et al., The Technology, Media and Telecommunications Review: Egypt in Murchison, (ed), The Technology, Media and Telecommunications Review, 2022.

[119] Ibid, unnumbered p. 16

[120] Ibid, unnumbered p. 18.

[121] Ibid, unnumbered p. 16

[122] The Cyber and Information Technology Crimes Law No. 175 of 2018 and Decree No. 1699 of 2020, 27 August 2020.

[123] Consumer Protection Law, Law no 181 of year 2018.

[124] Personal Data Protection Law, Law No. 151 of 2020.

[125] The Media and Journalism Law and Decree No. 418 of 2020, 16 February 2020.

[126] Hemdani, Data Protection in Egypt: The Present and the Future, Dissert., 2016, unnumbered p. 3.

League adopted the Convention for Combating Information Technology Crimes (Arab Convention)[127] in 2014, which came into force the same year. The main objective of the Arab Convention is to 'enhance and strengthen cooperation between the Arab States in the area of combating information technology offences [...] in order to protect the security and interests of the Arab States and the safety of their communities and individuals.'[128] As elaborated previously, ESCWA aims at harmonising ICT laws, including data protection legal frameworks, in member states. It provides for a template of a model data protection framework to support the harmonisation process. The model establishes a data protection framework that has links to the 1995 EU Data Protection Directive and the OECD Data Protection Guidelines.[129]
Despite Egypt's membership to the African Union, it has neither signed nor ratified the Malabo Convention.

The process to adopt the Data Protection Law was relatively swift and did not involve public or stakeholders' discussion. According to a research paper written by Kulaib, the draft Law presented by the Minister of Communications and Technology in 2019 was approved by the government (without debates) and ultimately approved by the House of Representatives in 2020.[130] Nevertheless, this Law is considered to be among the ten strictest data protection laws in the world.[131] The Law was published in an official Gazette on July 15th 2020 and came into force on October 16th 2020.[132] According to Article 4 (of the issuance Articles) of the Law, the Executive Regulations to support its enforcement will be issued six months from the day the Law came into force.[133] At the time of writing this report, no information on the status or publication of the Executive Regulations could be found. Nevertheless, the Law gives data controllers, processors and holders a one-year grace period to comply with the Law.[134]

3.2.3 Nature and Scope of the Data Protection Law No. 151 of 2020

The 2020 Data Protection Law is the first comprehensive data protection legislation in Egypt. Similar to the GDPR, the Law applies to companies, public and private, as well as individuals processing personal data[135]. The only (main) difference from the GDPR is that the Law does not apply to the processing of personal data exclusively in a physical format.[136] Like the GDPR, the Law has extraterritorial application; although the scope of its extraterritoriality is slightly different from the one in the GDPR. In the GDPR,

[127] League of Arab States, Arab Convention on Combating Information Technology Offences, enacted in 2010.

[128] Article 1 of the Arab Convention.

[129] See The ESCWA Cyber Legislation Digest, 2013; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); and Fatafta/Samaro, supra n. 40.

[130] Kulaib, Paper on Egypt's Personal Data Protection Law (PDPL) and where it stands according to the international standards, Research Unit of the Association for Freedom of Thought and Expression (n. d.) p. 10.

[131] Baig, 10 Strictest Data Privacy Laws By Country in 2022.

[132] Article 7 of the issuance Articles states: 'This law shall be published in the Official Gazette and shall come into force after three months from the following day of its publication.'

[133] Article 4 states; 'The Minister responsible for telecommunication and information technology shall issue the executive regulation of the accompanying law within six months from its effective date.'

[134] Article 6 of the issuance Articles.

[135] See Articles 1 (of the issuance Articles) and Article 1.

[136] Article 1.

the scope of application involves data controllers or processors who offer goods / services or monitor behaviour of data subjects in EU.[137] In the Egyptian Law, it involves the data controller, processor, or holder who has to be an Egyptian citizen (within and outside of Egypt) or a non-Egyptian citizen outside of Egypt as long as 'the act is punishable in any form in the country where it occurred, and the data subject (victim of the crime) belongs to Egyptian nationals or non-Egyptians residing within the Arab Republic of Egypt.'[138]

In terms of the material scope, the Law does not apply to the processing of personal data in a purely domestic context, for journalistic and statistic purposes, by national security agencies, for purposes relating to criminal justice enforcement and for judicial activities.[139] The Law differs from the GDPR in further excluding the processing of personal data by the Central Bank of Egypt and entities subject to its control and supervision.[140] Furthermore, the Law does not give any exceptions to the processing of personal data for scientific purposes or by NGOs processing personal data of its members.

Core concepts such as 'personal data', 'processing', 'data subject', 'data controller', and 'data processor' have a similar meaning with corresponding concepts in the GDPR.[141] Additionally, the Law introduces the new concept of 'data holder'[142]. This actor steps in alongside with the data controller and data processor. Accordingly, Article 1 states that data holder is 'any natural or juristic person legally or factually holding and retaining personal data in any manner, or by any means of storage, regardless of whether that person held such data initially or it was transferred to the person by any means of transfer.'

Similar to the GDPR, the Law provides for two categories of personal data, sensitive and non-sensitive data[143]. However, unlike the GDPR, the Law includes 'data relating to children' in the category of sensitive data,[144] which in addition requires an action by parents or legal guardians before it is processed.[145]

3.2.4 General Principles and Conditions for the Processing of Personal Data

The Law requires individuals or entities processing personal data to obtain a permit before commencing data processing activities.[146] In addition to the permit, entities must also obtain a licence from the Data Protection Center. Both the permit and the licence stipulate obligations in relation to the Law. The permit

[137] Article 3 (a) (b) GDPR.

[138] Article 2 (of the issuance Articles).

[139] See Article 3 (of the issuance Articles) of the Law and Article 2 of the GDPR.

[140] Article 3 (6).

[141] See Article 4 of the GDPR and Article 1 of the Law respectively.

[142] Cf., however, the proposal of the Data Act by the EU Commission, COM (2022), 68 final.

[143] See Article 12

[144] Article 1.

[145] Article 12.

[146] Article 1 defines a permit as 'an official document issued by the Center to natural or juristic person granting him the right to practice the activity of collecting, storing, transferring or processing personal data electronically or to partake in Electronic Marketing activities, or all of the above or to carry out a specific task or specific tasks.'

is granted for a period not exceeding one year and the licence for a period of three years.[147] This approach is different from the GDPR, where individuals and entities subject to the GDPR are not required to obtain a licence or permit prior to the processing personal data.

Once a permit is granted (and a licence, in the case of an entity), the processing of personal data can take place only if the data subject has given a consent[148] or if there is another legal basis to allow such processing to take place[149]. Additionally, the processing of personal data must adhere to basic processing conditions / principles. Article 3 of the Law provides for four principles; i.e. purpose limitation[150], data minimisation[151], data accuracy[152], and storage limitation[153]. These conditions are similar to those provided under the GDPR, although the list is short of three principles enshrined in the GDPR. These are lawfulness, fairness and transparency, integrity and confidentiality and accountability.[154] Noteworthy is the fact that 'integrity and confidentiality' as well as 'accountability' are stipulated as controllers' duties under Articles 4 (6) and 5 (9) as well as Articles 4 (12) and 5 (10), respectively. The principles 'lawfulness, fairness and transparency' are completely omitted from the Law. In addition, the principle of 'data minimisation' has a stricter regulation in relation to children taking part in games (a term not specified any further) or competitions. Article 12 of the Law requires that only data required to participate in such a game, competition, or related activity should be collected.

3.2.5 Selected Data Subject's Rights

The Law gives an individual the right to be informed of their data held by a data controller (right to information), to have access to such data, to request erasure, and object or block all or specific processing activities.[155] In case the data subject has consented to the processing of personal data, she or he has the right to withdraw such consent at any time.[156] The data subject also has the right not to be subjected to direct marketing without their consent.[157] Furthermore, in the event that the security of personal data is compromised, data subjects have the right to be notified of data breaches within three days of the data breach.[158] These rights resemble data subject's rights under the GDPR. However, the Law omits two rights

[147] Article 1.

[148] See Articles 2 and 6 (1).

[149] Legal basis for the processing of personal data is granted under the Law when the processing is *necessary* and *essential* in executing a contract or agreement or a legal action involving the data subject, performing an obligation under a law or order of a competent court or investigation authority, or to allow a data controller (or his legal representatives) perform his duties. See Articles 2 and 6 (2) – (6).

[150] Article 2 (3).

[151] Article 3 (1).

[152] Article 3 (2).

[153] Article 3 (4).

[154] See Article 5 of the GDPR.

[155] Article 2.

[156] Article 2 (2).

[157] Article 17.

[158] Articles 2 (5) and 7.

that are provided in the GDPR: the right to data portability and the right not to be subjected to automated decisions.

3.2.6 Implementation Status

The Law has not yet come into force. As mentioned previously, its implementation was expected to commence in the first quarter of 2022. As of August 2022, no information on the publication of the enforcement regulation or commencement of the Law could be found. However, during the Seventh Annual Conference of the Chamber of Information and Communication Technology Industry, it was announced that the regulations will be issued before the end of this year (2022).[159] Once entered into force, the Law envisions the establishment of an enforcement authority, named 'the Personal Data Protection Center'[160] (hereinafter 'the Center'), to be established under the Ministry of Communications and Information Technology.[161] Its mandate includes monitoring compliance of the Law by regulating processing of personal data and cross border movement of personal data.[162] In addition, the Law gives the Center powers to make policies relating to data protection, to receive complaints and resolve data protection related conflicts, accredit data protection professionals and cooperate with other entities in guaranteeing the protection of personal data.[163]

The Law prescribes administrative, civil, and criminal penalties for failure to comply. The Center can issue compliance notices (for non-compliance) or enforce administrative sanctions, which include the suspension or withdrawal of a licence and certification, the publication of the incident in media outlets, and / or the placement of the non-compliant person under technical supervision of the Center.[164] Non-compliance may also be subjected to judicial proceedings, leading to either court sanctions or imprisonment.[165] In addition to penalties imposed by courts, the Law requires that 'the conviction be published in two widely published newspapers and on the internet at the expense of the convict.'[166]

The system allows for the defendant to settle the matter at any stage of criminal proceedings.[167] This enables the defendant to avoid public 'shaming' by media publications. However, settlements require the approval of the Center and can only occur before the judgment is rendered.

[159] The announcement was made by Dr. Ahmed Abdel Hafez (Vice President of the National Telecommunications Regulatory Authority for Cyber Security Affairs).

[160] Article 19.

[161] Article 19.

[162] This entails issuance of licences, permits / authorisations, and accreditations for processing of personal data of data subjects within Egypt or Egyptian nationals outside Egypt as well as data that crosses Egyptian border. Cf. Articles 2 (of the issuance Articles) and 19.

[163] Article 19.

[164] Article 30.

[165] See Chapter 14 of the Law.

[166] Article 48.

[167] Article 49.

In terms of sanctions, two aspects differentiate the Law from the GDPR; first, under the GDPR (but under national law), imprisonment is not a possible sanction for breaches; second, the GDPR does not have a mandatory requirement for a court to order a media publication of a conviction.

3.2.7 Conclusion

The right to privacy under the Constitution is limited to citizens. Nevertheless, in 2020, Egypt adopted a data protection law that extends its protection beyond citizens of Egypt (see Article 2 of the issuance articles). In addition, the Law has an extraterritorial application. The extraterritorial application of the Law reaches further than many data protection laws in the continent. It also applies to Egyptians as well as foreigners outside of Egypt if they breach the Law and if the victim is an Egyptian citizen. The actual implementation of the Law is yet to be seen since the respective Center and the implementing regulations have not been published.

3.3 Mauritania

In 1991, the Islamic Republic of Mauritania adopted the first independent Constitution, replacing the 1959 Constitution which was drafted after the French Fifth Constitution. The 1991 Constitution reformed Mauritania to a democratic country with a multi-party system and bill of rights – which include the right to privacy. This Constitution was amended in 2006 introducing the country's commitment to repeal all laws that are contrary to the constitutional values.[168] In the same year, the National Human Rights Commission was established.[169] This section starts by looking into Mauritania's state of privacy protection followed by the development of the first data protection law. Thereafter, it provides the nature and the status quo of implementation of the data protection law.

3.3.1 Political Context of Data Protection

In 2019, Mauritania conducted its first peaceful presidential election since its independence in 1960. The newly-elected President Mohamed Ould Cheikh El Ghazouani vowed to implement wide-ranging reforms, including in the areas of human rights and public fundamental freedoms.[170]

Despite challenges, such as political instability, Mauritania is reported to have made a substantive improvement in the field of human rights in general.[171] As such, in 2020, the Mauritania National Human Rights Commission (*Commission Nationale des Droits de l'Homme*)[172] was granted a status A after being assessed to align with the Paris Principles.[173]

[168] Article 102 of the Constitution.

[169] Established through Ordinance nº 015-2006 of 12 July 2006.

[170] European Commission, Annual Report on Human Rights and Democracy in the World: 2020 Country Updates, et seq. p.128.

[171] Ibid.

[172] Commission Nationale des Droits de l'Homme, was established in 2006 and has had constitutional status since 2012.

[173] Ibid.

Mauritania is a member of the United Nations as well as the African Union. It has ratified several human rights instruments including the UDHR, the ICCPR[174], the Banjul Charter[175], and its Protocol on establishing the African Court on Human and People's Rights as well as the Optional Protocol on the establishment of the African Court on Human and Peoples' Rights[176], the African Charter on Rights and Welfare of the Child[177], the ACHR and has an observer member status to the ECOWAS since 2017. All of the above instruments, except the Banjul Charter, provide for the right to privacy. Similarly, Article 13 of the Constitution of the Islamic Republic of Mauritania guarantees the protection of private life, inviolability of homes, and privacy of correspondence.

3.3.2 Development of and Influence on Data Protection Regulation

In 2008, the EU suspended its cooperation with Mauritania due to its continued political instability, sparked by a *coup d'état*.[178] The cooperation between Mauritania and the EU resumed in 2010 after the signing of the Dakar Agreement, with the government of Mauritania promising to bring democratic reforms including improving the human right situation.[179] The EU is not only a major donor to Mauritania[180], but also a partner in the field of human rights.[181] In 2017, the Justice and Human Rights project was created, bringing the EU and other partners (member states of the EU) together to create a dialogue about human rights challenges in Mauritania. The EU's support in Mauritania's human rights dialogue positively impacted the process of policy change in Mauritania.[182]

Moreover, in 2020, Mauritania commenced its three years' term at the UN Human Rights Council (OHCHR). This brought improvement to the implementation of human rights enforcement in the country.[183]

In 2016, Mauritania started undertaking legal reforms to enable the country to fully participate in the information society. The reforms started with the adoption of two laws to regulate information systems and digital space against cyber crimes, namely "*Loi n°. 2016-006, d'Orientation de la Société Mauritanienne de l'Information* (SMI)"[184] and „*Loi n°2016-007 sur la cybercriminalité*" in 2016. The data protection law,

[174]Ratified in 2004, with reservations: Art.18, paragraphs 2-3 and 4, and Art.23, para. 4. These reservations were made as those provisions are regarded to be in conflict with sharia law.

[175] Ratified in 1986.

[176] Ratified in 2005.

[177] Ratified in 2005.

[178] In 2005, a military c*oup d'état* took place, overthrowing the then President Maaouya Ould Sid'Ahmed Taya. The military ruled until 2007, when the country held presidential elections in March 2007. A year later, in August 2008, high-ranking army officials who were dismissed by the elected President Sidi Ould Cheikh Abdallahi led another *coup d'état* in 2008. General Abdel Aziz, who led the high-ranking army officials through the *coup d'état*, took lead of the transitional government and remained President of Mauritania until 2019.

[179] Bøås, The State of Play of EU-Mauritania Relations, 2017, p. 22

[180] Ibid.

[181] European Commission, supra n. 170 at p. 130 et seq.

[182] Bøås, supra n. 179.

[183] European Commission, supra n. 170 at p. 130 et seq.

[184] Loi N ° 2016-006 Loi d'Orientation de la Société Mauritanienne de l'Information (SMI).

namely „*Loi 2017-020 sur la protection des données à caractère personnel"* (hereinafter "the Law"), followed in 2017. The Law establishes a comprehensive framework for data protection. The Data Protection Law was followed by „*Loi n°2018-022 sur les transactions électroniques*" in 2018. The four laws form the "*Cadre Juridique de la Société Mauritanienne de l'Information* (CJSMI)", adopted to lay the legal and institutional foundations for the Mauritanian Information Society.[185]

Mauritania signed the Malabo Convention on the February 26th 2015, but has yet to ratify it.

3.3.3 Nature and Scope of the Law: Loi 2017-020 sur la Protection des Données à Caractère Personnel

The Mauritania Data Protection Law of 2017 establishes a comprehensive framework for data protection. The Law applies to any processing of personal data by individuals, public as well as private organisations[186], whether or not such processing of personal data is done by an automated means[187]. In contrast to the GDPR, the Law does not have extraterritorial application. It applies to controllers established in Mauritania, carrying their activities or processing personal data using a means of processing located in Mauritania, except when the means for processing is used for transit purposes only.[188] Subject to provisions of specific laws and other exceptions, the Law states categorically that it also applies to the processing of personal data for public and national security, defence, and for criminal justice purposes.[189] This diverges from the GDPR. The GDPR exempts the processing of personal data by competent authorities in the field of justice and national security (which is – inter alia – covered by Regulation (EU) 2016/680).[190]

Similar to the GDPR, the Law does not apply to the processing of personal data in a purely domestic context. Other full exemptions in the Law include the processing of personal data by NGOs (of their members for purposes of the organisation) and for a sole purpose of keeping a register by virtue of a law to allow public consultation.[191]

Definition of core concepts such as 'personal data', 'data subject', 'data controller', 'data processor', and 'processing' are similar to corresponding concepts in the GDPR. In the definition of sensitive data, the Law excludes 'genetic' and 'biometric' data, although it lists 'health data' as sensitive data.[192] Additionally, the Law defines a third country as any country other than the Islamic Republic of Mauritania.[193]

Other aspects, such as personal data breach and direct marketing, are not defined in the Law.

---

[185] Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et des Technologies de l'Information et de la Communication.

[186] Article 2 (12) and 3 (1).

[187] Article 2 (14) and 3 (2).

[188] Article 3(4).

[189] Article 3 (5).

[190] Article 2 GDPR.

[191] Article 32.

[192] See Article 2 (7). However, Article 12 includes genetic data on the list of special categories of data.

[193] Article 2 (11).

3.3.4 General Principles and Conditions for the Processing of Personal Data

As in the GDPR, the primary basis for the processing of personal data is the consent of the data subject.[194] Similar derogations also apply. The processing of personal data can take place in the absence of the consent of the data subject when the processing of personal data is necessary to comply with controller's legal obligation or discharge official authority, in performance of a task in public interest, or in performance of a contract in which the data subject is a party or to protect data subject's vital interests.[195]

In addition to the consent, all processing of personal data must either be declared to or authorised by the DPA.[196] Authorisation is required when the processing of personal data involves interconnection of files either for public services or between two or more private entities whose main purpose are different.[197] Other instances requiring DPA authorisation include situations where the processing of personal data involves genetic data in health research, biometric data, criminal justice and security measures, national identification number or any identifier, and for public interest in the context of historical, statistical, or scientific purposes.[198]

With regards to the processing of personal data relating to offences, criminal convictions and security measures, the Law and the GDPR both allow the processing of personal data only by competent authorities in the exercise of their legal duty.[199] However, in the GDPR, the responsible competent authority must ensure that the processing is done under supervision of an official authority or when authorised by law that provides for appropriate security safeguards.[200]

In the Law, the processing of personal data for the purposes of journalism, research, or artistic / literary expression are subject to two conditions. First, the processing must be carried out solely for that specific purpose and, second, must be done on a professional basis, in compliance with guiding laws, professional ethics, and codes of conduct[201].

Although Article 12 of the Law prohibits the processing of sensitive data, Article 13 provides for a long list of exceptions where sensitive personal data can still be processed.[202] Furthermore, if the processing of sensitive personal data involves health purposes, the Law allows such data to be processed whenever it is necessary for the promotion and protection of public health, in prevention of a definite danger, or for

[194] Article 5.

[195] Article 5 (1), (2), (3), and (4).

[196] Articles 27, 28, 33 and 35.

[197] Article 27 and 28.

[198] Article 37.

[199] Article 14 of the Law and Article 10 of the GDPR.

[200] Article 10.

[201] Article 17.

[202] This is when data is made public by the data subject; data subject has given a written consent; in order to safeguard vital interests of the data subject or of another person and if the data subject is physically or legally unable to give consent; for purposes of criminal and civil justice enforcement; for a reason of public interest, in particular for historical statistical or scientific purposes; processing is necessary for the performance of a contract to which the data subject is party; processing is necessary for compliance with law; for the performance of a task carried out in the public interest or by an NGO processing data in discharge of their legitimate activities involving their members.

the purposes of preventive medicine, medical diagnosis, care, or treatment, either to the person concerned or to his or her relative, or where the health services are acting in the interests of the person concerned.[203]

The Law lays down basic conditions for the processing of personal data similar to those provided in the GDPR. Article 6 states that any processing of personal data must be done lawfully, fairly, and not fraudulently. Additionally, the processing of personal data must adhere to the principles of purpose limitation, data minimisation, storage limitation,[204] data accuracy[205], transparency[206], confidentiality[207], and accountability[208]. Although integrity is not expressly listed among the principles, Article 10 of the Law obliges the data controller to ensure personal data is protected in accordance with the provisions of Article 47. Article 47 obliges the data controller to take necessary measures to ensure security of personal data. Furthermore, the Law adjusted the first principle, i.e. 'lawfulness, fairness and transparency' by substituting 'transparent' with 'fraudulent'.

3.3.5 Selected Data Subject's Rights

The Law gives an individual the right to be informed about his or her data held by a data controller (information right)[209] and to have access to their data.[210] This right can also be exercised when the processing of personal data concerns the state's security, national defence, or public safety.[211] Other rights include the right to request erasure and correction of data as well as to block[212] and object[213] connected processing activities. The right to correct and erase personal data extends to the heirs of the data subject.[214]

The Law allows the data subject to withdraw the consent at any time. The data subject has also the right not to be subjected to direct marketing without their consent[215] or to automated decisions when it involves assessment of personal behaviour, aspects of their personality, or if it has legal effects on them.[216]

[203] Article 15. See also Article 40.

[204] Article 7, see also Article 48.

[205] Article 8.

[206] Article 9.

[207] Articles 10, 11 (second paragraph) and 46.

[208] Articles 11 and 47.

[209] Article 50, the right of information.

[210] Article 53. In case of health data, the right to access can be exercised by the patient's doctor or a legal guardian of a child, or spouse / children of the patient, in case the patient died (Article 56).

[211] Article 58. In this case, the request to access is sent to the DPA who shall ensure that such access does not jeopardise the purpose of processing before the data subject is granted access.

[212] Article 61.

[213] Articles 59 and 60.

[214] Article 63.

[215] Article 18.

[216] Article 19.

The Law disregards two rights provided in the GDPR: the right to data portability and the right to data breach notification.

3.3.6 Implementation Status

Article 64 established the Mauritania Data Protection Authority (*Autorité de Protection des Données à Caractère Personnel*). According to this provision, the DPA's task is to ensure that the use of information and communication technologies does not cause any threat to public liberty and privacy.

The establishment of the DPA brings the Law into force.[217] For the first time, the President and members of the DPA were sworn in in July 2022.[218] This formally establishes the DPA and brings the Law into force. According to Article 99 (1) (2) of the Law, data processors who are processing data on behalf of the state have a grace period of three years while all other data controllers are given a grace period of two years.

3.3.7 Conclusion

Despite Mauritania's civil and political unrest, the country is making efforts to reform its digital, legal and regulatory framework. It is one of 14 countries that have signed the Malabo Convention so far. The recent establishment of the DPA further signals the country's commitment to ensure the protection of personal data in the country. The actual implementation of the law will occur after the expiration of the grace period, i.e. 2024.

3.4 Morocco

Morocco is one of the most active countries in data protection in Africa. Morocco is also involved in several international data protection initiatives, such as the Convention 108 and 108+, the Global Privacy Assembly, and the Association of Francophone Data Protection Authorities (AFAPDP). This section presents the development and the state of data protection in Morocco as well as different initiatives taken by the data protection authority regarding enforcement.

3.4.1 Political Context of Data Protection

The first Constitution was adopted 80 years ago and has undergone several changes over the years. The latest referendum on constitutional reforms was held during the so-called Arab Spring. King Mohammed VI had announced it as a response to the large protest movements. This marked the last revision of the Constitution in 2011, which brought reforms but still granted the king far-reaching powers.

The Constitution declares Morocco as a monarchy Islamic state.[219] In addition to declaring its commitment to international principles on human rights, the Constitution reaffirms Morocco's commitment to strengthen its relations with neighbouring Euro-Mediterranean countries. Morocco is a part of several international and regional human rights instruments that provide for the right to privacy, including the

[217] Article 99.

[218] Agence Mauritanienne d'information (AMI), Le Président et les Membres de l'Autorité de Protection des Données Personnelles Prêtent Serment, July 5th 2022.

[219] The Constitution of 2011.

International Convention on Civil and Political Rights (ICCPR) which applies directly and has priority over domestic laws.[220]

In 2017, Morocco resumed its membership to the African Union after it withdrew its membership in 1984.[221] Morocco has ratified the Banjul Charter and the Protocol establishing the African Court. The Banjul Charter does not contain the right to privacy. Morocco has neither signed the African Union Convention on the Rights and Welfare of the Child (the only treaty providing for the right to privacy[222]) nor the Malabo Convention. Nevertheless, the Constitution guarantees the protection of privacy of private lives.[223] Hence, it provides for the foundation to a legal framework for the protection of personal data.

3.4.2 Development of and Influence on Data Protection Regulation

Since the Arab Spring uprising in 2011, Morocco has undergone tremendous reforms and is more stable socially and politically, compared to the other states in the MENA region.[224] Morocco has relatively strong e-commerce laws[225] and a comprehensive data protection framework. According to the World Bank commissioned report, Morocco is also a pioneer in open data in the MENA region. It developed an open data portal in 2011 and made it a policy priority in 2013.[226]

Morocco is the first country among the Mediterranean countries to negotiate a comprehensive trade agreement with the EU. As a result of the strong trade relations between Morocco and the EU, in 2008, Morocco was granted an advance status by the EU.[227] The advance status encompasses, among other objectives, democratic reforms in Morocco. In 2013, the Deep and Comprehensive Free Trade Agreement (DCFTA) was negotiated with the intention to integrate the Moroccan economy into the EU single market.[228] According to Makulilo, a renowned African data protection scholar, these strong trade relations between Morocco and the EU highly influenced the Moroccan data protection framework.[229]

The Moroccan Data Protection Law, the *Loi n° 09-08 Relative à la Protection des Personnes Physiques à L'égard du Traitement des Données à Caractère Personnel* (hereinafter 'the Law'), was enacted in 2009 as the first comprehensive Data Protection Law in Morocco.[230] The Law aligns with the 1995 EU Directive. This

[220] Preamble to the Constitution. See also Makulilo, Data Protection in North Africa: Tunisia and Morocco, in Makulilo (Ed), African Data Privacy Laws, 2016 p. 37.

[221] Louw-Vaudran, Report on North Africa: The Meaning of Morocco's Return to the African Union, Institute for Security Studies, January 2018.

[222] However, Morocco has ratified the UN Convention on the Right of the Child since 1993.

[223] Article 24.

[224] World Bank, Data Governance Practices in Mena Case Study: Opportunities and Challenges in Morocco, November 2020, p. 21.

[225] Ibid, pp. 21-22.

[226] Ibid, p. 17.

[227] Makulilo, supra n. 220 at p. 35 et seq.

[228] Ibid.

[229] Ibid.

[230] Law 09-08 of 2009.

alignment is viewed as a strategy to allow data flows between Morocco and EU member states as a pre-requisite in maintaining trade.[231]

In the same year, Morocco requested an adequacy recognition decision from the European Commission. Such a decision was never issued. Currently, the Moroccan data protection framework is undergoing reforms to align its Law with the GDPR; the hope is to seek an adequacy decision (Article 45 GDPR) from the European Commission,[232] after the first request in 2009 failed. This intention was underlined during a seminar between the Moroccan Data Protection Authority with an EU delegation discussing the alignment of Moroccan data protection framework with the EU framework (i.e. GDPR).[233]

Morocco is also involved in the Council of Europe (CoE) data protection initiatives. In 2019, Morocco became the 55th country in the world and the sixth African country to accede to the CoE Convention 108 on the protection of individuals with regard to the Automatic Processing of Personal Data.[234] The country is also a member of the Association of Francophone Data Protection Authorities (AFAPDP).[235] The AFAPDP has been helping Francophone African countries with data protection legal reforms and in strengthening their enforcement capacities.

3.4.3 Nature and Scope of the Law: Loi n° 09-08 Relative à la Protection des Personnes Physiques à L'égard du Traitement des Données à Caractère Personne

The Law establishes a comprehensive data protection framework. Article 2 (1) states that the Law applies to the processing of personal data regardless of the means of processing (whether by automated or non-automated means). Both public and private companies as well as individuals processing personal data are bound by the Law. This scope of application is similar to the one provided by the GDPR. In contrast to the GDPR, the Law does not establish extraterritorial application. It applies to data controllers established in Morocco or to those using a means of processing personal data located in Morocco.[236]

In terms of material scope, the Law, like the GDPR, does not apply to the processing of personal data in a purely domestic context, in the interest of national security and public safety, and for law enforcement purposes. The exemption for law enforcement purposes is conditioned on the existence of a law authorising such processing of personal data.[237] The processing of personal data for journalistic, artistic, and literary purposes are only exempted from the 'data protection information obligation' as per Article 5. The Law does not explicitly exempt the processing of personal data for historical, scientific purposes, or processing of personal data by NGOs. NGOs are only exempted from the prior authorisation requirement.[238]

---

[231] Tassinari, The Externalisation of Europe's Data Protection Law in Morocco: An Imperative Means for the Management of Migration Flows, Peace & Security – Paix et Sécurité Internationales, No 9, 2021, p.1

[232] Ibid.

[233] Hindi, Moroccan Data Protection Law: Moving to Align with EU Data Protection?,

[234] Council of Europe newsroom, Welcome to Morocco, 55th State Party to Convention 108, May 28th 2019.

[235] See https://www.afapdp.org/lafapdp/members.

[236] Article 2 (2).

[237] Article 2 (4)

[238] Article 12 (1) (a).

The definition of core concepts such as 'personal data', 'data subject', 'data controller', 'data processor' and 'processing'[239] are similar to corresponding concepts in the GDPR. A slight difference is found in the categories of sensitive data. The Law, in contrast to the GDPR, does not list the use of genetic and biometric data for identification purposes and data concerning person's sexual life and sexual orientation as sensitive data.[240] Additionally, the Law lacks other definitions such as those of personal data breach as well as definitions of genetic and biometric data.

3.4.4 General Principles and Conditions for the Processing of Personal Data

The processing of personal data is subject to the consent of the data subject.[241] In this case, consent is also required before data is shared with any third party. A prior declaration filed with the data protection authority (*Commission Nationale de Protection des Données Personnelles*) (CNDP)[242] or prior authorisation by the CNDP is required. Authorisation is required when the processing involves sensitive data (genetic data, data concerning criminal justice enforcement and security[243], national identity number, and interconnection of files between controllers whose purposes are different) or the processing of personal data for purposes other than those for which they were collected.[244] As an additional safeguard to the processing of sensitive personal data, the processing must be backed-up by a specific law.[245]

By way of a derogation, the processing of personal data can also take place without consent of the data subject for contractual purposes involving the data subject[246], in protecting the interest of the data subject[247], by official authority in the public interest[248], to comply with a legal obligation or pursue legitimate interest by the controller or recipient[249]. The derogations are similar with those provided under Article 6 of the GDPR.

In the same way, the Law provides for instances were sensitive personal data could still be processed in the absence of the data subject's consent. This is when the processing is essential for the exercise of the legal or statutory functions of the controller, to safeguard vital interests of the data subject or of another person and if the data subject is physically or legally unable to give consent, if such data is made public by the data subject, or for justice and law enforcement purposes. In all cases, CDNP authorisation must

[239] Article 1 (2).

[240] Article 1 (3).

[241] Article 4.

[242] Article 14. This requirement does not apply to processing of personal data whose sole purpose is to keep a register which is, by virtue of legislative or regulatory provisions, intended for the public, and as long as the controller appoints a data protection officer.

[243] Unless processing is by a court officer.

[244] Article 12.

[245] Article 21.

[246] Article 4 (b).

[247] Article 4 (c).

[248] Article 4 (d).

[249] Article 4 (a) (e).

be obtained.[250] In the GDPR, derogation for similar purposes is allowed, as long as the law of the member state explicitly name those instances.[251]

In addition, the processing of personal data must adhere to data processing principles. Article 3 (1) (a) to (e) sets out five principles which are similar with principles in the GDPR. Accordingly, the processing of personal data must be fair and lawful[252] as well as must adhere to the principles of purpose limitation[253], data minimisation[254], data accuracy[255], storage limitation[256], and accountability[257]. Compared to the GDPR, the first principle 'fair and lawful' is short of the 'transparency' aspect. In addition, the principles of 'integrity and confidentiality' are not listed among the principles in Article 3. Instead, Articles 23 and 25 obligate the controller to ensure the integrity of personal data by putting in place appropriate technical and organisational measures to protect personal data processed by the controller or anyone under his authority. On confidentiality, Article 26 compels anyone processing personal data to adhere to codes of professional secrecy, even after they cease to exercise their duties.

3.4.5 Selected Data Subject's Rights

The data subjects' rights include the right to information, i.e. the right to know of the existence of the data hold and the identity of the controller, his representatives and any third party that might be given access to the data, the purpose of the processing, and the rights data subjects' have over their data.[258] This right to information also covers situations where data is collected from an open network.[259]

In addition to the right to information, data subjects have the right to have access to their data[260], to request rectification, erasure and block all or specific processing activities [261,] or object to the processing

[250] Article 21.

[251] Recitals 15, 53 and 54 of the GDPR.

[252] Article 3 (1) (a).

[253] Article 3 (1) (b).

[254] Article 3 (1) (c).

[255] Article 3 (1) (c).

[256] Article 3 (1) (c).

[257] Article 3 (3). The controller, when the processing is carried out on its behalf, must choose a processor who provides sufficient guarantees with regard to the technical and organisational security measures relating to the processing to be carried out and must ensure that these measures are complied with;

3- The carrying out of the processing by subcontracting must be governed by a contract or a legal act which binds the subcontractor to the controller and which provides in particular that the subcontractor acts only under the sole instruction of the controller and that the obligations referred to in paragraph 1 above are also incumbent upon him;

4- For the purposes of preserving evidence, the elements of the contract or legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 above shall be recorded in writing or in another equivalent form. [Article 23].

[258] Article 5 (1). This right cannot be exercised in case the processing of personal data is necessary for national defence, security of the State, law enforcement purposes or if there is a law that permits the collection of personal data.

[259] Article 5 (4).

[260] Article 7.

[261] Article 8.

of their personal data all together[262]. In case a data subject has consented to the processing of personal data, she or he has the right to withdraw such consent at any time.[263] Data subjects also have the right not to be subjected to direct marketing without their consent.[264] An exception is direct marketing via e-mail. In this case, the Law allows it as long as the e-mail is collected directly from the data subject in the course of sale or provision of services, and the direct marketing email concerns similar products or services. Also, data subjects must be able to opt-out of direct marketing.

Data subjects have the right not to be subjected to automated decisions when such involve a behavioural assessment, evaluate aspects of one's personality or affect contractual obligations in cases where the data subject had no opportunity to give his opinion.[265]

In case the security of personal data is compromised, data subjects have the right to be informed of data breaches within three days of the data breach.[266]

The aforementioned rights resemble data subject's rights under the GDPR. However, the Law lacks the right to data portability.

3.4.6 Implementation Status

Article 27 of the Law establishes an agency to enforce the Law and any other regulations adopted to complement the Law. In August 2010, the Data Protection Commission (CNDP) was established. In March 2011, the Government published in the official Gazette rules and procedures to operationalise the CNDP. Beyond enforcement of the Law[267], the CNDP is also empowered to give legal and policy opinions to the government and guidance to individuals, public and private sectors on matters relating to the protection of personal data in Morocco[268].

The CNDP is the Permanent Secretariat of the Network of African Data Protection Authorities (NADPA-RAPDP) since 2018 and a member of the Executive Committee of the Global Privacy Assembly (GPA) since 2021.

The CNDP is very active in the region and undertakes different strategies to bring about public awareness and promote the enforcement of the Law. Such initiatives include a two months publicity campaign 'digital trust' launched in 2020 which resulted in over 100 percent increase in the number of complaints to the CNDP and reduced number of notifications by controllers.[269] In July 2020, the CNDP launched the DATA-TIKA[270] project. The project aims to create a platform for exchange of experience and best practices

[262] Article 9.

[263] Article 2 (2).

[264] Article 10.

[265] Article 11.

[266] Articles 2 (5) and 7.

[267] See Articles 27, 28, 30 and 31.

[268] Articles 27 (A) and 29.

[269] World Bank, supra n. 224 at p. 26 et seq.

[270] According to the Global Privacy Assembly Newsletter (vol. 4 no. 1) 2022, the term "Tika" means "trust" in Arabic. Therefore, the objective of the project is to promote digital trust, advance culture and operational dimension of personal data protection to support compliance with laws.

between DPAs and other sectors in data protection. Through DATA-TIKA, the CNDP signed different Memorandums of Understanding with other DPAs from Africa including Niger - *Haute Autorité De La Protection Des Données À Caractère Personnel* (HAPDP); Chad - *Agence Nationale de Sécurité Informatique et de Certification Électronique* (L'ANSICE)[271]; Senegal - Commission de Protection des Données Personnelles (CDP); Burkina-Faso - *Commission de l'Informatique et des Libertés* (CIL)[272]; Benin - *L'Autorité de Protection des Données à caractère Personnel* (APDP)[273]. Additionally, the CNDP signed Memorandums of Understanding with local companies, public and private institutions as well as ministries in Morocco.

Internationally, the CNDP is cooperating with the CoE since 2015. The cooperation involves substantive exchanges as well as supporting the CNDP.[274] The CNDP is also a member of the AFAPDP in which the data protection authorities of French-speaking countries exchange and cooperate.

3.4.7 Conclusion

Morocco is not only ahead of other North African countries in data protection reforms and initiatives, but also tops many other African countries from other regions. The cooperation and involvement of the CNDP with other data protection authorities, regional and international organisations is one of the reasons of Morocco's success. Morocco is also one of the two countries (the other being Mauritius) in Africa to request for an adequacy recognition from the European Commission. In this endeavour, in 2018, the CNDP held a meeting with an EU delegation to assess Morocco's framework for the protection of personal data against the GDPR. The purpose of the assessment was to identify gaps and divergences of the Law against the GDPR and align the Law accordingly. Interestingly, despite its proactivity, CNDP has not shown interest in the regional data protection framework, the Malabo Convention.

3.5 Tunisia

Tunisia is one of the first countries in Africa to adopt a comprehensive data protection law. This section reviews the legal framework established by the data protection law in the protection of personal data in Tunisia.

3.5.1 Political Context of Data Protection

Tunisia got its independence from France in 1956. In 1959, Tunisia adopted the Constitution that established Tunisia as an Islamic state and an integral part of the Greater Maghreb, committed to promote

[271]Marrakech: CNDP Inks Partnerships with African Personal Data Protection Authorities, Agence Moroccain de Presse, Mai 13th 2022.

[272]Morocco: Personal Data - Morocco, Burkina Faso Strengthen Their Cooperation, Maghreb Arabe Presse, June 28th 2022.

[273]Marrakech: CNDP Seals Partnership with Beninese Counterpart, Daily News: Morocco, May 14th 2022.

[274] Soutien à la Protection des Données Personnelles au Maroc, 2022.

human values and human rights.[275] Following the independence in 1956, Tunisia was under a repressive regime of the Constitutional Democratic Rally (CDR) until the 2011 Tunisian Revolution.[276]

Article 9 of the 1959 Constitution guaranteed the inviolability of the home and the secrecy of correspondence. The Constitution did not explicitly provide for the right to privacy. In 2002, the Constitution was reviewed to include the protection of personal data.[277] An action considered by Clément Perarnaud as a strategy by the government to impress the international partners, especially since Tunisia was to hold the World Summit on Information Society in 2005.[278] Two years after the incorporation of data protection in the Constitution, Tunisia adopted a comprehensive framework for data protection[279], the first in the Maghreb region[280].

In 2014, Tunisia adopted a new Constitution. According to this Constitution, Tunisia was to remain an Islamic state with strong ties to the Greater Maghreb with a strong commitment to build a true democratic government that respects human rights.[281] Article 24 of the Constitution continued to protect personal data but added the right to privacy as well. Article 49 of the Constitution obligated the Legislative Assembly to adopt specific laws to ensure the actual enforcement of the right to privacy and data protection (among other constitutional rights). In June 2022, a new draft Constitution was published. The preamble to the Constitution vows to support rights of the people, including the right to self-determination. Article 30 of the draft Constitution provides for the protection of private life, sanctity of homes, confidentiality of communication, and personal data.

3.5.2 Development of and Influence on Data Protection Regulation

Like Morocco, Tunisia has strong trade relations with the EU.[282] Tunisia and the EU have signed several trade agreements and policies, including the EU-Tunisia Association Agreement in 1995[283], the Euro-Mediterranean Partnership[284], and in 1995, the EU and Tunisia started negotiating for a Deep and Comprehensive Free Trade Area (DCFTA)[285]. As a result of their partnership, the government of Tunisia prioritises legal improvement in sectors that may affect EU-Tunisia trade.[286]

[275] Preamble of the 1959 Tunisia Constitution.

[276] Makulilo, supra n. 220 at p. 28 et seq.

[277] Article 9.

[278] Perarnaud, Data Protection in Tunisia: a Legal Illusion?; Centre for Internet and Human Rights (n.d).

[279] Law 2004-63 dated July 27, 2004.

[280] Ibid.

[281] Preamble and Article 1 and 5 of the 2014 Constitution.

[282] Makulilo, supra n. 220 at p. 29 et seq.

[283] The agreement entered into force on 30 March 1998.

[284] Entered in 1995. In 2021, EU and Southern Neighbourhood partner countries started working on renewing their partnership entered in light of the Euro-Med agreement.

[285] European Commission. The EU and Tunisia are Jointly Making Public the Initial Texts of the Future Deep and Comprehensive Free Trade Area.

[286] Perarnaud, supra n. 278.

In an effort to align the Tunisian data protection framework with the EU framework, Tunisia signed and ratified the CoE Convention 108 in 2017 and signed the modernised Convention 108+ in 2019.[287] In 2018, Tunisian Council of Ministers approved a review of the Data Protection Law[288] to align the Law with International standards[289] and specifically the GDPR[290].

Tunisia is a member of the African Union, the Arab League, and the AFAPDP. It has ratified the Banjul Charter, the Protocol establishing the African Court, and other international law instruments providing for the right to privacy such as the International Covenant on Civil and Political Rights and the Convention on the Rights of the Child. In April 2019, Tunisia signed the Malabo Convention but has not yet ratified it.

3.5.3 Nature and Scope of the Law: Loi Organique Numéro 63 en Date du 27 Juillet 2004 Portant sur la Protection des Données à Caractère Personnel

The 2004 Data Protection Law, the *Loi Organique Numéro 63 en Date du 27 Juillet 2004 Portant sur la Protection des Données à Caractère Personnel* (hereinafter 'the Law') established the first comprehensive data protection regime in Tunisia, and also repealed all laws in Tunisia that were contrary to its provisions. In 2007, two Decrees were published to bring the Law into force: Decree No. 2007-3004 which provides for substantive and procedural aspects and Decree No. 2007-3003 establishing *l'Instance Nationale de Protection des Données à Caractère Personnel (INPDP)* as the National Authority for the Protection of Personal Data. The INPDP is the authority responsible for the enforcement of the Law.

The Law reiterates that data protection is an extension of the constitutional right to privacy.[291] Thus, any processing of personal data must be done in a transparent and fair manner, and in respect of human dignity, public liberties, and the Law.[292] In addition, the Law prohibits the use of personal data to harm individuals or their reputation.[293] The Law came into force a year after its promulgation.[294]

By virtue of Article 2, the Law applies to the processing of personal data by individuals and legal entities, whether or not by automated means. The Law does not describe territorial scope of application. However, Article 22 states that controllers and processors must fulfil the following conditions: to have a Tunisian citizenship or reside in Tunisia and have no criminal record. As a consequence, the processing of personal data by a foreign controller and processor is prohibited.

Like the GDPR, the Law categorises data into sensitive[295] and non-sensitive data. Accordingly, the processing of sensitive personal data is prohibited unless the data subject has given an express consent in a written record. Sensitive personal data can still be processed in the absence of the consent where the

[287] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223.

[288] https://www.accessnow.org/tunisia-protecting-personal-data-during-elections-is-at-stake/.

[289] Perarnaud, supra n. 278.

[290] DLA Piper, Data protection Laws of the World, p. 2.

[291] Article 1. The Article insists that every person has the right to the protection of personal data as one of fundamental rights guaranteed by the Constitution.

[292] Articles 1 and 9.

[293] Article 9.

[294] See Article 105.

[295] Article 14.

processing is necessary for historical or scientific purposes, to safeguard the interests of a data subject, for health purposes or when such data is made public by the data subject. In any case, the processing of sensitive personal data requires an authorisation from the DPA.[296]

The Law does not apply to the processing of personal data in a purely domestic context.[297] Other exemptions include the processing of personal data for employment purposes by an employer[298] or for monitoring health status of a data subject[299]. These categories of processing of personal data are exempted from the application of Articles 7, 8, 27, 28, 31 and 47 of the Law.[300] Unlike other data protection laws discussed in this report, this Law regulates the processing of personal data for surveillance purposes.[301] A prior authorisation is required before any video surveillance device is installed. In addition, video surveillance is allowed only on public places and places of collective work (Articles 69 and 70).

In addition, public bodies / authorities, local government and public health institutions, criminal justice and national security agencies have wide-ranging exemptions to the processing of personal data whenever they use prerogatives of public power to accomplish their objectives.[302] In addition, the processing of personal data for scientific purposes is exempted from the scope of the Law, as long as identifiers have been removed.[303]

Core concepts such as 'personal data', 'processing', 'data subject', 'data controller', and 'data processor'[304] correspond with definitions of similar concepts in the GDPR. The Law lacks a definition of sensitive data. However, Article 14 prohibits the processing of category of data usually considered sensitive data. This includes the processing of personal data that reveals the racial and genetic origins, religious beliefs, political, philosophical and trade union belonging or health.

3.5.4 General Principles and Condition for the Processing of Personal Data

Before processing personal data, the Law requires data controllers must obtain an express and written consent of a data subject.[305] In case of data of a child, not only parents and legal guardians can give consent, but also a judge of a Family Court. The judge may give consent even when parents or legal guardians choose to withhold the consent. This is the case when the judge considers the processing of child's data as being in the best interest of the child.[306] The data subject's consent is also required when

[296] Article 15.

[297] Article 3.

[298] Article 16.

[299] Article 17.

[300] These articles require declaration and authorization of data processing activities to the DPA (Articles 7 and 9), consent (Article 27, 28 and 47), information right (Article 31).

[301] Article 70.

[302] Articles 53, 54 and 56.

[303] Articles 66 and 67.

[304] See Articles 4, 5 and 6.

[305] Article 27.

[306] Article 28.

the data processor or controller intends to share data with a third party.[307] The Law specifically prohibits linking the data subject's consent with provision of services or granting of an advantage to the data subject.[308]

In addition to the consent, a prior declaration must be filed with the DPA.[309] Article 7 strictly requires that the filing of the declaration must be evidenced with a receipt or a written proof.[310] In addition, the following processing activities require an authorisation from the DPA: the processing of sensitive personal data[311], a transfer of personal data to a third country[312], or processing personal data for surveillance purposes[313]. Authorisation is required before the processing of personal data commences.[314] In exceptional circumstances, the processing of personal data can be carried out without the consent of the data subject. This includes situations in which the processing is necessary to protect interests of the data subject, when obtaining consent may involve disproportionate efforts, or it is impossible to contact the data subject, for contractual purposes to which the data subject is a party to, or when such processing operation is allowed by another law.[315]

Nonetheless, the processing of personal data must adhere to data processing principles. Articles 10 to 12 set out five principles which are similar to the principles in the GDPR. Accordingly, the processing of personal data must be lawful and fair and must adhere to purpose limitation, data minimisation, and data accuracy. In comparison to the GDPR, the Law is short of the storage limitation, accountability, and transparency principles.

In addition, principles of 'integrity and confidentiality' are not listed on the list of principles. Instead, Articles 18 and 19 oblige the controller to ensure integrity of personal data by putting in place appropriate technical and organisational measures to protect personal data processed by the controller or anyone under his authority. On confidentiality, Article 23 compels anyone processing personal data to adhere to codes of professional secrecy, even after they cease to exercise their duties. Article 45 reinforces the storage limitation principle. Per this principle, personal data shall be destroyed once the purpose of their processing is fulfilled or in accordance with laws and regulations setting storage limitation periods. In the context of data collected though video surveillance, Article 74 provides for specific storage limitations.

[307] Article 47. In this case, data subject has the right to be informed of the purpose of the disclosure of their data to a third party and the rights attached thereto.

[308] Article 17.

[309] Article 7.

[310] If there is no communication within a month of filling a declaration from the DPA to object the processing of personal data that means the processing is allowed.

[311] Although the Law does not have a definition of 'sensitive or special category of data', Article 14 lists data relating to racial, genetic, religious belief, political, philosophical or trade union fraternity and health as category of data that needs special / additional protective measures.

[312] Article 52.

[313] Article 69.

[314] Article 15.

[315] Article 29.

If personal data is being processed for purposes of video surveillance (CCTV), CCTV must be installed in places open to the public (including public transportation or work places) and be placed on the entrance. The installation of the CCTV must be for the purposes of ensuring security, prevention of accidents and monitoring entrances and exits from specific places. The CCTV should not be supported by sound[316] and a clear notice must be given to the public on the presence of the CCTV[317]. Finally, the sharing of CCTV recordings is prohibited unless the data subject gives consent, for criminal justice enforcement, or to facilitate public authorities accomplish their tasks.[318] In all cases, DPA authorisation must be obtained. The GDPR does not have dedicated provisions on CCTV.

The processing of health-related data can only be done by doctors or by people bound by their duties to professional confidentiality.[319]

3.5.5 Selected Data Subject's Rights

Article 31 of the Law confers the right to information of data subjects. In addition to this right, the data subject has the right of access to her / his data. According to Articles 32 and 34, the right to access to personal data can be exercised by data subject's heirs or legal guardian as well. Other rights include the right to rectify, modify, or delete personal data[320], oppose the processing of personal data[321], complete incomplete data and clarify equivocal data[322]. In addition, the data subject as well as respective heirs or legal guardians have the right to be given a copy of the data in an intelligible form. The law explicitly states that the right to access cannot be waived in advance.[323] Nevertheless, the right to access can be limited in case there is a need to protect the data subject or a third party or when the processing of personal data is for scientific purposes.[324] Furthermore, the data subject has the right not to be subjected to direct marketing without their consent.[325]

In case the data subject has consented to the processing of personal data, she or he has the right to withdraw such consent at any time.[326] The Law and GDPR differ in two aspects. Firstly, the Law lacks the rights to breach notification and the right not to be subjected to automated decision-making which are stipulated in Articles 33 and 22 of the GDPR respectively. Secondly, under the GDPR the rights of data subjects are not transferrable to their heirs, as opposed to the Tunisian Law. However, member states may still provide for a transfer of a data subject's right to their heirs by virtue of a derogation provision

[316] Article 71.

[317] Article 72.

[318] Article 73.

[319] Article 63.

[320] Articles 37, 42 and 43.

[321] Article 42.

[322] Article 40.

[323] Article 33.

[324] Article 35.

[325] Article 30.

[326] Article 27.

(cf. Rec. 27 GDPR). Countries such as Italy, Spain, and Hungary have made use of a respective derogation provision to provide for the right of heirs.

3.5.6 Implementation Status

Article 75 of the Law establishes the Data Protection Authority in Tunisia (*L'Instance Nationale de Protection des Données à Caractère Personnel)* (INPDP). Although the budget of the authority is attached to the budget of the Ministry in charge of Human Rights, i.e. Ministry of Justice, the Law stipulates that the INPDP is an independent authority with financial autonomy. The authority was created by Decree No. 3003 of November 2007 but it commenced its function in 2009.

In addition to the enforcement of the Law (authorise / decline the processing of personal data and sanction breaches), the INPDP is empowered to join dissolution, merger, and acquisition proceedings to ensure such procedures do not infringe on personal data protection.[327] This aspect is not provided for in the GDPR. A breach of this Law can lead to civil, administrative, or penal sanctions. Penal sanctions include fine and imprisonment.[328]

3.5.7 Conclusion

Tunisia pioneered data protection reforms in Northern Africa, being the first country to enact a comprehensive data protection law in 2004. This Law differs from the other laws analysed in this report in several aspects; first, it grants a wide scope of derogation to public bodies processing personal data (Chapter V: Section 1 – Articles 53-61); second, a judge has overriding powers in relation to consent of a minor (Article 28); third, the law regulates the processing of personal data by video surveillance (Section IV: Articles 69-74). Nevertheless, the framework established by the Law is similar to the other laws assessed in this report in terms of data protection principles, rights of the data subjects and the comprehensive nature of the Law, i.e. it applies to private, public entities as well as individual processing personal data.

3.6 Libya

Libya does not have a comprehensive framework for the protection of personal data. However, several initiatives towards the protection of personal privacy and data exist. This section provides for an overview of Libya's present legal framework and future prospects for the development of a comprehensive data protection framework.

3.6.1 Political Context of Data Protection

In 2011, the Arab Spring that had sparked in Tunisia also brought changes to Libya, as the 42-year-long leadership of Colonel Muammar Gaddafi was overturned. In the four decades of Gaddafi's leadership, the country was ruled according to Gaddafi's Green Book on political philosophy, which linked public

[327] Article 60 and 53. This power is limited for mergers and dissolutions by public authorities, local government and administrative public institutions, including health public institutions.

[328] See Chapter VII of the Law.

institutions with the people's committee as a form of direct popular democracy; a system that did not permit the establishment of any independent organisation.[329]

Following the end of Gaddafi's leadership, the country embarked on institutional change beginning with the establishment of the National Transitional Council (NTC) and the publication of an Interim Constitution in 2011.[330] The Interim Constitution declares Libya as an Islamic state and Shari'a (Islamic Jurisprudence) as the source of law.[331] The preamble states Libya's mission as to 'retrieving all the rights looted by Al-Gaddafi and his collapsed regime', and establish a political democratic regime[332] that safeguards human rights and fundamental freedoms. One approach to ensure this ambition is by joining regional and international declarations and covenants which protect human rights.[333] To honour this promise, Libya joined the UN Human Rights Council for a three-year term beginning 1 January 2020, signalling its commitment to enforce human rights and cooperate with human rights organisations.[334]

In 2020, two rival fractions in Libya signed a permanent ceasefire agreement, marking the end of the second Lybian civil war, a military conflict between troops and militias of the government of Fayiz as-Saraj under the United Nations-recognised *Government of National Accord* (GNA), which controls parts of western Libya with the capital Tripoli, and the troops of the ruler of eastern Libya, Khalifa Haftar. The 'government' of then-prime minister Abdullah Al-Thani is located in the Eastern city of Tobruk, supported by the Libyan *House of Representatives* (HoR) and is backed by Khalifa Haftar's *Libyan National Army* (LNA) forces.

Starting late 2020, a series of intra-Libyan meetings called *Libyan Political Dialogue Forum* (LPDF) took place and political negotiations were held. In February 2021, the provisional Government of National Unity (GNU) was formed and Abdulhamid Dbeibah was selected as an interim Prime Minister.[335] The GNU was supposed to organise the country's first presidential election, originally scheduled in December 2021 but then delayed to June 2022.[336] Dbeibah called for a new Constitution after the draft Constitution of 2017 was rejected by the HoR. [337] In February 2022, Fathi Bashagha was appointed as Prime Minister.[338] Bashagha formed a new government which marked the end of the GNU.[339] It is yet uncertain how this new government will impact the development of the country and human rights situation; presidential

[329] Nyman-Metcalf, Assessment of Media Legislation in Libya, 2015, p. 7.

[330] The preamble states that the Declaration is temporary and is to be replaced by a permanent constitution adopted through a referendum.

[331] Article 1.

[332] Article 4.

[333] Article 7.

[334] Ministerie van Buitenlandse Zaken, Country of Origin Information Report on Libya, June 2020, p. 9.

[335] BREAKING: New Unified Libyan Government Selected by LPDF in Geneva, Libya Herald, February 5th 2021.

[336] Libya Electoral Commission Dissolves Poll Committees, Aljazeera, December 21st 2021.

[337] Libyan PM Wants Constitution before Elections, France 24, January 23rd 2022.

[338] Libya Parliament Appoints Bashagha as New PM, Daily Sabaha, February 2nd 2022.

[339] Libya's Parliament gives Confidence to Bashagha's Government; Libya Observer, March 1st 2022.

elections scheduled for December 2021 have repeatedly been postponed and the two rival factions have repeatedly violently clashed, raising fears of a return to the civil war.

On the right to privacy, Article 11 of the Interim Constitution of 2011 protects sanctity of dwelling houses and homes while Articles 12 and 13 protect individual privacy of citizens. Article 12 prohibits the state from spying on citizens except by a causal judicial warrant and in accordance with the provisions of the law. Article 13 protects the privacy of correspondence (including telephone calls and any other means of communication) from being monitored or confiscated without legal justification and judicial warrant.
Although the 2011 Constitution was intended to be temporary, the political situation prevented the adoption of a permanent constitution. In 2014, the Constitutional Assembly was established and the drafting of the Constitution began in the same year.[340] In July 2017, the Constitutional Assembly presented a final draft of the Constitution but it could not be submitted for approval by popular referendum. Unfortunately, to date, no permanent constitution has been adopted.[341]

3.6.2 Status of Data Protection Regulation

As already mentioned, Libya does not have a comprehensive data protection framework. However, there is a realistic possibility that a data protection framework will be developed in the near future. In June 2021, the Ministry of Justice working together with the Central Bank of Libya (CBL) announced the Cyber Libya Project. The project intends to draft a package of cyber laws which includes a data protection law.[342] In addition, in 2013, Libya established the National Information Security and Safety Authority (NISSA).[343] NISSA is 'responsible for safeguarding the integrity, availability and resilience of ICT infrastructure, resources, services and data in Libya.' In 2019, NISSA launched a data protection manual for the public and private sector.[344] Unfortunately, we were unable to get hold of the manual to assess its content. The last update the authority shared on their website was a meeting with the Minister of State for Institutional restructuring, Dr. Iman Bin Younis. During the meeting, they discussed NISSA's 'powers and its role in preserving the safety of information security in state institutions in general'. In this context, NISSA was seeking to obtain institutional quality.[345] The objective is to extend NISSA's regulatory power and make it an information regulator for Libya.
Presently, there are laws with data protection and privacy provisions, but these are old laws, passed before the 2011 revolution. For example, the Telecommunication Law[346] provides for confidentiality of communication and prohibits interception, monitoring or altering of individual communications without

[340] Nyman-Metcalf, supra n. 329 at p. 9 et seq.

[341] Dorda/Crowley, Inside Libya: Special Edition, Konrad-Adenauer-Stiftung e. V.

[342] Cyber Libya Project Launched; Libya Herald June 23rd 2021.

[343] By a Decree No.28 of the Ministerial Council of the State of Libya.

[344] Libya's Data Protection Authority NISSA Launches Information Security Guide; Libya Herald, August 10th 2019.

[345] NISSA News, 2020 at https://nissa.gov.ly/en/bin-younis-meets-the-director-general-of-the-national-authority-for-information-security-and-safety-to-discuss-the-authoritys-terms-of-reference/

[346] Law No. (22) of 1378 FDP (2010 AD).

a warrant of a competent court.[347] Article 16 of the Telecommunication Law prohibits service providers from processing personal data without legal basis or the consent of the data subject. The Article also creates an accountability framework by tasking the service providers to ensure the protection of personal information in their custody. The Telecommunication Law also prohibits disclosure of personal data by service providers. Breach of these obligations can lead to an imprisonment term and a fine.[348]

3.6.3 Constitutional Guarantees

The Interim Constitution of 2011 guarantees the protection of personal privacy, privacy of dwelling houses as well as privacy of correspondence and communications.[349] The proposed 2017 Constitution also guarantees the protection of personal privacy and that of dwelling houses. It also protects personal data, individual communications, and correspondence.[350] Furthermore, the proposed Constitution declares the primacy of international laws over local laws, as long as they do not contradict Shari'a law. The Constitution remains superior to both international law and Shari'a.[351]

Libya ratified the International Covenant on Civil and Political Rights[352] and its first optional Protocol, the Convention on the Rights of the Child[353], the Banjul Charter[354], the protocol establishing the African Court[355], and the African Charter on the Rights and Welfare of the Child[356]. Except for the Banjul Charter, all these instruments provide for the right to privacy. By virtue of Article 36 of the proposed Constitution, they have a direct application and are supreme to local laws in case there is a conflict between the two regimes.

3.6.4 Human Rights Implementation Aspects

The 2014[357] and 2020[358] United States country reports on Libya's Human Rights practices describe the absence of implementation of human rights in Libya. This includes the lack of implementation of the right to privacy as provided in the interim Constitution. The reports depict the ongoing unlawful surveillance of individuals through interception and tapping of their communications and illegal home searches. These acts are performed by GNA- aligned groups, LNA-aligned groups, criminal groups, and other non-

[347] Article 15.

[348] Article 26.

[349] Article 11-13.

[350] Article 36.

[351] Article 13 of the proposed Consolidated Draft Constitution Submitted by a number of members of the Constitutional Consolidation Committee Al Bayda – 16 April 2017 AD.

[352] Ratified in 1976.

[353] Ratified in 1993.

[354] Ratified in 1986.

[355] Ratified in 2003.

[356] Ratified in 2000.

[357] Country Reports on Human Rights Practices for 2014 for Libya.

[358] Human Rights and Labor Country Reports on Human Rights Practices for 2020, pp. 13-14.

state actors.[359] In addition, these groups reinforce road barricades and stop and search individuals' communication devices (such as mobile phones and laptops). Unfortunately, as a result of impunity, these groups are not held accountable for violation of privacy (among other parallel offence committed during the illegal search and surveillance).[360] Despite the continued degradation of human rights and threats to human rights defenders, the EU is helping Libya to improve the situation. For example, the EU is supporting Libya in reporting to the UN treaty bodies and in establishing a national report mechanism, human rights advocacy, and transitional justice. Additionally, the EU offered support to the UN in establishing the Working Group on Human Rights and International Humanitarian Law for Libya.[361]

3.6.5 Conclusion

There is evidence of efforts to reform Libya's data protection law(s) (or generally, the digital, legal and regulatory framework). This can be observed in the introduction of Article 36 in the proposed Constitution of 2017 which specifically guarantees the protection of personal data. Another evidence is the launch of the Cyber Libya Project with an intention to review ICT laws and the proposed extension of NISSA's mandate to include protection of personal data. Also, NISSA's efforts to draft the personal data protection manual. Given the political will, there is a great chance that Libya will experience legal reforms in ICT related laws including data protection.

3.7 Sudan

Like Libya, Sudan is one of the African countries that does not have a comprehensive data protection law in place. But the Constitution and the law(s) concerning cybercrime guarantee the right to privacy. This section provides for the current state and prospects for the adoption of a comprehensive data protection law in Sudan in the near future.

3.7.1 Political Context of Data Protection

The year 2019 marked a new era in the history of human rights in Sudan. The end of Omar al-Bashir, who was removed from presidency, marked the end of three decades of gross human rights violations.[362] To demonstrate its commitment to human rights and accountability, the new transitional government adopted a transitional Constitutional Charter in the same year. The Constitution Charter asked the transitional government to dismantle the old regime characterised with a 'structure for consolidation of power (tamkeen), and to build a state of laws and institutions.' This included 'a legal reform, the rebuilding and development of human rights and the justice system, and to ensure the independence of the judiciary as well as the rule of law.'[363]

[359] Ibid.

[360] Ibid.

[361] European Commission, supra n. 170 at pp. 47-48 et seq.

[362] SOAS, Legal and Institutional Reforms in Sudan: Policy Briefing, March 2021, p. 6.

[363] Article 8 (5) and (15).

In 2020, the transitional government published in the Official Gazette the Miscellaneous Amendments (Repeal or amend the provisions restricting freedoms) Law No 12 of 2020 (hereinafter 'MAL'). MAL amended several oppressive laws. The purpose of MAL was to align Sudanese laws with international human rights standards.[364] Article 1 of MAL states the objective of MAL as to 'repeal or amend the provisions restricting freedoms.' Alongside MAL, the country also adopted another law that establishes an authority to implement legal reforms and improve the justice system. This is the Law of the Commission for the Reform of the Legal and Justice System of 2020 (hereinafter 'the Justice System Law').[365] This Commission is tasked with reforming the justice system to ensure the rule of law and to promote judicial independence and accountability.[366]

Article 42 (2) of the Constitutional Charter declares that '[a]ll rights and freedoms contained in international and regional human rights agreements, pacts, and charters ratified by the Republic of Sudan shall be considered an integral part of [the] Charter.' Article 15 guarantees the right to privacy of an individual and of family life including in the homes and correspondence of citizens.

To support Sudan's efforts to reform its justice and human rights system, the Max Planck Foundation for International Peace and Rule of Law has been assisting Sudan with constitutional reform; including legal and institutional capacity building.[367] The latter includes training of judicial personnel, i.e. judges, attorneys, and prosecutors.[368] Despite these efforts, the current political situation makes it unlikely for the development of a comprehensive data protection framework. Sudan is a conflict-prone country and currently facing political unrest. The 'Sovereignty Council of Sudan', who took over from the 'Transitional Military Council (TMC)' in 2019, was dissolved in October 2021 through a *coup d'état*. It was supposed to lead the country through the process of transitioning to democracy until 2022.[369] Today, Sudan is still under military control. Regional and international organisations, including the United Nations Integrated Transition Assistance Mission in Sudan (UNITAMS), the African Union (AU), and the Intergovernmental Authority on Development (IGAD) are working together to help Sudan towards a peaceful, 'civilian-led transition to democracy'[370]. In the current state, data protection is not expected to be a priority in Sudan. There is a possibility of a change in the political and human right situation. In 2020, the EU – through the European Instrument for Democracy and Human Rights project – funded several projects to promote democratisation and human rights reforms in Sudan.[371] The EU also financed the operation of the Office of the UN High Commissioner for Human Rights in Sudan for the period of 2021-2022 and the Ministry

[364] Ministry of Justice, the Official Gazette, Issue No. 1904 on 13-07-2020.

[365] Law No. (13) of 2020.

[366] Article 4 of the Law No. (13) of 2020.

[367] Max Planck Foundation, Sudan: Support to Constitutional and Legal Reform in the Republic of the Sudan, project started in 2013.

[368] Ibid, Legal Training of Judges, Attorneys, Prosecutors and Lawyers in Public Service at All Levels of the Judiciary and the Administration in Sudan, project started in 2020.

[369] Sudan's Burhan Declares State of Emergency, Dissolves Government, Reuters, October 10th 2021.

[370] Press Statement, US Department of State, United States Support for the Sudanese Tripartite Political Process, May 9th 2022.

[371] European Commission, supra n. 170 at pp. 156-157 et seq.

of Justice to implement legal reforms. The Commissioner assists Sudan towards human rights monitoring and supports local organisations working in the human rights field.[372]

3.7.2 Status of Data Protection Regulation

Although Sudan does not have a comprehensive data protection framework, there are laws that protect privacy and personal data. One of them is the Penal Code of 1991 on offences that are related to the infringement of personal freedoms. Specifically, section 166 makes it an offence to eavesdrop, to watch others in their homes, or read the letters of other persons. A conviction for these offences could lead to an imprisonment term of not more than six months or a fine or both. Similar protections are enshrined under section 34 of the Telecommunication Act of 2001. Furthermore, the Child Act of 2010 protects the privacy of a child in court proceedings. Section 79 insists on protecting privacy of the child during trial and prohibits the publication of any information relating to child's appearances in court unless a permission to publish is granted by the court. Section 83 (1) (e) prohibits the publication of information relating to children who are victims. This provision emphasizes on protecting a child's privacy and identity.[373]

3.7.3 Constitutional Guarantees

The right to privacy is guaranteed by the Constitution Charter of 2019. Article 55 prohibits interference with private family life of individuals or their homes or their correspondence, except when such interference is permitted by a law. According to Article 66, on the one hand, the Constitutional Court has the jurisdiction to adjudicate on matters relating to human rights and on the other hand, the Human Rights Commission oversees that these rights are upheld.

In addition to the Constitution Charter, Sudan ratified the International Covenant on Civil and Political Rights, the Arab Charter on Human Rights, the African Charter on the Rights and Welfare of the Child, the Cairo Declaration on Human Rights in Islam, and the Arab Convention of Anti-Information Technology Crimes. They all contain provisions on the right to privacy.

3.7.4 Enforcement Aspects

The efforts made since the year 2019 to restore human rights and legal institutions have been substantively hampered by the *coup d'etat* of 2021. According to the statement of the UN High Commissioner for Human Rights, human rights violations increased since then. The situation is eroding also due to total impunity granted to security and law enforcement agencies.[374] The declaration of state of emergency also granted the Sudanese law enforcement, security, and intelligence agencies 'law enforcement powers and temporary immunity from prosecution.'[375] These powers led to the derogation of the right to privacy

[372] Ibid, p. 157.

[373] See also Abdelhameed/Hassan/Bagheri; The Accused Privacy Rights in the Sudanese Legal System, *Journal of Politics and Law* 12 (2019).

[374] Bachelet, Oral update on the situation of human rights in the Sudan at the 49th Session of the Human Rights Council, March 7th 2022. See also, The State of the World's Human Rights, Amnesty International Report 2021/22.

[375] Ibid.

(among many others) as provided in the Constitution. The law enforcement, security, and intelligence agencies invade homes and hospitals and arbitrarily arrest and detain civilians, including children.[376] These violations were reported to have been reduced after 2019.[377] A report by the United States Department of State – The Bureau of Democracy, Human Rights and Labor stated that 'this type of activity [arbitrary or unlawful interference with privacy, family, home, or correspondence] appeared to have ceased, or been dramatically reduced, under the CLTG (Civilian-Led Transitional Government).[378]

3.7.5 Conclusion

The situation in Sudan in general and with respect to the possibility of a data protection framework and / or for legal reforms is hard to determine. This does not diminish the possibility completely, but at this moment (in time) it probably is not – for understandable reasons – at the top of the political agenda.

[376] Bachelet, supra n. 374.

[377] United States Department of State - Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2020, p. 8.

[378] Ibid.

4 General Observations, Comparison, and Recommendations

The assessment indicates substantive similarities between the GDPR and the data protection frameworks of the five countries with comprehensive data protection frameworks. In terms of scope, the laws have similar material scope of application. They all apply to public and private entities, categorise data into sensitive and non-sensitive data, have natural personal (as opposed to legal persons) as data subjects and apply to automated and non-automated data. Egypt differs slightly from the other four countries in the latter (aforementioned) aspect. The Egyptian Law does not apply to purely manual files. Substantive divergence is seen in the exemptions (below).

Material Scope of the Laws

	GDPR	Algeria	Egypt	Mauritania	Morocco	Tunisia
	Entities Covered					
Public entities	Yes	Yes	Yes	Yes	Yes	Yes
Private entities	Yes	Yes	Yes	Yes	Yes	Yes
	Data Subject					
Natural person	Yes	Yes	Yes	Yes	Yes	Yes
Juristic person	No	No	No	No	No	No
	Categories of Data					
Sensitive data	Yes	Yes	Yes	Yes	Yes	Yes
Non-sensitive data	Yes	Yes	Yes	Yes	Yes	Yes
	Type of Data Processing					
Electronic data	Yes	Yes	Yes	Yes	Yes	Yes
Non-electronic data	Yes	Yes	No	Yes	Yes	Yes
	Scope of Exempted Processing activities					
Complete exempted	NDJ	NDJ	NDJ	NDJ	NDJ	NDJ
Partially exempted	MD	-	-	-	JSS	ELNH
Not exempted	-	JLSs	SNs	NJL	HSNs	-

Key:
1. NDJ: In purely domestic context, national security, justice, and law enforcement purposes.
2. MD: Member states have discretion to determine conditions and scope for the processing of personal data for historical, literary, artistic, and scientific purposes.
3. JSS: Journalistic, statistic, and scientific purposes.
4. ELNH: Employment, law enforcement, national security, and health purposes.

5. JLSNs: Journalistic, literary, scientific purposes, and the processing of personal data by NGOs.
6. SNs: Scientific purposes and the processing of personal data by NGOs.
7. NJL: National security, justice, and law enforcement purposes.
8. HSNs: Historical, scientific purposes, and the processing of personal data by NGOs.

Egypt is the only country whose data protection law has extraterritorial application. This can be attributed to the fact that Egyptian Law is the only (law) adopted in the GDPR era. Algeria, Mauritania, Morocco, and Tunisia adopted their laws before the GDPR, during the 1995 EU Directive period, and hence it is only logical that their frameworks are modelled after the Directive which had no extraterritorial application (other than the restrictions on cross border flow of data to third countries).

There is a striking alliance in the omission of 'transparency' principle in the laws. All the five countries provide for similar data protection principles, whether within the specific section that itemises the data protection principles or in form of an obligation of the data controllers. But none of the laws include transparency, neither as a data protection principle nor as an obligation of the data controllers.

See the table below:

Data Protection Principles

GDPR	Algeria	Egypt	Mauritania	Morocco	Tunisia
Lawfulness, fairness and transparency					
Yes	Yes T/O	No	Yes T/O	Yes T/O	Yes T/O
Purpose limitation					
Yes	Yes	Yes	Yes	Yes	Yes
Data Minimisation					
Yes	Yes	Yes	Yes	Yes	Yes
Data Accuracy					
Yes	Yes	Yes	Yes	Yes	Yes
Storage Limitation					
Yes	Yes	Yes	Yes	Yes	NDP
Integrity and Confidentiality					
Yes	Yes	NDP	Yes	Yes	NDP
Accountability					
Yes	Yes	NDP	NDP	NDP	Yes

Key:

1. YES T/O: Yes. Transparency is omitted.
2. NDP: Not on the list of data protection principles but as an obligation of data controllers.

In all laws, data subject's consent is the primary basis for the processing of personal data. Algeria and Tunisia provide for consent of a judge on behalf of a minor. This is alongside parental and guardian consent. Also, all laws provide for circumstances where personal data can be processed in absence of a data subject's consent. In such situations, the law provides specific circumstances as 'legal basis' for the processing of personal data. The legal basis for the processing of personal data varies slightly from one law to the other. The following legal basis appears in all laws; these are the processing of personal data for contractual purposes to which the data subject is a party, in order to protect vital interest of a data subject, and to perform a task carried out for reasons of public interests.

The table below contains an overview:

Basis for the Processing of Personal Data

GDPR	Algeria	Egypt	Mauritania	Morocco	Tunisia
Data Subject's Consent					
Yes	Yes	Yes	Yes	Yes	Yes
Consent of a Minor: Parents or Guardians					
Yes	Yes	Yes	No	No	Yes
Consent of a Minor: Judge or a Court					
No	Yes	No	No	No	Yes
Legal Basis for the Processing of Personal Data					
Yes	Yes	Yes	Yes	Yes	Yes
Data Protection Mandatory Approval: Prior Authorisation					
No	Yes	No	Yes	Yes	Yes
Data Protection Mandatory Approval: Prior Declaration to the Data Protection Authority					
No	Yes	No	Yes	Yes	Yes

In all five countries, data subjects have the following rights:
Information right, access right, right to correct and right to erase, right to withdraw consent, right to object or block the processing of personal data, the right to breach notification, and the right not to be subjected to direct marketing data. The right not to be subjected to automated decisions is missing in Egypt, Morocco, and Tunisia. Algeria, Mauritania and Tunisia provide for the right to 'transfer' these rights to the heirs of the data subject upon her / his death. This is not the case in the GDPR, Morocco, and Egypt.

See the table below:

Data Subject Rights

GDPR	Algeria	Egypt	Mauritania	Morocco	Tunisia
Information Right					
Yes	Yes	Yes	Yes	Yes	Yes
Access Right					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Correct Information					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Request Erasure of Information					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Object / Block Data Processing Activities					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Withdraw Consent					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Data Portability					
Yes	No	No	No	No	No
Right not to be Subjected to Automated Decisions					
Yes	Yes	No	Yes	No	No
Right not to be Subjected to Direct Marketing					
Yes	Yes	Yes	Yes	Yes	Yes
Right to Receive Breach Notifications					
Yes	Yes	Yes	Yes	Yes	Yes
Right of Heirs (Succession Rights)					
No	Yes	No	Yes	No	Yes

One difference stands out in relation to the enforcement of the data protection laws in North African countries and the GDPR. All the five laws assessed include imprisonment as a penalty for the breach of the data protection law. The GDPR does not contain provisions for imprisonment – also because criminal law is a national competence, so that criminal law penalties can be found on the national level[379]. So far, we did not come across any case where a controller or processor has been imprisoned for the breach of the data protection law in any of the five countries. Further, all the five laws provide for individual redress mechanisms whereby a data subject can either lodge a complaint with a data protection authority or a court of competent jurisdiction.

See the table below:

Redress Mechanisms

GDPR	Algeria	Egypt	Mauritania	Morocco	Tunisia
Individual Right of Action					
Yes	Yes	Yes	Yes	Yes	Yes
Data Protection Authority: Administrative Powers to Enforce the Law					
Yes	Yes	Yes	Yes	Yes	Yes
Civil Remedy from a Civil Court					
Yes	Yes	Yes	Yes	Yes	Yes
Criminal Sanctions					
(Yes, in parts on national level)	Yes	Yes	Yes	Yes	Yes
Imprisonment					
(Yes, in parts on national level)	Yes	Yes	Yes	Yes	Yes
Alternative Dispute Resolution System					
No	No	Yes	No	No	No

[379] Cf. § 42 German Federal Data Protection Law.

5 Summary and Outlook

This report presents legal status and trends of data protection laws and the regulatory framework of seven North African countries – including a comparative analysis of five countries with comprehensive data protection laws. The analysis was mainly limited to the 'law in the books' – providing details of the content and context of the laws, their convergences and divergences as well as their alignment with the GDPR. An assessment of actual implementation of these laws was beyond the scope of this analysis – and is reserved for future research. Nevertheless, the current analysis allows a general overview of the data protection situation in North Africa and a future outlook.

1. Other than Egypt, the data protection laws in four countries analysed in this report were adopted before the GDPR. Given their similarities to the EU data protection framework, it is safe to assume that the laws in the four countries are based on the 1995 Directive which was replaced by the GDPR. This being the case, there is a need to revisit these laws to determine their robustness in light of the current technological and legal development(s) beyond the region.

2. In Libya and in Sudan, no reforms in the data protection field have happened in a period in which other African countries were reforming. The main reason is that the two countries are prone to internal civil and political unrest. Nevertheless, given the political and economic pressure on the need to protect personal data, it is possible to see reforms in the very near future. Given the involvement of the EU in the area and the extra-territorial application of the GDPR, it is possible that any reform would follow the suit of the other North African countries with an adoption of a law / establishment of a data protection framework similar to the EU data protection framework (despite – arguably – shortcomings of the EU legislation in substance).

3. The laws in the five countries analysed in this report, resemble the GDPR very closely. Nevertheless, minor divergences (such as the omission of the transparency principle and the Judge's power to give consent on behalf of a minor in Tunisia and Algeria) exist. These divergences might show local needs and African legal culture in general. In addition, and especially, a transfer of data subject rights to heirs (in Algeria, Mauritania and Tunisia) is an aspect that is not explicitly present in the EU data protection framework – neither in the GDPR (which leaves it to the member states) nor in the previous Directive. As stated in the African Charter of Human and Peoples Rights (Article 29 (1)), a family is a custodian of rights and has the right to ensure the respect of the family and its harmonious development. By exercising rights to data protection of a deceased, heirs are in the position to protect the family from the processing of data of the deceased that might bring disgrace to the dead's and the family's honor.

4. Also, despite sharing the same core data principles and similar enforcement frameworks, we do see enforcement challenges across the region (and beyond). These challenges include the lack of / delay in the establishment of data protection authorities to implement data protection laws, lack of funds and of qualified personnel, and lower concessions with regional data protection initiatives such as the Malabo Convention.

5. Lastly, none of the five countries have received an EU adequacy decision, despite the similarities in the legal content of their laws to that of the GDPR. It is clear from Article 45 (2) GDPR that a country – if it wants a respective decision – needs to go beyond approximating the GDPR (or any other data protection legal framework). The adequacy assessment of a data protection framework looks at the data protection beyond the mere legal text.

In order to harmonise data protection frameworks, to promote data flows within the North African region (and beyond) and to increase trust in the use of technology, there is a need for the North African countries to work together towards a common approach concerning data protection. As a first step, a deeper cooperation between DPAs and legislators in the development and enforcement of data protection laws could be an option to proceed. Any created harmonised legal framework across the region should also bear the compatibility of such a framework with other regional and international data protection frameworks in mind. The recently adopted African Union Data Policy Framework, whose objective is to create a policy framework to support 'a consolidated data environment and harmonised digital data governance system', may be just the right step towards resolving these disparities.[380]

[380] The AU Data Policy Framework was endorsed by the Executive Council during its 40th Ordinary Session held on 2 – 3 February 2022 through Decision with reference EX.CL/ Dec.1144(XL) in Addis Ababa.

Annex: The GDPR

In 2016, the EU adopted the EU General Data Protection Regulation (GDPR), replacing the 1995 Data Protection Directive 95/46/EC. The GDPR came into effect on 25 May 2018. The framework established by the GDPR for the protection of personal data consists of core concepts and rules, i.e. data protection principles, rights of data subjects and duties of data controllers / data processors, rules on cross-border data transfer, and independent data protection agencies and provides for sanctions for non-compliance. The core terms of the GDPR include 'personal data', 'processing of personal data', 'data subject', 'data controller', 'data processor', 'recipient', and 'sensitive data' (Article 4 GDPR).

General Principles

Article 5 of the GDPR sets out the general principles of processing and on which the regulatory take of the regulation is based on: "lawfulness, fairness and transparency", "purpose limitation", "data minimization", "accuracy", "storage limitation", "integrity and confidentiality", and "accountability". In general, the principles of Article 5 of the GDPR are mirrored by manifold specific rules within the GDPR.

The principle of "lawfulness, fairness and transparency" can be considered to be the most important one. Any processing of personal data needs a justification to be lawful. Any data processing is forbidden from the outset, if no justification is given. Against this background, Article 6 of the GDPR sets out the parameters for a lawful processing – pointing to the main and elementary justification ground: the data subject's consent. Other grounds for justification are – inter alia – linked to contractual performance, legal obligations and other legal justifications as well as (overweighing) legitimate interests. Fairness and transparency means that the data subject should be made aware of the processing of their personal data – in a clear, easily accessible, concise, transparent, and intelligible manner. The principle of transparency, for example, is substantiated by – inter alia – Article 12 of the GDPR ("Transparent information, communication and modalities for the exercise of the rights of the data subject") as well as the data subject's rights to information and access according to Articles 13, 14, and 15 of the GDPR.

Another principle points to the central limit of processing of personal data: the specific purpose of processing (Article 5(1)(b)). According to Article 5(1)(c), collection of personal data is restricted to what is necessarily adequate, relevant, and not excessive in relation to the purposes for which data is processed. The data accuracy principle (Article 5(1)(d)) obliges data controllers to ensure that processed data is accurate and up-to-date; the storage limitation principle (Article 5(1)(e)) requires that personal data should not be kept for longer than is necessary for the purposes for which is processed. According to the data security principle (integrity and confidentiality; Article 5 (1) (f)), data controllers / data processors are required to ensure that personal data is kept and processed in a manner that ensures its security from unauthorised access, unsanctioned processing, accidental loss, or destruction. Finally, data controllers are accountable for the processing of personal data (Article 5(2)). This includes mechanisms to produce evidence of a compliant processing – inter alia, by documenting the activities to enable an audit or an assessment.

Data Subject's Rights

The GDPR gives the individual, i.e. the data subject, several rights of action. Data subjects have the right to information (Articles 12, 13, 14), the right to access their personal data (Article 15), the rights to correct, delete, stop or restrict the processing of personal data, right to be forgotten and right to data portability (Articles 16-21). With regards to the processing of personal data, data subjects have the right not to be subjected – with exceptions – to automated decision-making that might have a (negative) legal effect on them.

Enforcement

If the processing of personal data fails to abide to the abovementioned principles or any other violation of the GDPR occurs, the data subject has the right to lodge a complaint with the competent authorities. Similarly, if a data subject is denied the right to exercise any of the abovementioned rights, she/he has the right to bring a respective complaint.

Data protection authorities enforce the GDPR as a public task. The respective authority is expected to be an independent administrative agency with powers to issue administrative sanctions (such as enforcement notices and fines; see Chapter 6 of the GDPR). For example, the general principles set out above are fully enforceable – non-compliance may lead to a fine according to Article 83(5)(a) of the GDPR.

Next to public enforcement, private enforcement is also possible (Article 82 GDPR).

International Dimension of the GDPR

The GDPR contains two main provisions that have a significant effect on countries outside the EU as well as non-EU companies which have to comply with GDPR standards to be able to target EU customers / trade partners. Article 45 of the GDPR restricts the flow of personal data to countries outside EU (the so called "third countries") unless such country provides an adequate level of protection similar to that provided by the GDPR. The European Commission (EC) is the organ that decides whether or not a third country provides an adequate level of protection. Another far-reaching provision leads to an "extra-territorial" application of the GDPR: According to Article 3(2)(a) and (b), the GDPR has a direct application to data processors located in non-EU countries whenever goods or services are offered to European residents or when a profiling of EU residents' behaviours inside the EU takes place.

These two provisions presumably have led to "pull-" and "push-effects" towards the GDPR – resulting in non-EU countries adopting GDPR lookalike / similar frameworks for data protection – often in aiming for the "adequate level of protection". This is especially the case for countries with trade relations with the EU to ensure continued and unimpeded trade with the EU.

Scope

The comparative assessment in this report is confined to the abovementioned aspects, i.e. core concepts and basic data protection principles, rights of data subjects and the nature, status, and implementing powers of established data protection authorities.

Bibliography

'N.N' Sudan's Burhan Declares State of Emergency, Dissolves Government, Reuters, October 10th 2021; https://www.reuters.com/world/africa/sudans-burhan-declares-state-emergency-dissolves-government-2021-10-25/

'N.N' Morocco: Personal Data - Morocco, Burkina Faso Strengthen Their Cooperation, Maghreb Arabe Presse, June 28th 2022; https://allafrica.com/stories/202107020205.html

'N.N' Marrakech: CNDP Inks Partnerships with African Personal Data Protection Authorities, Agence Moroccain de Presse, Mai 13th 2022; https://www.mapamazighe.ma/en/actualites/general/marrakech-cndp-inks-partnerships-african-personal-data-protection-authorities

'N.N' Marrakech: CNDP Seals Partnership with Beninese Counterpart, Daily News: Morocco, May 14th 2022; https://dailynewsmorocco.com/marrakech-cndp-seals-partnership-with-beninese-counterpart/

'N.N' Libya Electoral Commission Dissolves Poll Committees, Aljazeera, December 21st 2021, https://www.aljazeera.com/news/2021/12/21/libya-electoral-commission-dissolves-poll-committees

'N.N' Libya Parliament Appoints Bashagha as New PM, Daily Sabaha, February 2nd 2022, https://www.dailysabah.com/world/africa/libya-parliament-appoints-bashagha-as-new-pm

'N.N' Libyan PM Wants Constitution before Elections, France 24, January 23rd 2022; https://www.france24.com/en/live-news/20220123-libyan-pm-wants-constitution-before-elections

Abdelhameed/Hassan/Bagheri, The Accused Privacy Rights in the Sudanese Legal System, *Journal of Politics and Law* 12 (2019).

Agence Mauritanienne d'information (AMI), Le Président et les Membres de l'Autorité de Protection des Données Personnelles Prêtent Serment, July 5th 2022.

Amnesty International, The State of the World's Human Rights, Amnesty International Report 2021/22; https://www.amnesty.org/en/location/africa/east-africa-the-horn-and-great-lakes/sudan/report-sudan/

APC/Hivos, Global Information Society Watch, 2009.

Assad, Libya's Parliament gives Confidence to Bashagha's Government; Libya Observer, March 1st 2022; https://www.libyaobserver.ly/news/libya%e2%80%99s-parliament-gives-confidence-bashaghas-government

Bachelet, Oral update on the situation of human rights in the Sudan at the 49th Session of the Human Rights Council, March 7th 2022.

Badawy, The Technology, Media and Telecommunications Review: Egypt in Murchison, (ed), The Technology, Media and Telecommunications Review, 12 (2022).

Baig,10 Strictest Data Privacy Laws By Country in 2022; https://www.techopedia.com/10-data-privacy-laws-every-business-should-know/2/34759#10-egypt

Bøås, The State of Play of EU-Mauritania Relations, 2017.

Boshe/Hennemann/von Meding, African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward, GPLR 3 (2022).

Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, Stan. Tech. L. Rev. 389 (2021).

Chenaoui, Moroccan Data Protection Law: Moving to Align with EU Data Protection?, IAPP; https://iapp.org/news/a/moroccan-data-protection-law-moving-to-align-with-eu-data-protection/

Council of Europe Newsroom, Welcome to Morocco, 55th State Party to Convention 108, May 28th 2019.

Daigle, Data Protection Laws in Africa: A Pan-African Survey and Noted Trends, Journal of International Commerce and Economics, 2 (2021).

Dieye, Assessing Trade Relations between Africa and Europe in Abimbola/Aggad (Eds), Towards a Policy fit for Purpose between Africa and Europe, APRI 2021.

DLA Piper, Data protection Laws of the World, (modified in 2021); https://www.dlapiperdataprotection.com/

Dorda/Crowley, Inside Libya: Special Edition, Konrad-Adenauer-Stiftung e. V.; https://www.kas.de/documents/282499/282548/Inside+Libya+-+Special+Edition.pdf/a7080761-581f-2f45-f77e-8feb5e398416?t=1639643880962

Dupret/Hounet, Anthropological Perspectives on Law and Property in Algeria. Law and Property in Algeria: An Anthropological Perspective in Hounet, (ed), Brill, 2018.

European Commission, Accord Euro-Mediterraneen Etablissant une Association entre la Republique Algerienne Democratique et Populaire d'une Part, et, la Communaute Europeenne et ses etats Membres, d'autre Part, 2005.

European Commission, EU Annual Report on Human Rights and Democracy in the World: 2020 Country Updates; file:///C:/Users/Hubert/Downloads/2020_eu_human_rights_and_democracy_country_reports.pdf

European Commission, Renewed partnership with the Southern Neighbourhood: A new Agenda for the Mediterranean, SWD (2021) 23 final.

European Parliament - Directorate General for Research, Developing Countries and the ICT Revolution, March 2001.

Executive Research Associates (Pty) Ltd, China in Africa: A Strategic Overview, October 2009.

Fatafta/Samaro, Exposed and Exploited: Data Protection in the Middle East and North Africa, January 2021.

Finley et al., 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).

FREDI, Global Data Law Maps: Africa and Malabo Convention (2022); https://www.jura.uni-passau.de/fileadmin/dokumente/fakultaeten/jura/lehrstuehle/hennemann/Mapping_Global_Data_Law/Sample_Malabo_Convention.pdf

Hennemann, Wettbewerb der Datenschutzrechtsordnungen – zur Rezeption der Datenschutz-Grundverordnung, RabelsZ 84 (2020).

Hennemann/Boshe/von Meding, Datenschutzrechtsordnungen in Afrika – Grundlagen, Rechtsentwicklung und Fortentwicklungspotenziale, ZfDR 2021.

Human Rights and Labor Country Reports on Human Rights Practices for 2020; https://www.state.gov/wp-content/uploads/2021/03/LIBYA-2020-HUMAN-RIGHTS-REPORT.pdf

Ilori, Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions, June 15th 2022; https://www.apc.org/en/pubs/data-protection-africa-and-covid-19-pandemic-old-problems-new-challenges-and-multistakeholder

Jaller/Molinuevo, Digital Trade in MENA Regulatory Readiness Assessment - Policy Research Working Paper, March 2020.

Kulaib, Paper on Egypt's Personal Data Protection Law (PDPL) and where it stands according to the international standards, Research Unit of the Association for Freedom of Thought and Expression (n. d.)

Libya's Data Protection Authority NISSA Launches Information Security Guide; Libya Herald, August 10th 2019, https://libyaherald.com/en/2019/08/libyas-data-protection-authority-niissa-launches-information-security-guide/

Lons et al, China's Great Game in the Middle East, Policy Brief Commissioned by the European Council on Foreign Relations, October 2019.

Louw-Vaudran, Report on North Africa: The Meaning of Morocco's Return to the African Union, Institute for Security Studies, January 2018.

Makulilo "One size fits all": Does Europe Impose its Data Protection Regime on Africa?' Datenschutz und Datensicherheit 37 (2013).

Makulilo, Data Protection in North Africa: Tunisia and Morocco, in Makulilo (Ed), African Data Privacy Laws, Springer 2016.

Max Planck Foundation, Legal Training of Judges, Attorneys, Prosecutors and Lawyers in Public Service at All Levels of the Judiciary and the Administration in Sudan, project started in 2020.

Max Planck Foundation, Sudan: Support to Constitutional and Legal Reform in the Republic of the Sudan, project started in 2013.

Ministerie van Buitenlandse Zaken, Country of Origin Information Report on Libya, June 2020.

Ministry of Strategy and Finance/Republic of Korea, Establishment of Algeria's National Vision 2030, 2013.

NISSA News, 2020 at https://nissa.gov.ly/en/bin-younis-meets-the-director-general-of-the-national-authority-for-information-security-and-safety-to-discuss-the-authoritys-terms-of-reference/

Nyman-Metcalf, Assessment of Media Legislation in Libya, 2015; https://www.menamedialaw.org/sites/default/files/library/material/medmedia_libya.pdf

Perarnaud, Data Protection in Tunisia: a Legal Illusion?; Centre for Internet and Human Rights (n.d).

Shinn, China's Approach to East, North and the Horn of Africa, China's Global Influence: Objectives and Strategies, a Testimony before the U. S.-China Economic and Security Review Commission, July 21, 2005.

SOAS, Legal and Institutional Reforms in Sudan: Policy Briefing, March 2021.

Tassinari, The Externalisation of Europe's Data Protection Law in Morocco: An Imperative Means for the Management of Migration Flows, Peace & Security – Paix et Sécurité Internationales, No 9, 2021.

The People's Republic of China, China's Arab Policy Paper, January 14, 2016; http://english.www.gov.cn/archive/publications/2016/01/13/content_281475271412746.htm

United States Department of State - Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2020.

United States Department of State: Press Statement, United States Support for the Sudanese Tripartite Political Process, May 69th 2022; https://www.state.gov/united-states-support-for-the-sudanese-tripartite-political-process/

World Bank, Data Governance Practices in Mena Case Study: Opportunities and Challenges in Morocco, November 2020.

World Bank, Report on the Foundation for the Development of Information and Communications Technologies in Algeria, 2003.

Zaptia, Cyber Libya Project Launched; Libya Herald June 23rd 2021.

Zaptia, BREAKING: New Unified Libyan Government Selected by LPDF in Geneva, Libya Herald, February 5th 2021.

* * *

About the Authors

Prof. Dr. Moritz Hennemann holds the Chair for European and International Information and Data Law and is head of the Research Centre for Law and Digitalisation at University of Passau Law Faculty, Germany. His research focuses on interface issues in civil law, business, data, media, and information law. He is particularly concerned with the legal and regulatory framework of the data and digital economy as well as with the global development of data (protection) law and comparative data (protection) law. In his past professional experience, he has been a senior researcher at University of Freiburg Law Faculty, a Visiting Researcher at Harvard Law School, an affiliate to the Berkman Klein Center for Internet & Society of Harvard University, and a guest lecturer in at the China-German School of Law in Beijing, after also working as an attorney-at-law at a renowned German law firm.

Dr. Particia Boshe is a research assistant and a lecturer at the Research Centre for the Law of Digitalisation and at the Chair of European and International Information and Data Law at the Passau University. She holds a Ph.D. in law with a thesis on data protection legal reforms in Africa, LL.M in IT & Telecommunications law. She is a co-founder and co-director of the African Law and Technology Institute (AFRILTI); a research institute focusing on the interrelation between law, technology and society from an interdisciplinary perspective. She is also a practicing advocate in Tanzania, and has more than 10 years' experience as a law lecturer in Tanzania.

Imprint

Disclaimer: "The information and views set out in this publication are those of the authors and do not necessarily reflect the views of the Konrad-Adenauer-Stiftung or its Regional Rule of Law Programme Middle East & North Africa."

Philipp Bremer
Director
Rule of Law Programme Middle East & North Africa

Konrad-Adenauer-Stiftung e.V.

Rule of Law Programme Middle East & North Africa
European and International Cooperation
Konrad-Adenauer-Stiftung e.V.
23, Benoît-Barakat-Street
Jabre-Building, 5th floor
Badaro – Beirut
Lebanon

Tel: +961(1)385094 or + 961(1)395094

Web: http://www.kas.de/rspno

Cover Design: KALUZA+SCHMID Studio GmbH, Berlin

This report provides an in-depth overview of the current state and trends of data protection regulation of seven North African countries – namely Algeria, Egypt, Mauritania, Morocco, Libya, Sudan, and Tunisia. The study tackles regulatory approaches, key principles, and selected instruments. From the outset, the analysis was limited to a textual analysis of the respective data protection laws, including constitutional law (i.e., the "law in the books").

In detail, the study engages with the development and status of regional and sub-regional data protection frameworks in Africa. Political as well as international influences on the development (or the lack of) of data protection laws in North Africa were considered. In addition, for countries with a comprehensive data protection laws (i.e. Algeria, Egypt, Mauritania, Morocco, and Tunisia), the comparative assessment also looked into the scope of alignment and of divergence with the EU General Data Protection Regulation (GDPR).