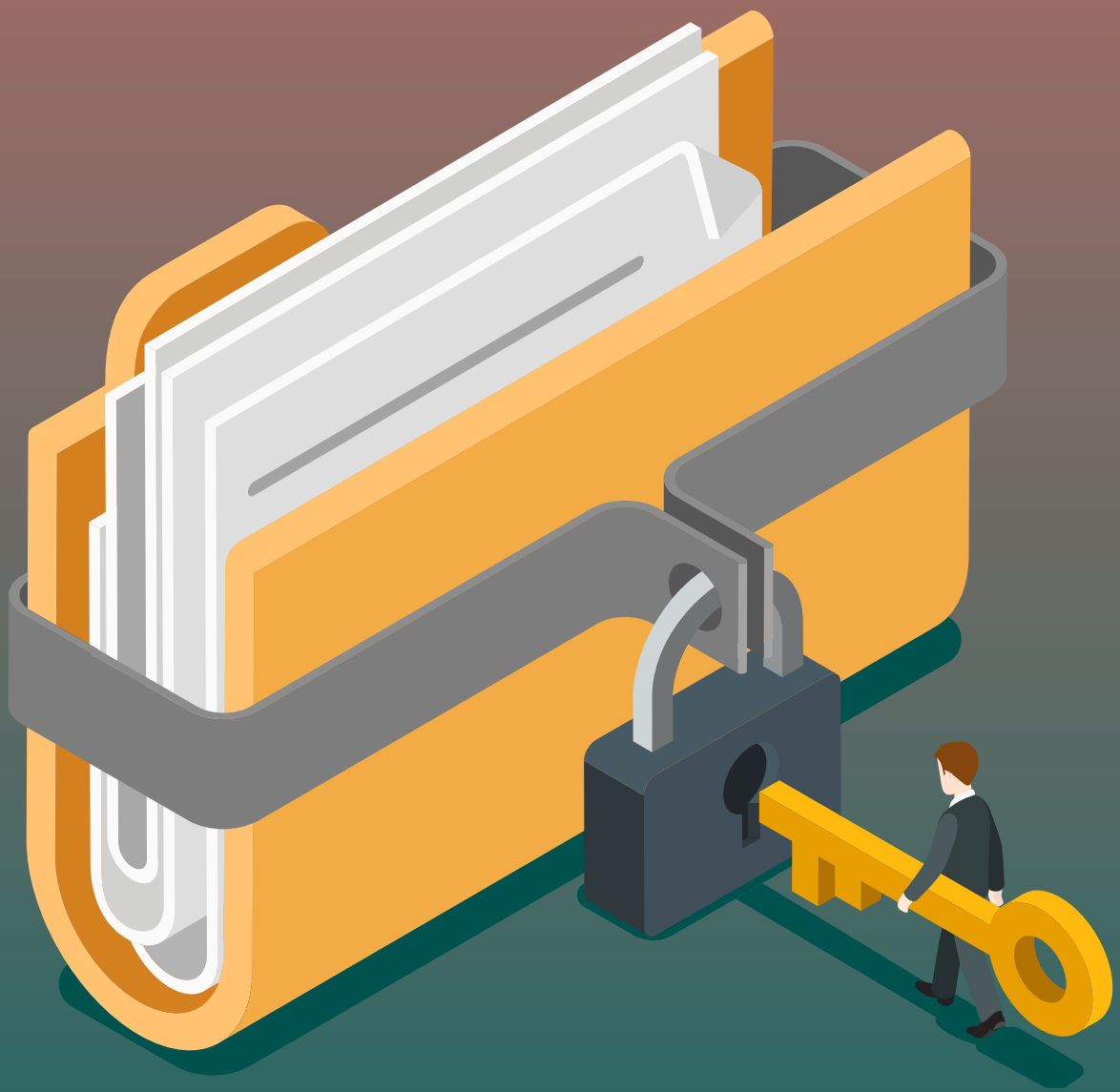
UniMAC GIJ | PARADIGM INITIATIVE

AN APPRAISAL OF GHANA'S DATA PROTECTION ACT (2012)



AN APPRAISAL OF GHANA'S DATA PROTECTION ACT (2012)

Published by:
Paradigm Initiative

Written by:
ABIWU THEODORE (DRIMF -GIJ)

Design & Layout by:
Chima David, Communications Intern, Paradigm Initiative

ACKNOWLEDGEMENTS

I am eternally grateful to my father, and friend, Dr James Kwaku Asante. His support, tutorship, directions, and advice led to the successful completion of this paper. I am grateful to Paradigm Initiative for the opportunity to be embedded in the digital rights and inclusion environment.

INTRODUCTION

The Internet has fast become a fundamental human right that must be accessible to mankind. The United Nations (UN) has declared access to the Internet as a fundamental human right[1]. Article 19 of the Universal Declaration of Human Rights (UDHR) provides for freedom of expression and access to information stating the following:

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers." This is applicable to the online space as rights offline apply online.

In some ways, the Internet has become the most sought-after means of exchanging and storing information. The African Declaration on Internet Rights and Freedoms[2], a Pan-African declaration dedicated to advancing openness and human rights norms in the creation and application of Internet policy throughout the continent, notes that the Internet is particularly relevant to social, economic, and human development in Africa.

A substantial amount of data is currently generated in everyday activities, including shopping, travelling, banking, manufacturing and trade, public utilities, state and government, sports, entertainment, science, education, and health due to recent technological advancements. Governments, research institutions, and commercial enterprises have begun to recognise the value of utilising this data for growth[3].

This indicates that Organizations can obtain immediate and comprehensive insights into consumers thanks to the availability of data on consumers' web browsing, online buying activity, customers' feedback, and marketing research on social networks.

Today, more than ever, businesses, organisations, and institutions that provide goods and services to citizens offline and online obtain much data from their patrons. Such data, now primarilystored online in clouds and other storage packages, are prone to attacks and misuse. Attacks on organisations' storage units, physically or digitally, have led to reports of multiple personal data breaches.

Over the years, such breaches have re-

[1] Howell, West, (2016), The Internet as a human right. (Link)
[2] Accessed via Link
[3] Stansberry, K., Anderson, J., Rainie, L., (2019), The Internet will continue to make life better, Pew Research Center (Link)

sulted in the exposure of millions of records of individuals, including their names, geographical locations, financial and medical records, as well as their political opinions[4].

The systems used in the collection and storage of such personal information can pose significant challenges to one's right to privacy. With the advent of more sophisticated technology capable of storing massive amounts of data, it is critical to address privacy concerns through data protection laws.

As a Transnational Organisation, the United Nations established the Personal Data Protection and Privacy Principles in 2018[5] as a "framework for the processing of personal data, which is defined as information relating to an identified or identifiable natural person ('data subject'), by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities."

Recognising the importance of data to achieving Sustainable Development Goals and at the same time accepting the legitimate concerns regarding the abuse of data and breach of privacy of people all over the world, the United Nations Development Group[6] has come up with guidelines that provide the UN Development Group (UNDG) with broad guidance on data privacy, data protection, and data ethics concerning the use of big data that is being collected in real-time by companies in the private sector as part of their commercial offers, in all member states.

In the European Union, data protection is a fundamental human right[7]. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)8 provide that everyone has the right to the protection of personal data concerning him or her. Subsequently, in 2016, the EU adopted the General Data Protection Regulation (GDPR) to protect natural persons concerning the handling and free movement of personal data.

In 2014, the African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection[9], known as the Malabo Convention, to which, as of May 2019, Ghana was one of five African countries to have signed on and ratified[10].

The "Supplementary Act [A/sa.1/01/10] On Personal Data Protection within ECOWAS[11]" is built on the consciousness that the increasing use of Information and Communication Technology (ICT) may be prejudicial to the private and professional life of the user and that despite the existence of national legislations re-

[4] Dowuona & Company, (2021), Ghana's Data Protection Act, 2012 (Act 843) (Link)
[5] UN High-Level Committee on Management, (2018), Personal Data Protection and Privacy Principles (Link)
[6] United Nations Development Group, (2017), Data Privacy, Ethics, and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda (Link)
[7] European Union, (2016), Regulation (Eu) 2016/679 of the European Parliament and of The Council of 27 April 2016, Legislative acts, Official Journal of the European Union (Link)
[8] (Accessed via Link)
9 African Union, (2014), African Union Convention on Cyber Security and Personal Data Protection. (Link)
[10] Accessed via Link and Link)
[11] ECOWAS, (2010), Supplementary Act on Personal Data Protection Within ECOWAS (Link)

lating to the protection of privacy of the citizens in their private and professional life and relating to the guarantee of the free movement of information, it becomes a matter of urgency to fill the legal vacuum generated by the use of the Internet which is a new instrument of communication.

Ghana's Data Protection Law[12], however, seems to predate that of the UN, EU, and the AU and rather proceeds from that of the ECOWAS, having been promulgated in 2012. The law is founded on the recognition that, despite the existence of national legislation relating to the protection of citizens' privacy in their private and professional lives and relating to the guarantee of the free movement of information, it becomes urgent to fill the legal void created by the use of Internal Communication Technology (ICT).

The Data Protection Act (DPA) 2012 (Act 843) spells out the rules and principles which govern the collection, use, disclosure, and care for personal data or information by a data controller or processor (Sections 21, 48, 84)[13]. The DPA recognises a data subject's right to protect their personal information by mandating any organisation or institution which handles such personal data to do so cognisant of the individual's rights. The law further guarantees the right to privacy under Article 18 (2) of the 1992 Constitution.

This paper explores the relationship between Ghana's DPA and the guidelines on data protection from international bodies, notably the UN, EU, AU, and ECOWAS in the context of best practice. Through content analysis, this paper explores whether Ghana's DPA corresponds to international best practices.

[12] Accessed via link
[13] Accessed via link

LITERATURE REVIEW

Digital Rights

Digital rights are essentially human rights in the Internet space. For example, online privacy and freedom of expression are simply extensions of the equal and inalienable rights enshrined in the Universal Declaration of Human Rights (UDHR)[14]. According to the UN, disconnecti these rights and goes against international law. Although the above definition is widely known and adopted, it has not been enforced as part of the UDHR. The UDHR has helped to clarify human rights and has been translated into numerous legally enforceable regulations, yet, the same cannot be said for the phrases "digital," "technology," or "Internet."

Data Protection

The Storage Networking Industry Association (SNIA) defines data protection as the process of protecting critical data from corruption, compromise, or loss, as well as providing the ability to restore the data to a functional state if something happens to render the data inaccessible or unusable[15]. Data protection ensures that data is not corrupted, is only accessible for authorised purposes, and complies with all applicable legal and regulatory requirements. Protected data should be accessible and usable for the intended purpose when needed. Consequently, a large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss (Crocetti, 2021)[16].

In their blog publication, the SNIA also posits that[17] the scope of data protection extends beyond availability and usability to include immutability, preservation, and deletion or destruction. It further argues that data protection spans three broad categories, namely, traditional data (i.e., backup and restore copies), data security, and data privacy.

Furthermore, the General Data Protection Regulation (GDPR)[18] which applies to most forms of processing of personal data in the European Union, along with other national rules set out in the Irish Data Protection 2018, exempts an individual's processing of personal data for purely personal or household activities with no connection to a professional or commercial activity. This is also called the 'personal/household/domestic exemption. The GDPR applies to controllers who process personal data to facilitate these activities (such as social networks).

International Policies on Data Protection

While the Internet and other technologies provide tremendous benefits, they

[14] United Nations (nd), Universal Declaration of Human Rights. (Link)
[15] SNIA (n.d), What is Data Protection. (Link)
[16] Crocetti, P., (2021) What is Data Protection and why is it important? (Retrieved from Link)
[17] Accessed via Link
[18] Accessed via Link

also pose unique challenges. The digital rights landscape is constantly changing as new technologies emerge and increasingly put the people's enjoyment of their fundamental human rights to the test.

The United Nations (UN) has now firmly established that the same rights that people have offline must also be protected online, particularly the right to freedom of expression[19]. In the Personal Data Protection and Privacy Principles adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11th October 2018[20], they state that in processing of personal data of people, the United Nations System Organization concerned must ensure:

1. Fairness and legitimacy
2. Specificity of purpose
3. Proportionality and necessity
4. Retention
5. Accuracy
6. Confidentiality
7. Security
8. Transparency
9. Appropriateness of third-party transfer
10. Accountability

In the General Data Protection Regulation (GDPR) the European Union[21] posits that the right to personal data protection is a fundamental right that must be considered with its function in society:

1. The protection of natural persons concerning the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
2. The principles of and rules on the protection of natural persons about the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular, their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security, and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and the well-being of natural persons (2018, L 119/1).

The GDPR also notes that data protection should be provided for natural persons, regardless of nationality or place of residence.

The Regional and Sub-regional Situation

Though drafted in 2011, the African Union's Convention on Cyber Security and Personal Data Protection was adopted in 2014. Until now, Ghana is one of only 15 out of 55 states which have ratified it as of May 2023[22].

[19] Article 19, (2017), ARTICLE 19 at the UNHRC: "The same rights that people have offline must also be protected online (Link)
[20] United Nations, Personal Data Protection and Privacy (Link)
[21] Accessed via link
[22] Accessed via link

In its opening statement, the convention speaks to governments on the urgent need to establish a mechanism to address the dangers and risks posed by using electronic data and individual records to respect privacy and freedoms while promoting and developing ICTs in African Union Member States. In Article 8, the Convention enjoins AU member states to establish legal frameworks to protect citizens' data. Accordingly, the Convention insists that:

1. Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the free flow of personal data
2. The mechanisms established shall ensure that any form of data processing respects the fundamental rights and freedoms of natural persons while recognising the state's prerogative, the rights of local communities, and the purpose for which businesses were established.

Notwithstanding, the convention has similar provisions as the EU's GDPR, which covers:

1. Any collection, processing, transmission, storage, or use of personal data by a natural person, the state, local communities, and public or private corporate bodies,
2. Any automated or non-automated processing of data contained or meant to be part of a file,
3. Any processing of data relating to public security, defense, research, criminal prosecution, or state security.

On another level, the protection of personal data and private life is a major challenge for governments and other stakeholders in the Information Society thus, such protection necessitates a balance between the use of information and communication technologies and the protection of citizens' privacy in their daily or professional lives while ensuring the free flow of information.

The convention states that:

> "Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data" (2014, 13)".

However, there are exemptions where a natural person undertakes data processing exclusive to his or her household or personal use without any third-party involvement.

The ECOWAS Supplementary Act on Personal Data Protection establishes a data protection authority and details how personal data processing should be carried out in member states. It sets out principles for collecting, processing, storing, and transferring personal data while also emphasising individuals' rights regarding their information.

By harmonising data protection laws and practices among ECOWAS member states, the act aims to facilitate cross-border data flows and promote trust in the digital economy.

The Act aligns with the guidelines in the AU Malabo Convention. The relationship between these two initiatives lies in their shared objective of protecting personal data and promoting data protection practices in Africa. While the ECOWAS Supplementary Act primarily focuses on data protection within the ECOWAS region, it aligns with the broader principles outlined in the AU Malabo Conventions. Together, these instruments contribute to a comprehensive data protection framework in Africa, emphasising privacy rights and digital security.

Data Protection in Ghana

The Data Protection Bill was first introduced in Ghana's parliament by the then Minister of Communication, Haruna Iddrisu, in November 2010. It was immediately assigned to the joint committee on Communications and Constitutional Legal and Parliamentary Affairs for consideration and recommendation. The Committee presented its report in March 2011 and the house was scheduled to begin debate in July 2011. But there was a stall when the sector minister notified parliament and withdrew the bill in late July 2011 (Biztechafrica, 2011). The bill was passed into an Act in February 2012 going through the gazetting process in May and then becoming effective in October 2012.

Summary and Structure of the Act

The Act is divided into 12 Headings with 99 Sections under which Subsections and Paragraphs follow[23]. Part 1 establishes the Data Protection Commission (DPC). From Section 1 to Section 10, the Act details the mandate for creating the DPC, the object, functions, and governing body of the Commission with the tenure of officers. This first part goes on to clarify meeting schedules and defines a quorum. It also touches on how members can disclose their association to a case that's being considered and stipulates that such should dissociate themselves from the same. It has stipulations on committees of the commission, and payment of allowances, and ends with a declaration that the sector minister can give directives to the commission on matters of policy.

Part 2 of the Act, titled "Administration," spans three sections; 11, 12, and 13. The stipulation herein borders the appointment of the Executive Director of the Commission and functions thereof and the appointment of other staff. The third part focuses on the finances of the Commission. All three sections in this part stipulate sources of revenue for the commission, auditing of the commission's accounts, and submission of annual reports to Parliament through the office of the sector minister.

Part 4 of the Act contains 18 sections, beginning from section 17 to section 34. In those sections, the Act enshrines data protection principles such as en-

[23] Accessed via link

suring privacy, seeking consent, collecting and using data for a specific clearly-defined purpose, collecting data directly from the data subject, and not retaining data unless necessary, among others, and stipulates that these principles be employed by data controllers and data processors, who must be duly registered with the Commission.

In Part 5, the Act enshrines the rights of data subjects. Here, a data subject has the right to be informed by the controller or processor about which data is being collected, the rationale for collection, and the recipients of such data. It stipulates that where another person seeks the data of another from the controller, the controller ensures the identity of the seeker and obtains the subject's consent before processing any data.

Part 6 of the Act starts from section 37 and ends at section 45. It establishes and prohibits the processing of "Special Personal Data," in section 37, which it explains as data that relates to:

A. a child who is under parental control following the law, or
B. the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life, or criminal behavior of an individual.

Section 40 prohibits the processing of personal data for direct marketing without the subject's consent. Section 41 stipulates against automated decision-making and in section 43, the Act allocates compensation to anyone who suffers damages due to the negligence of a data controller. The Act also gives power to the Commission to "order the data controller to (a) rectify, (b) block, (c) erase, or (d) destroy the data" if it is found to be inaccurate. It is also in this part that the Act spells out its application jurisdiction.

Part 7 is titled "Data Protection Register" and spans sections 46 to 59. Section 46 establishes the Register, which is entrusted to the care and maintenance of the Commission and urge all data controllers to enter their detail therein. Requirements for applying to be added to the Register are detailed out in section 47, and power is given to the Commission to deny registration to an applicant where certain conditions are rife. In section 54, the Commission must publish the Data Protection Register and make it available to the general public in written and electronic formats. Section 56 enshrines that a person who processes the personal data of others without registration with the Commission shall face punitive measures. In section 58, the Act mandates data controllers to appoint Data Protection Supervisors who should be "responsible for the monitoring of the data controller's compliance with the provisions of this Act."

In Part 8, the Act details 15 types of data that are exempt from the provisions of the Act, including National security, health, education, and social work, Journalism, literature and art, Domestic purposes, Examination marks, and Professional privilege, among others. Part 9 carries provisions that give power to the Commission to enforce the

Act through various ways, including serving notice and prosecution. Yet, it allows 'appealing' to an accused data controller.

Part 10 of the Act (in sections 83 and 84) forbids demand for records as a condition for providing public goods or services unless it is backed by law. It also prescribes demanding health records of a person. Part 11 avers that information given to that information provided to the Commission or its agents be treated with confidentiality.

Part 12 has miscellaneous and general provisions like duties of the Commission, ban on sales, purchase, or reckless disclosure of another's personal data and application to the State. There are also provisions on administrative operations of the Commission and interpretation of certain terms used in the Act as well as parts of certain existing laws that stand repealed by the Act.

What's Praiseworthy?

For purposes of this review, whatever is praiseworthy about the Act must correspond to internationally accepted data protection principles and/or, in some ways, maintain or extend the individual's freedom of expression and right to information. There are quite a few commendable provisions in Ghana's Data Protection Act.

To begin with, this Act is a direct response to both the AU [Malabo] Convention on Cyber Security and Personal Data Protection (CCSPDP) and the ECOWAS Supplementary Act on Personal Data Protection (SAPDP). In Article 8 (1) and (2) and Article 2, respectively, both the Regional and Subregional bodies call for Member States to establish a legal framework of protection for the privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State. Particularly, since the ECOWAS SAPDP was adopted in 2010 and Ghana's DPA was enacted in 2012, it stands to reason that the latter was highly influenced by the former in many positive ways.

Besides that, the creation of a Data Protection Authority and mandating it to "(a) protect the privacy of the individual and personal data by regulating the processing of personal information, and (b) provide the process to obtain, hold, use or disclose personal information," is commendable. An identifiable body in charge of data protection is international best practice. The EU's GDPR identifies a "Supervisory Authority" which oversees the work of data controllers and processors and ensures compliance with the Regulations. Similarly, Article 11 (1a) of the AU CCSPDP directs member states to "an authority in charge of protecting personal data", which should be an independent administrative body. Interestingly, the ECOWAS SAPDP, which sets the tone for Ghana's Act, in Article 14 (1), states, *"Within the ECOWAS space, each Member State shall establish its own Data Protection Authority. Any State that does not have shall be encouraged to establish one."*

Another commendable feature of the Act is the insistence on applying data protection principles such as accountability, the lawfulness of processing, specification of purpose, compatibility of further processing with the purpose of collection, openness, data security safeguards, and data subject participation24 . These are values espoused by the UN, AU (Article 13), EU (Article 5), ECOWAS, and numerous researchers, like Mateeva Zhivka (2020). What is even more admirable is the addition of "data subject participation" to the principles. Though other high bodies and researchers intimate this in articles and clauses, it is more clearly stated in the Act, and so it is given a prime place and made more glaring. The best way to protect a person's data is if the person is involved in collecting, processing, storing, and using that data.

Figure 1: **The EU's Privacy Principles**

The principles are expatiated in subsequent sections (18 to 33). Section 19 (1)[25], for instance, states "Personal data may only be processed if the purpose for which it is to be processed, is necessary, relevant and not excessive," and gives a right to data subjects to object to the processing of their data outside the law. Section 22[26] further directs that a data controller collect the data for a specific, explicitly defined and lawful purpose "and related to the functions or activity of the person." Section 28[27] instructs a data controller to "take the necessary steps to secure the integrity of personal data … through the adoption of appropriate, reasonable, technical and organizational measures to prevent loss of, damage to, or unauthorized destruction; and unlawful access to or unauthorized processing." Where there are any security compromises of the data, the Act bids the controller or the processor to, as a matter of urgency, inform both the Commission and the data subject, and steps must be taken to restore "the integrity of the information system[28]."

Further, in Section 33[29] of Ghana's DPA (2012), the right to demand correction, deletion, or erasure is allotted to data subjects. This is another factor that has become very crucial recently as a result of the Internet and digital technology keeping records and track of people's data forever. It is also known as the "right to be forgotten." According to Experian[30], "the underlying principle of this right is that when there is no compelling reason for their data to be processed, the data subject can request the data controller erase/remove their personal data, stop any further distribution of their personal data and potentially stop third parties from processing their personal data." This is captured by the ECOWAS (Article 41)[31], AU (Article 19)[32], and the EU (Articles 16 and 17)[33].

Another laudable provision of the Act is Section 35 (2) which states, "where the data constitutes a trade secret, the provision of data related to the logic or rationale involved in any decision taken does not apply." This is clear protection of intellectual property rights. This provision gives bars a data controller from collecting information on the unique device or technique used by an entity in manufacturing its products.

Furthermore, the Act is clearly against all forms of discrimination through data collection and processing and protects minors. In Section 37, the Act inhibits the processing of personal data which relates to "(a) a child who is under parental control per the law, or (b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behavior of an individual." Article 30 of the ECOWAS SAPDP, Article 14 of the AU CCSPDP, and Articles 8 and 9 of the EU GDPR prohibit the same.sfdxdv

[25] Section 19 (1), Data Protection Act (2012) (Link)
[26] Section 22, Data Protection Act (2012) (Link)
[27] Section 28, Data Protection Act (2012) (Link)
[28] Section 28 (1), Data Protection Act (2012) (Link)
[29] Section 33, Data Protection Act (2012) (Link)
[30] Expeian, (n.d), What is the right to erasure? (Link)
[31] Article 41, ECOWAS Supplementary Act (Link)
[32] Article 19, AU Malabo Convention (Link)
[33] Articles 16 & 17, EU GDPR (Link)

Another best practice found in the Act is the establishment of a Data Protection Register by the Commission. In Section 46, the Act stipulates:

1. There is established by this Act a register of data controllers to be known as the DataProtection Register.
2. The Commission shall keep and maintain the Register.
3. A data controller shall register with the Commission.

And from there till section 59, details are given for how the register should be compiled, availed for public viewing, both physically and digitally, and what happens to a person "who fails to register as a data controller but processes personal data." In Article 70 (1) (o), the EU GDPR also states that one of the tasks of the European Data Protection Board is to "carry out the accreditation of certification bodies and its periodic review pursuant to Article 43 and maintain a public register of accredited bodies pursuant to Article 43(6) and of the accredited controllers or processors established in third countries pursuant to Article 42(7)." In Article 12 (4), the AU Convention also tasks the National Protection Authorities in member states to revoke authorisation given to data controllers if there is a breach of privacy principle. Also, Article 19 (1) (j) of the ECOWAS Supplementary Act states, "update a register of personal data processing and make it available to the public" as part of the responsibilities of the Data Protection Authorities in member states.

It is also worthy to note that the Act exempts situations of national security, crime and taxation, academic freedom, health, and social work, journalism, literature, and art, and the armed forces from the provision of the Act and principles of privacy (from section 60 to 71). This means that the media and academia, especially, are protected and can go about their duties. Again, in Sections 88 and 89, the Act illegalises the commercialisation of personal data.

Appropriately, in section 91, the Act binds the Republic and confers the status of "data controller" on all government departments and agencies. This is a democratic principle of equal justice and the rule of law.

The Act is very clear on punitive measures for breachers of its provisions (sections 56, 80, 85, etc). In fact, in section 91, the Act states, *"where a person commits an offense under this Act in respect of which a penalty is not specified, the person is liable on summary conviction to a fine of not more than five thousand penalty units or a term of imprisonment of not more than ten years or both."* Clarity on punishments for offenders of a law makes it easier to dispense justice. Where there is a lack of clarity, justice is left in the hands of regulatory bodies and court judges, who, as humans, are liable to allow their personal biases sometimes to take the better of them

A Few Criticisms

Though the Data Protection Act, 2012, seems to correspond largely with international, regional, and subregional principles of privacy and data protection, it also leaves a lot to be desired in certain aspects. For a law to serve the citizens efficiently, it must be balanced and place more power in the hands of the people.

One glaring deficiency of the Act is placing so much power in the hands of the Executive Arm of Government. In section 4 (2), the President of the Republic is given the power to appoint members of the Commission's Board. In addition, the President appoints the Executive Director (ED) of the Commission, who acts as the Chief Executive Officer of the Commission (Section 11). Of concern is the tenure of the ED, which is left at the mercy of the President. As if that is not enough, in section 13, the president is again given the power to appoint staff of the Commission.

Though these powers align with the 1992 Constitution of Ghana, the framers of this Act had the chance to balance the power play by sharing it between the Executive and Parliament. Knowing that "he who pays the piper calls the tune" and seeing how Governments on the continent, in the last few years, have threatened to or blocked Internet access for any number of reasons, it is scary to leave sensitive bodies like the Data Protection Commission solely in the hands of the Executive. The possibility is that the DPC may end up doing the bidding of the Government of the day instead of protecting the citizens of the nation.

The sector minister is given the power to approve the allowances of members of the Commission's Board and Committees created by the board (Section 9). And *"the Minister may give directives to the Board on matters of policy"* (section 10). If the Minister, an appointee of the President, has the power to decide how much Board members are paid, this may place the DPC in a position of being interfered with, rendering the Commission inefficient.

From the foregoing, the DPC lacks total independence, a situation that can curtail its operations and which is against best practice. Unfortunately, nowhere in the Act does it expressly state that the DPC is independent of its appointors, unlike in the case of the EU's GDPR, which states so in Article 69. This situation is in sharp contrast to Article 11 (2) of the AU Convention and Article 14 (2) of the ECOWAS Supplementary Act, both of which state, "The Data Protection Authority shall be an independent administrative Authority..."

Likewise, in section 41, where the Act gives the right to a data subject to resist automated decision-making, the Act says the Section does not apply to the Minister, and no reasoning was giv-

en to back the same. It looks as if the Minister is being left off the hook. That seems like the Act is set to favour some and not others.

Similarly, in section 49, the Act gives power to the Commission to register and license data controllers and processors at a fee payable by the applicant. In section 50, the Act stipulates that registration with the Commission must "be renewed every two years," which presupposes that payment will be made. Again, in section 54, the Commission is responsible for supplying *"a member of the public with a duly certified manual or electronic copy of the particulars contained in an entry made in the Register on payment of the prescribed fee."* " Interestingly, the Minister is given the power to prescribe all these fees. This is another layer of unnecessary power given to the Minister. The Act could have simply prescribed these fees to lay all matters to rest. As it stands now, any sector minister, at any given time, can decide how much any of these services rendered by the Commission should cost. That is too much power for one person. If anything, Parliament should decide the fees and not the Minister.

In section 43, the Act provides for compensation to be paid to anyone who "suffers damage or distress through the contravention by a data controller of the requirements of this Act," but the amounts payable or the type of compensation are not prescribed. This is interesting because, in all other sections where punitive measures are mentioned (56, 80, and 85), clear stipulations are made. Even more, in section 95, a "General Penalty" is prescribed by the Act for cases where the penalty for offences is not specified. Yet, the issue of compensation is left hanging and probably at the mercy of the judge on duty, the commission, or the data controller. Such a situation creates space for corruption and injustice to breed.

RECOMMENDATIONS

1. The Data Protection Commission must propose amendments to the Parliament of Ghana regarding ensuring more independence from the Executive arm for the Commission and the Board. This will allow the Commission and the Board to work assiduously without bias or prejudice.
2. Massive education on the Act is recommended. The Data Protection Commission must embark on an intensive and exhaustive awareness campaign for citizens and data controllers, and processors to know the provisions of the Act and how to get issues addressed when faced with any.
3. Media practitioners must get hold of the Act, update themselves with it, and use their platforms as a point of debate on its provisions. Such debates can involve data experts and civil society and will lead to fine-tuning the Act and increasing public awareness.
4. Academic institutions that teach communication and Media Related programs must add this Act to their reading materials for students. This can encourage further research and unearth strategies that lead to a resilient data protection jurisdiction for the country.
5. Institutions collecting and processing personal data must register with the Data Protection Commission and educate themselves on the law's requirements. Registration demonstrates commitment to data protection, allowing the Commission to monitor compliance. Institutions should educate staff and stakeholders on their responsibilities, promoting proper data handling practices. This cultivates a privacy-conscious culture and reduces the risk of breaches. By registering and prioritising education, institutions protect individuals' data, build trust, and contribute to a secure digital environment in Ghana.

CONCLUSION

To a large extent, the Act captures data protection best practices espoused by international standards. Though there are a few issues, mainly on the administrative part, which portend a lack of independence for the Commission and the Board that the Act has established to implement the provisions therein, Ghana's Data Protection Act (2012) captures the applicable principles and practices of data privacy and protection

It is highly recommended that the Parliament of Ghana amend the Act to ensure more independence for the Commission. This will strengthen the Commission's autonomy, ensuring it can enforce data protection regulations and safeguard privacy rights impartially. An independent Commission can operate efficiently, develop robust rules, investigate breaches, and provide guidance. By demonstrating a commitment to data protection and aligning with international practices, Ghana can enhance trust in data handling and foster a secure digital environment.

Ghana's Data Protection Commission (DPC), already set up, should endeavour to execute its mandate without fear or favor. The DPC, as an established entity, should diligently fulfil its mandate without bias, favouritism or recourse to partisan affiliation and social status. This entails carrying out its responsibilities with integrity and impartiality without being influenced by external pressures. By executing its duties without fear or favor, the Commission can effectively enforce data protection regulations, ensure the privacy rights of individuals, and foster a trustworthy digital environment. This approach builds public trust and confidence in the Commission's ability to safeguard personal data and reinforces the importance of its role in upholding data protection principles.

Ghanaians need to keep informed on the provisions of the Act. The Data Protection Act applies to everyone, and individuals have a responsibility to understand their rights and obligations regarding handling and protecting personal data. By actively engaging with the Act, Ghanaians can ensure that they respect the privacy of others, comply with data protection regulations, and contribute to a culture of responsible data management. Additionally, being informed about the Act empowers individuals to exercise their rights regarding their data and seek recourse if they believe their privacy has been violated. Therefore, Ghanaians must stay updated on the Act's stipulations and embrace their role in promoting a secure and privacy-conscious society.

REFERENCES

1. Constituteproject.org, (2013), Ghana's Constitution of 1992 with Amendments through 1996, Comparative Constitutions Project.
2. Parliament of Ghana, (2012), Data Protection Act.
3. European Union, (2016), Regulation (Eu) 2016/679 of the European Parliament and of The Council of 27 April 2016, Legislative acts, Official Journal of the European Union.
4. African Union, (2014), African Union Convention on Cyber Security and Personal Data Protection.
5. African Commission on Human and People's Rights, (2019), Declaration of Principles on Freedom of Expression and Access to Information in Africa.
6. ECOWAS, (2010), Supplementary Act on Personal Data Protection Within ECOWAS.
7. UN High-Level Committee on Management, (2018), Personal Data Protection and Privacy Principles. Access via https://unsceb.org/privacy-principles
8. UNHCR, (2018), Guidance on The Protection of Personal Data of Persons of Concern To UNHCR.
9. United Nations Development Group, (2017), Data Privacy, Ethics, and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda. Accessed via https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda
10. Parker, T., (2021), Internet and Social Media Shutdowns on the African Continent accessed via: https://globalriskinsights.com/2021/02/Internet-and-social-media-shutdowns-on-the-african-continent/
11. Hudak, J., Wallack, G., (2016), Political appointees as barriers to government efficiency and effectiveness: A case study of inspectors general, Center for Effective Public Management, The Brookings Institution.
12. Mateeva, Z., (2020), Principles of personal data protection, 28, pp95-104.
13. Johnson, J., (2021), Global digital population as of January 2021, accessed via: https://www.statista.com/statistics/617136/digital-population-worldwide/
14. Dowuona & Company, (2021), Ghana's Data Protection Act, 2012 (Act 843), accessed via: https://www.lexology.com/library/detail.aspx?g=21818b3a-d2d3-427c-a7c7-dbd-9672cb848
15. Biztechafrica, (2011), Data Protection bill withdrawn, accessed via: http://www.biztechafrica.com/article/data-protection-bill-withdrawn/933/
16. GhanaWeb, (2012), Data Protection Bill Passed, accessed via: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717
17. Experian, (2021), What is the Right to Erasure? accessed via: https://www.experian.co.uk/business/glossary/right-to-erasure/
18. 18. Crocetti, P., (2021) What is Data Protection and why is it important? Retrieved from https://searchdatabackup.techtarget.com/definition/data-protection
19. APC https://www.apc.org/en/news/coconet-what-are-digital-rights

HQ: 374 Borno Way, Yaba, Lagos - Nigeria.