African Journal on Privacy & Data Protection

To cite: B Mutiro & O Saki 'The Cyber and Data Protection Act of Zimbabwe: A critical analysis' (2024) 1 *African Journal on Privacy & Data Protection* 50-80

The Cyber and Data Protection Act of Zimbabwe: A critical analysis

*Blessing Mutiro**
Early-Stage Researcher, Castlebridge, Dublin; PhD Researcher, Trinity College, Dublin, Ireland

*Otto Saki***
Doctoral candidate, University of the Western Cape, South Africa

Abstract:

The Cyber and Data Protection Act of Zimbabwe is the first comprehensive data protection statute covering both the public and private sectors and setting up a data protection authority. Its provisions are vital to the protection of the fundamental human right to privacy. This is in the context of the government prioritising cybersecurity over privacy, with the private sector being complicit. This context of cybersecurity over privacy is seen through the government's intention in passing the Act of which the provisions focus more on cybersecurity rather than on data protection. Against this background, this study evaluates the Cyber and Data Protection Act to establish whether its provisions are adequate to protect and ensure privacy and data protection despite the cybersecurity

* LLBS (University of Zimbabwe) LLM (University of Birmingham) blessing.mutiro@castlebridge.ie/mutirob@tcd.ie. The author has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement 813497.

** LLBS (University of Zimbabwe) LLM (Columbia University) LLM (Open University Tanzania); otto.saki@caa.columbia.edu. The authors acknowledge the editorial support and attention to detail that Mr Mduduzi Ruwitah provided in preparing this article. The authors are grateful to the two anonymous reviewers for their comments. All errors are those of the authors.

intention and focus. The study examines the Zimbabwean data protection regime from a customary law, common law and international law perspective, comparing the Act against European Union-style legislation that has inspired and is the bedrock of the Act. This is a study of what has been enacted, and what may have been enacted in Zimbabwe.

Key words: data privacy; data protection; personal information; cybersecurity

1 Introduction

On 3 December 2021 the Cyber and Data Protection Act (CDPA)[1] of Zimbabwe became law.[2] The object of the Act is 'to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects'.[3] Before the CDPA, there was no Zimbabwean law governing data protection following the repeal of the Access to Information and Protection of Privacy Act (AIPPA)[4] that only applied to public entities. A literal reading of the CDPA objectives indicates the government's intent to invest in cybersecurity, not data protection. CDPA comes at a time when there has been misuse of personal data by public and private entities.[5] Concurrently, the government has increased surveillance on citizens using artificial intelligence.[6]

The CDPA enactment benefits from the global and continental discussions on data protection spurred by developments in the European Union (EU) through the General Data Protection Regulation (GDPR) and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The GDPR is viewed as having considerably influenced African data protection frameworks, with disastrous impact.[7] The Malabo Convention, which entered in force on 8 June 2023, attempts to frame an African approach

1 CDPA [Chapter 11:12] 5 of 2021.
2 Before it was gazetted as law, the short title of the Act was Cyber Security and Data Protection Bill. Several changes were made by legislators and the minister responsible for the Bill. These changes are to be found at http://www.veritaszim.net/node/4863 (accessed 6 December 2021).
3 CDPA (n 1) sec 2.
4 Access to Information and Protection of Privacy Act (AIPPA) [Chapter 10:27] Act 5 of 2003.
5 Media Institute of Southern Africa 'Zimbabwe's urgent need for data privacy laws' 13 July 2018, http://zimbabwe.misa.org/2018/07/13/zimbabwes-urgent-need-data-privacy-laws/ (accessed 27 March 2023). One such incident was during the 2018 elections when voters received messages that urged them to vote for a specific Zimbabwe African National Union – Patriotic Front (ZANU PF) Member of Parliament specific to their constituency and to vote for the ZANU PF presidential candidate. It was most likely that the information had been obtained from the voters' roll and subsequently used to target voters. However, there was no way in which one could compel ZANU PF to disclose from where they had obtained the information and, as such the scandal simply faded and everyone forgot about it.
6 G Maunganidze 'Letter to Speaker of National Assembly: Increase in collection of personal data in the absence of adequate data privacy legislation' 4 December 2018, http://zimbabwe.misa.org/2018/12/04/letter-to-speaker-of-national-assembly-increase-in-collection-of-personal-information-in-the-absence-of-adequate-data-privacy-legislation/ (accessed 27 March 2023).
7 C Mannion 'Data imperialism: The GDPR's disastrous impact on Africa's e-commerce markets' (2021) 53 *Vanderbilt Journal of Transnational Law* 685.

to data protection, albeit with limitations.[8] In addition, the Council for Europe has modernised Convention 108 on data processing (Convention 108+),[9] which is open to non-European countries for membership. Zimbabwe has not been invited to accede to Convention 108+ and has not ratified the Malabo Convention. Several judicial and legislative developments also affect data protection. Considering these developments, this article continues by studying the resonance of CDPA with African multinational data protection agreements and international standards. It also provides a critical analysis of general protections of personal data in Zimbabwe.

Through a doctrinal assessment of the main features and provisions of the CDPA, the article focuses on what has been enacted and what may have been enacted. The article also discusses data protection under common and customary law. It then discusses international privacy and data protection standards and commitments. This is followed by a historical background to data protection in Zimbabwe. An overview and discussion of the obligations, main components, and rights in CDPA follows. The discussion is alongside a critique of CDPA, and recommendations to improve the Act's utility in the protection of personal information.[10]

2 Data protection under common law and customary law

Zimbabwe has a dual legal system of general law consisting of common law and statute, and African customary law.[11] According to section 192 of the Constitution of Zimbabwe, the law to be administered by the courts is the law in force on the 'effective date',[12] being the date on which the Constitution became law.[13] According to section 89 of the Constitution,[14] the applicable law is the 'law in force in the Colony of the Cape of Good Hope on 10 June 1891, as modified by subsequent legislation having in Zimbabwe the force of law'.[15] The law applicable at the Cape of Good Hope on 10 June 1891 was Roman-Dutch law with English law grafting.

The right to protection of personal data is novel. There is no common law right to data protection within Roman-Dutch law. A right to privacy, however, exists.

8 G Greenleaf & B Cottier 'International and regional commitments in African data privacy laws: A comparative analysis' (2022) 44 *Computer Law and Security Review* 105638.
9 Council of Europe Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 (Convention 108+).
10 It does not cover consequential amendments to the Criminal Law Codification and Reform Act [Chapter 9:23], the Criminal Procedure and Evidence Act [Chapter 9:07] and the Interception of Communications Act [Chapter 11:20].
11 L Madhuku *An introduction to Zimbabwean Law* (2010).
12 Constitution of Zimbabwe Act 20 of 2013, sec 332.
13 As above.
14 Constitution of Zimbabwe Act, 2008. The Act, which was the 19th Amendment to the Constitution entered into force on 13 February 2009 and amended the Constitution of Zimbabwe. It was repealed and amended by the Constitution of Zimbabwe Act 20 of 2013.
15 Constitution of Zimbabwe (n 12) sec 89.

Zimbabwe's common law right to privacy derives from the common law of South Africa.[16] It is worth considering whether the common law right to privacy applies to data protection given the overlap between the right to private life, a pillar of the right to privacy, and the right to protection of personal data.[17] A claim for a right to privacy under common law is related to personality.[18] When the right to privacy is violated, there are four main remedies,[19] namely, the *actio iniuriarum*, which is the recovery of sentimental damages or satisfaction for injured feelings; the *actio legis Acquiliae*, where the plaintiff has suffered monetary loss; an interdict where there is impending or continuous infringement;[20] and a retraction coupled with an apology.[21] The applicability of the common law right of privacy to data protection is questionable. Ncube argues that the active control principles of data protection differ from common law privacy protections, making common law privacy protections inadequate for purposes of data protection.[22] Further, for a common law right to privacy to apply to data protection, a two-point process must be undertaken. The first is full utilisation of the common law, and the second is an individual controlling the data. If the individual is not in control of the data, it is unlikely that the common law right to privacy applies. Examples of where the common law right to privacy would apply to data protection are where photographs are taken[23] and telephones are tapped without the subject's consent.[24] In these examples, Zimbabwean courts can extend the common law right to privacy to data protection. However, they have been reluctant to give the common law right to privacy an expansive interpretation.[25] Although *Nsoro*[26] shows a shift towards an expansive interpretation as the Court held that society ought to respect privacy of communications,[27] it is unlikely that a common law right to privacy applies to data protection.

The concept of data protection in Zimbabwe was first introduced by AIPPA and, subsequently, the CDPA. There is no prior Zimbabwean case law on customary law and on data protection. Similarly, the existence of a right to privacy in Zimbabwe's customary law is doubtful as privacy is an abstract concept in traditional African societies.[28] An individual's personhood is intricately linked

16 C Ncube 'A comparative analysis of Zimbabwean and South African data protection systems' (2004) 1 *Journal of Information, Law and Technology* 1.
17 M Gracia Porcedda 'The recrudescence of security v privacy after the 2015 terrorist attacks and the value of "privacy rights" in the European Union' in E Orrù, M Grazia Porcedda & S Weydner-Volkmann *Rethinking surveillance and control. Beyond the 'security vs privacy' debate* (2017) 149.
18 *S v A & Another* 1971 (2) SA 476 (C) 297.
19 Ncube (n 16) 107.
20 *Rhodesian Printing & Publishing v Duggan* 1975 (1) SA 590 (A).
21 *Mineworkers Investment Co (Pty) Ltd v Modibane* 2002 (6) SA 512.
22 *Rhodesian Printing & Publishing v Duggan* (n 20).
23 *La Grange v Schoeman* 1980 (1) SA 885.The Court held that taking photographs without consent of the person constituted an invasion of the right to privacy.
24 *Reid v Daly v Hickman & Others* 1980 ZLR 540 (A).
25 *Mr & Mrs X v Rhodesia Printing & Publishing Co Ltd* 1974 (4) SA 508 (R).
26 *S v Nsoro* HH 190-16 (unreported).
27 As above.
28 AB Makulilo 'Protection of personal data in sub-Sahara Africa' doctoral thesis, University of Bremen, 2012 277; EM Bakibinga 'Managing electronic privacy in the telecommunications

with their community, as aptly defined by concepts such as ubuntu.[29] *The identity of the individual is based on them being a member of the community, which is the custodian of the individual's rights*.[30] It thus is difficult for an individualistic right to privacy to thrive. The communitarian environment, however, provides a framework for relational or group privacy.[31] It therefore is unlikely that there exists an African customary law right to privacy useable to assert personal data protection.

3 International privacy and data protection standards and commitments

Zimbabwe's international privacy commitments stem mainly from the Universal Declaration of Human Rights (Universal Declaration)[32] and the International Covenant on Civil and Political Rights (ICCPR).[33] The right to privacy is also to be found in article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter).[34] These instruments inspired the right to privacy in most African countries under post-independence constitutions.[35] Zimbabwe's first post-independence Constitution, however, lacked an explicit right to privacy.[36]

African data protection standards have been influenced by developments in the EU.[37] These include the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)[38] and the Data Protection Directive.[39] Convention 108 allows non-Council of Europe members to accede to it. Some African countries have ratified the Convention and its additional protocol.[40] The Convention was recently modernised into Convention 108+. Zimbabwe has neither signed nor ratified either convention. Data protection standards of Convention 108, the additional

sub-sector: The Uganda perspective' Africa Electronic Privacy and Public Voice Symposium (2004).

29 A cultural term commonly used in Southern Africa that defines how an individual exists in a community. U Reviglio & R Alunge '"I am datafied because we are datafied": An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy and Technology* 595.

30 P Boshe, M Hennemann & R von Meding 'African data protection laws: Current regulatory approaches, policy initiatives and the way forward' (2022) 3 *Global Privacy Law Review*.

31 As above.

32 Universal Declaration of Human Rights art 12.

33 International Covenant on Civil and Political Rights art 17.

34 African Charter on the Rights and Welfare of the Child art 10.

35 AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 3.

36 The Constitution of Zimbabwe was published as a Schedule to the Zimbabwe Constitution Order 1979 (SI 1979/1600 of the United Kingdom).

37 G Greenleaf & B Cottier 'Data privacy laws and bills: Growth in Africa, GDPR influence' (2018) *Privacy Laws and Business International Report*; AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) *Computer Law and Security Review* 78.

38 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).

39 Council Directive 95/46/EC 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 [1995] OJ L 281.

40 Convention 108 (n 38) art 23.

protocol and the Data Protection Directive in Africa are seen continentally and regionally. Continentally, the standards are reflected in the Cyber Security and Personal Data Protection Convention (Malabo Convention) of the African Union (AU).[41] The Malabo Convention establishes regulatory regimes of cybersecurity, electronic transactions and data protection. It harmonises data protection frameworks in AU states, prioritises free movement of data, and ensures the protection of privacy.[42] Zimbabwe is not a signatory to the Malabo Convention. Regionally, the standards are reflected in the Southern Africa Development Community Data Protection (SADC) Model Law.[43] The Model Law is not binding but may be used by SADC states to develop their data protection legislation.

Since the SADC Model Law, there have been developments within the EU with global implications. These are the replacement of Convention 108 with Convention 108+ and GDPR. GDPR is a global benchmark for data protection law[44] and enjoys extraterritorial application.[45] This obliges compliance with the GDPR if African countries engage with digital users in the EU. Countries such as Zimbabwe can comply by either adopting laws and regulations aligned with GDPR or adopting of GDPR-compliant procedures by entities operating in Zimbabwe.[46] The global implications of the GDPR, therefore, cannot be ignored. This influence, however, disregards the unique socio-economic and cultural realities in Africa.[47] The influence of standards developed because of EU legislation in Zimbabwe's data protection Act is presented in Table 1 below. This is done by comparing the standards and provisions of CDPA against the SADC Model law, the Malabo Convention and GDPR. The criteria of the standards used in the comparison stem from the categorisation of them into three levels developed by Greenleaf and Cottier.

41 At the time of writing the Convention is not yet in force. There currently are 13 ratifications, two short of the required 15 for the Convention to enter into force.
42 Convention 108 (n 38) Preamble.
43 Greenleaf & Cottier (n 37).
44 Boshe and others (n 30) 4.
45 Council Regulation (EU) 2016/679 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 [2016] OJ L 119, art 3(2)(a).
46 Mannion (n 7) 685.
47 As above.

Table 1 – Comparison of CDPA against data protection standards[48]

First Generation Standards	SADC 2012	AU 2014	GDPR 2016	CDPA
Collection – limited (not excessive), lawful (for legitimate purposes) and by fair means	12	x	5(1)(a)	7(1)(a)
Data quality – relevant, accurate, up to date	11(1)	13(4)	5(1)(d)	7(1)(b)
Purpose specification by time of collection	13	x	5(1)(b)	9(1)
Notice of purpose/rights	21(1)	15	13, 14	15, 16
Uses limited (including disclosures) to purposes specified or compatible	13(1)	13(3)(a)	5(1)(b)	13(c)
Security through reasonable safeguards	24	13(6); 20; 21	5(1)(f), 32	18
Openness re personal data practices (not limited to data subjects)	x	x	14(5)(b)	
Access – individual right of access	31	17	15	14(b)
Correction – individual right of correction	32	19	16, 19	14(d)
Accountable – identified data controller accountable for implementation	x	x	5(1)(f)	24(1)(a)-(b)
Second Generation				
Minimum collection necessary for purpose (data minimisation)	x	10(3)(b)	5(1)(c)	13(d)
Destruction or anonymisation after purpose completed	32(1)(b)	22	5(1)(e)	13(f)
Additional protections for sensitive data in defined categories	15	1 def; 14	9, 10	11, 12
Legitimate bases for processing defined	12, 14	1 def	6	10(2)-(3)
Additional protections on some sensitive processing systems (notification; 'prior checking' by DPA etc.)	26, 28	10(2)-(4)	36	12
Limits on automated decision-making (inclu. right to know processing logic)	31(1c), 36	x	22	25
To object to processing on compelling legitimate grounds	33	18	21	14(c)

48 The table used in this comparison is derived from Greenleaf and Cottier (n 8). It has been modified to include the provisions of the CDPA. The EU Data Protection Directive, C108 and C108+ have been removed from the table.

Restricted data exports requiring recipient country 'adequate', or alternative guarantees	43	14(6)(a)	45-47	28-29
Independent Data Protection Authority(-ies) (DPA)	3(1)	11(1) (b)	51-59, 77	5-6
Recourse to the courts to enforce data privacy rights C108 AP 1(4)	78, 79, 82			x

3rd Generation – Common European Standards	**SADC 2012**	**AU 2014**	**GDPR 2016**	**CDPA**
Data protection by design and by default	x	x	25	x
Demonstrable accountability by controllers	30(1) (b)	x	5(2)	24
Data breach notification to DPA for serious breaches	25	x	33	19
Direct liability for rocessors as well as controllers	x	x	28-31	x
Stronger consent requirements	1(2), 37	x	7, 8	3, 10(1)
Proportionality required in all aspects of processing	x	x	GDPR passim	
DPAs to make decisions and issue administrative santions incl. fines	5(2)	12(2) (h)	58(1)	x
Biometric and genetic data require extra protections	16	104(a), (d)	9	12
Stronger right to erasure incl. 'to be forgotten'	x	19	17, 19	x
DPAs to cooperate in resolving complaints with international elements	x	12(2) (m)	50	x
3rd Generation – GDPR additional standards, 2018 (not in CoE 108+)				
Mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing	x	x	35, 36	x
Extra-territorial jurisdiction, where goods or services offered, or behaviour monitored	x	x	3	4(2)
Extra-territorial controllers or processors must be represented within jurisdiction (EU/other)	x	2(3)	27	4(3)
Right to data protability (UGC/other)	x	23	20	x
Mandatory Data Protection Officers (DPOs) for sensitive processing	x	x	37-39	20(4) (b)-20(6)

Data breach notification to data subjects (if high risk)	x	x	34	x

The Agreement Establishing the African Continental Free Trade Area (AfCFTA) imposes additional data protection obligations on Zimbabwe. According to article 15 of the Protocol on trade in services, member states can enforce and adopt measures 'necessary to secure compliance with law or regulations that are not inconsistent' with the protocol.[49] This includes protection of the privacy of individuals, 'in relation to the processing and dissemination of personal data and the protection of confidentiality of individuals' records and accounts'.[50] The import of article 15 is that members can adopt their own data protection laws if such laws are consistent with the provisions of AfCFTA.[51] The extent of influence of AfCFTA is limited as it remains to be seen how consistency with AfCFTA will be maintained as each member adopts its data protection laws.

4 The Cyber and Data Protection Act of Zimbabwe

4.1 Historical background

CDPA succeeds AIPPA which was Zimbabwe's first data protection legislation. It follows the government's drive to create a technology-driven business environment and encourage technological development while ensuring that technology is used lawfully.[52] The Act targets issues of data protection concerning the Declaration of Rights under the Constitution. It also extends to cyber-related offences, establishing a Cyber Security Centre and a Data Protection Authority and to provide for their functions. The Act further provides for the investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and for admissibility of electronic evidence for such offences.[53] Before presidential assent, CDPA was criticised for neglecting human rights in regulating personal data protection and being below the minimum standards of modern data protection law.[54] Nonetheless, CDPA constitutes a significant improvement from AIPPA.

AIPPA only applied to public institutions with data processing by private, natural and juristic persons unprotected. Individuals lacked rights associated with

49 Agreement Establishing the African Continental Free Trade Area (AfCFTA) art 15(c).
50 AfCFTA (N 49) art 15(c)(ii).
51 E Salami 'Implementing the AfCFTA Agreement: A case for the harmonisation of data protection law in Africa' (2022) 1 *Journal of African Law* 285.
52 CDPA (n 1).
53 As above.
54 Media Institute of Southern Africa 'Cybersecurity and Data Protection Bill entrenches surveillance' 19 May 2020, https://zimbabwe.misa.org/2020/05/19/cybersecurity-and-data-protection-bill-entrenches-surveillance-an-analysis/ (accessed 6 December 2021).

data protection legislation against private persons. AIPPA also only provided for a right to correction.[55] AIPPA was unsuitable as a regulatory framework for data protection.[56] CDPA, thus, is an attempt to fix the shortcomings of AIPPA while ensuring that Zimbabwe satisfies the minimum threshold of data protection and also ensure the transfer of data from other nations to the country. Nonetheless, CDPA contains pitfalls that may undermine the protection of personal data.

4.2 Definitions

This part considers the key terms in the Act whose interpretation is crucial to the protection of the rights of data subjects.

4.2.1 Personal information

Personal information is at the core of CDPA. However, the term as defined fails the comprehensibility test, which entails not only the language used to make an act understandable but its readability. It is broken down into three definitions, namely, 'personal information', 'data subject' and 'identifiable person'. 'Personal information' is defined as 'information relating to a data subject'.[57] A 'data subject' is defined as 'an individual who is an identifiable person and the subject of data'. An 'identifiable person' is defined as a person who can be identified directly or indirectly in particular reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.[58] Personal information, therefore, is any information relating to an identified or identifiable person who can be identified, directly or indirectly, by reference to an identifier, which includes an identification number.

CDPA applies only to natural persons. Only natural persons are addressed using gender pronouns and have specific physical, physiological, mental and cultural identities. A key phrase from the definition formulated by this article is 'information relating to an identified or identifiable natural person'. A person is identifiable if one considers all the means reasonably likely to be used by a controller or other person to identify the natural person directly or indirectly.[59] Information, therefore, will not relate to an individual where a disproportionate effort is required to identify the individual. The concept of personal data, however, now is more dynamic. Without additional effort, anonymised data

55 AIPPA (n 4) part IV & part V.
56 Ncube (n 15) 99.
57 This includes a person's name, address or telephone number.
58 CDPA (n 1) sec 2.
59 M Finck & F Pallas 'They who must not be identified – Distinguishing personal from non-personal data under the GDPR' (2020) 10 *International Data Privacy Law* 11-36; Recital 65 GDPR.

remains non-personal data, but the economic and technological trends portend for less of a distinction.[60]

4.2.2 Data

The CDPA defines data as

> any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data.[61]

This creates ambiguity about the scope of CDPA. Section 4 resolves this quandary by providing that CDPA applies to matters relating to the processing and storage of data. 'Processing' is defined as 'any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data'. This creates a strong supposition that non-personal information is within the scope of CDPA, which is atypical of data protection legislation. This ambiguity could have been resolved by the insertion of 'data subject' or by altogether removing the definition of data.

If the above supposition is correct, controllers, processors and the data protection authority (DPA) will have additional responsibilities because of non-personal information. This, however, creates compliance fatigue. Entities will seek a compliance balance between personal and non-personal information. This is worsened by the inclusion of 'information' in the definition of 'data' as the distinction between information and data might be too technical. The result undermines the objectives of CDPA. The inclusion of non-personal information as a subject of regulation, however, might have been an attempt by the legislature to harmonise personal and non-personal information.[62] This is important as technology has blurred the boundary between personal and non-personal.[63]

4.3 Application of the Act

CDPA applies to access to information, protection of privacy of information, and the processing and storage of data.[64] The territorial scope of CDPA stands

60 As above.
61 CDPA (n 1) sec 3.
62 J Drexl 'Legal challenges of the changing role of personal and non-personal data in the data economy' in A di Franceschi & R Schulze (eds) *Digital revolution – New challenges for law: Data protection, artificial intelligence, smart products, blockchain technology and virtual currencies* (2019) 19-41.
63 As above.
64 CDPA (n 1) sec 4.

on an 'establishment' and a 'means' criterion.[65] While the Act does not use 'establishment' in section 4(2)(a), it is apparent that the legislature intended an 'establishment' criterion. According to section 4(2)(a), CDPA applies to the processing of data in the 'effective and actual activities of any data controller'. This seems to derive from Recital 22 of GDPR, which provides that '[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.'

Recital 22 aids the interpretation of the GDPR establishment criterion. As such, the first territorial criterion is one of 'establishment'. The use of the words 'effective and actual' suggests a departure from the traditional notion of establishment focusing on the entity's place of registration.[66] CDPA applies where a data controller has some stability within Zimbabwe and where the nature of the services offered and the economic activity undertaken are within Zimbabwe. An example is services exclusively offered over the internet.

Evidence of the means criterion is in section 4(2)(b), which provides that it applies to the processing of data by a controller who is not established in Zimbabwe where the means used is in Zimbabwe.[67] The requirement of whether processing occurred by means in Zimbabwe must be assessed when the relevant trigger activity occurs. This would ordinarily be the moment the good or service is offered to the data subject. The provision is aimed at activities deliberately using means in Zimbabwe to process data. As such, where processing and storage of data are undertaken by a controller with Zimbabwe being a data transit, CDPA is inapplicable.[68]

The Act is silent as to where it is inapplicable, yet it has become customary for data protection legislation to define its scope and exceptions. Data protection legislation can be an anathema to the enjoyment of people's rights, particularly in the digital age where individuals conduct some form of processing of personal data.[69] This is why the SADC Model Law, the Malabo Convention and GDPR exclude processing for purely personal or domestic purposes. The Malabo Convention further excludes processing for artistic and literary expressions and journalistic purposes within professional codes of conduct. Not every act of data processing by an individual invokes the application of data protection law. Such an approach would make data protection law oppressive and tedious to apply.[70]

65 European Data Protection Board 'Guidelines 3/2018 on the Territorial Scope of the GDPR' (Article 3) – Version Adopted after Public Consultation; O Saki 'Guide to the Zimbabwean Cyber And Data Protection Act', https://data.misa.org/en/entity/28jfydpjr4c (accessed 16 June 2022).
66 *Weltimmo v Hungarian National Authority for Data Protection and Freedom of Information* (C230/14).
67 CDPA (n 1) sec 4(2)(b).
68 As above.
69 A Murray *Information technology law* (2018).
70 As above, 583.

With more people spending time online, CDPA should exclude processing outside professional or commercial activity.[71] It must include a provision exempting processing for domestic or household activities. The scope and interpretation of the exception would then be left to the courts through interpretative guidance given by the DPA in line with the decisions in *Lindqvist*[72] *and Rynes.*[73]

4.4 Data protection authority

CDPA designates the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as the data protection authority (DPA)[74] responsible for the enforcement of CDPA. POTRAZ is established under section 3 of the Postal and Telecommunications Act.[75] Its major function is to 'ensure the provision of sufficient domestic and international telecommunication and postal services throughout Zimbabwe on such terms and conditions as the Authority may fix'.[76] POTRAZ is run by a board appointed by the President after consultation with the responsible minister.[77] The functions of POTRAZ as a DPA are contained in section 6 of CDPA. These include regulating the processing of personal information, by establishing conditions for lawful processing;[78] the promotion and enforcement of fair processing;[79] and the issuing of opinions on matters relating to the application of the Act on its own accord or at the request of a person with a legitimate interest.[80]

POTRAZ may submit to any court any administrative action that is not compliant with the fundamental principles of CDPA and any law on the protection of privacy concerning the processing of data.[81] POTRAZ, however, must first consult the Minister responsible for Information, Publicity and Broadcasting Services.[82] POTRAZ is responsible for conducting inquiries or investigations either of its own accord or at the request of a data subject or interested person.[83] It must also ensure that feedback is given to the complainant.[84] It is responsible for researching policy and legal matters about international best practices on the protection of personal information and facilitating cross-border cooperation in the enforcement of privacy laws.[85] POTRAZ is mandated to provide guidelines and approve codes of conduct and ethics governing rules of conduct for data

71 GDPR (n45) Recital 18.
72 Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596.
73 Case C-212/13 *Rynes v Urad pro ochranu osobnich udaju* [2014] ECLI: EU:C:2014:2428.
74 CDPA (n 1) sec 5.
75 Postal and Telecommunications Act (PTA) [Chapter 12:05] Act 4 of 2000.
76 PTA (n 75) sec 4.
77 PTA (n 75) sec 5.
78 CDPA (n 1) sec 6(1)(a).
79 CDPA (n 1) sec 6(1)(b).
80 CDPA (n 1) sec 6(1)(c).
81 CDPA (n 1) sec 6(1)(d).
82 As above.
83 CDPA (n 1) sec 6(1)(f).
84 CDPA (n 1) secs 6(1)(a)-(h).
85 CDPA (n 1) secs 6(1)(i)-(j).

controllers. Controllers desiring to have codes of conduct approved must submit them to POTRAZ for ascertaining compliance with CDPA. In deciding whether to approve a code of conduct, the DPA can consult data subjects or their representatives.[86]

POTRAZ was established as an independent body.[87] The independence, however, is worth evaluating as it is essential for protecting personal information. This is important in the Zimbabwean context where there have been incidents of abuse of personal information by political parties during campaigns, and by the government.[88] In evaluating the independence of POTRAZ, reliance will be placed on attributes of independent data protection supervisory authorities identified by Greenleaf in his study of international instruments on the independence of data protection authorities.[89] These include (i) the establishment of the authority by legislation rather than executive order or delegated legislation; (ii) the ability to investigate and report free of direction or permission from any other political or governmental authority; (iii) a fixed term of office to avoid a commissioner being at the whim of the executive; (iv) removal from office only for defined reasons and with procedural safeguards; and (v) powers and duties to report directly on issues, either to Parliament or to inform the public of its activities.

Other key factors influencing independence include immunity from personal lawsuits against commissioners for conduct relating to the performance of duties; independent determination of resources; positive qualification requirements for commissioners; the prohibition on commissioners to undertake other concurrent positions the prohibition on the appointment of commissioners from specified backgrounds with potential conflicts of interests; decisions of the authority being subject to a right of judicial appeal and review; and the personal character of the commissioner. The factors influencing independence are similar to the factors safeguarding independent commissions created under chapter 12 of the Zimbabwean Constitution. The similarity of the attributes by Greenleaf and the safeguards makes them ideal for evaluating the independence of POTRAZ.

The independence of POTRAZ is compromised. First, POTRAZ remains under government control. In terms of its establishing Act, the minister may direct the POTRAZ board on policies that the minister deems necessary for the national interest.[90] The minister may also direct the board to reverse, suspend or rescind its decisions or actions. The only requirement for interference is that the minister must satisfy themselves that there are reasonable grounds that the decision or action is not in the national or public interest.[91] What constitutes

86 CDPA (n 1) sec 30(4).
87 CDPA (n 1) sec 6(2).
88 Maunganidze (n 6).
89 G Greenleaf 'Independence of data privacy authorities: International standards and Asia Pacific experience' (2012) 28 *Computer Law and Security Review* 3.
90 PTA (n 75) sec 25.
91 PTA (n 75) sec 26.

national or public interest is not defined in the Postal and Telecommunications Act (PTA), thus creating broad powers for interference. An example of this is provided by section 11(4) of CDPA which provides that the Minister of State Security, in consultation with the minister responsible for information and communications technologies,can give directions on the implementation of the Act in respect of sensitive information affecting national security or the interests of the state. This undermines the independence of POTRAZ as a DPA.

CDPA does not exclude decisions made by the POTRAZ board on the functions of a DPA from interference by the minister. It does not describe how POTRAZ will function as a DPA and whether it will be a division within POTRAZ. Being a separate division means that the decisions and actions of the DPA will be subject to reversal, suspension or rescission by the minister. Any investigation that it may want to undertake against the government would be interfered with. POTRAZ, therefore, will be unable to investigate matters without direction or permission from the minister. While section 6(2) of CDPA excludes anyone from giving directives to POTRAZ as a DPA, this is not convincing. There are provisions in CDPA, such as section 11(4) demonstrating that POTRAZ will operate under directives on national security interests, and these issues ignite possibilities of state-sanctioned surveillance. This is concerning, with data transfers for jurisdictions such as the EU considering decisions such as *Schrems* I[92] and II.[93]

The board's independence is also compromised by the terms and conditions of service, which are determined by the President.[94] Board members, thus, are prone to manipulation by the appointing authority. Where board members act contrary to the expectations of the appointing authority, they may be dismissed or subsequent appointments may be threatened with unfavourable terms and conditions of service, undermining their independence. Moreover, there is poor security against removal as they may be removed from their positions on mere allegations. Board members are simply required to make representations but may be dismissed despite the representations.[95] This further undermines their security of tenure. An example is the 2014 POTRAZ board that was dismissed on allegations of corruption and poor corporate governance.[96] However, there are counter-allegations that, instead, the board was dismissed because the then Minister of Information Communication Technology wanted to appoint a

92 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.
93 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.
94 PTA (n 75) sec 7.
95 PTA (n 75) sec 10.
96 F Munyoro 'Potraz board fired over graft ' *The Herald* 3 July 2015, https://www.herald.co.zw/potraz-board-fired-over-graft/ (accessed 27 March 2023).

board amenable to his instructions.[97] This lack of security of tenure, therefore, significantly impacts the independence of POTRAZ in its supervisory functions.

CDPA is similarly silent on how POTRAZ in its supervisory function will be funded. The funding will be from the executive as POTRAZ is under governmental control. Funds will thus be given to POTRAZ as an entity and then distributed to its several functions, including the data protection supervisory function. This may cause problems given that POTRAZ will have to balance its two roles, being a telecommunications regulator and a DPA. Government funding will be inadequate for POTRAZ to diligently fulfil these functions. Financial independence is essential for a DPA to effectively conduct investigations and carry out its responsibilities.[98] Without financial independence, the effectiveness of POTRAZ is questionable. Further, CDPA is silent on the recruitment of staff working in the DPA function. The failure to stipulate criteria and conditions for staff employment potentially creates questions on their partiality based on who eventually appoints them, how they will be appointed, and under what conditions. Arguably, the designation of POTRAZ as a data protection authority is also against the rules of natural justice as POTRAZ essentially is a judge, jury and executor in its own cases where it acts as a data controller in carrying out its regulatory function.

While the above concerns remain possibilities, the legislature could have done more to ensure the independence of the supervisory function. There was a need to have a stand-alone institution akin to constitutional commissions that would be established by CDPA and given a status similar to constitutional commissions.[99] Constitutional commissions' objectives include supporting and entrenching human rights and democracy; protecting the sovereignty and interests of the people; promoting constitutionalism; promoting transparency and accountability; and ensuring that injustices are remedied.[100] The general objectives of independent commissions are like those of a DPA.[101] Thus, with the same status as a constitutional commission, the DPA would be empowered to employ staff and regulate their terms of service.[102] It would have its independence guaranteed,[103] with members of staff being non-political. The staff members would then be appointed by the President after they have been interviewed by Parliament. They would then enjoy security of tenure.[104] Another proposal

97 This allegation is made by Reward Kangai, former CEO of NETONE in a series of tweets that can be seen at https://twitter.com/rewardkangai/status/1344989184885469184?s=21 (accessed 26 March 2023).
98 Greenleaf (n 89).
99 These include the Zimbabwe Human Rights Commission; Zimbabwe Electoral Commission; Zimbabwe Media Commission; Zimbabwe Gender Commission; and National Peace and Reconciliation Commission.
100 Constitution of Zimbabwe (n 12) sec 233.
101 *Commission v Germany* (2010) (OJ C 113 of 01.05.2010. The case stipulated the general objective of a supervisory authority and its importance.
102 Constitution of Zimbabwe (n 12) sec 234.
103 Constitution of Zimbabwe (n 12) sec 235.
104 Constitution of Zimbabwe (n 12) sec 237(3).

is to mandate the Zimbabwe Media Commission (ZMC), responsible for administering the Freedom of Information Act.[105] This mirrors the South African approach where the Protection of Personal Information Act (POPIA)[106] and the Promotion of Access to Information Act (PAIA)[107] are under the Information Regulator.

4.5 Obligations of data controllers and processors

A data controller is a natural or legal person licensable by POTRAZ, who determines the purpose and means of processing.[108] A data processor processes data for the data controller under the instruction of the controller.[109] Persons under the direct employment or authority of a data controller are not considered processors. Processing is any operation performed upon data, whether or not by automatic means. It includes obtaining, recording, holding, organising, adaptation, alteration, retrieval, consultation, alignment, combining, blocking or erasure of data. CDPA has three tiers of obligations applicable to data controllers and processors. The first tier consists of specific rules on data quality applicable to data controllers.[110] The second tier consists of general rules applicable to both data controllers and processors when processing data.[111] The third tier consists of rules relating to the processing of personal information, applicable to data controllers and processors.[112] Each of the tiers is discussed below.

First-tier obligations relate to data quality with data controllers being required to ensure that processing is adequate, relevant and not excessive regarding the purpose for which it is collected.[113] Data processed must be accurate, current, and retained in a form allowing identification of data subjects for periods no longer than is necessary for the purpose for which it was collected.[114] It must be accessible regardless of the technology used, and technological evolution must not hinder the accessing or processing of such data.[115] CPDA, however, does not stipulate who is entitled to access the data. The presumption is that it should be accessible to the data subject as it is collected from them.

Second-tier obligations relate to lawfulness and fairness. Data must be processed only where necessary, fairly and lawfully.[116] It must be for a specific, explicit and legitimate purpose and must not be further processed in a way that

105 (FoIA) [Chapter 10:23] 1 of 2020.
106 Protection of Personal Information Act 4 of 2013.
107 Promotion of Access to Information Act 2 of 2000.
108 CDPA (n 1) sec 2.
109 As above.
110 CDPA (n 1) sec 7.
111 CDPA (n 1) secs 8-12.
112 CDPA (n 1) sec 13.
113 CDPA (n 1) sec 7(1)(a).
114 CDPA (n 1) secs 7(1)(b)-(c).
115 CDPA (n 1) sec 7(2).
116 CDPA (n 1) sec 8.

is incompatible with the purpose of its collection.[117] POTRAZ can specify conditions where further processing of data for historical or scientific research purposes is compatible with the original processing purpose.[118] These obligations are reinforced as duties of a data controller in section 13 of CDPA. The second tier also imposes rules on the processing of non-sensitive personal information,[119] sensitive personal information,[120] genetic data, biometric sensitive data and health data.[121] These rules provide a legal basis for the processing of data.

Third-tier obligations are in the form of duties imposed on the data controller or processor. These duties mirror the principles of the processing of personal data in international data protection instruments and leading data protection instruments.[122] As such, interpretation or guidance on these principles may be used in interpreting the general duties imposed by CDPA. The first duty requires personal information to be processed in accordance with the right to privacy of the data subject.[123] This means that the protection of personal information is premised on the right to privacy. The second duty requires personal information to be processed lawfully, fairly and transparently.[124] Data subjects, therefore, must be informed beforehand about what will be done with their personal information. The duty placed on administrative authorities processing personal information mirrors the 'to act lawfully'.[125] To lawfully process personal information, data controllers and processors can rely on the different lawful processing conditions provided in CDPA.[126]

The third duty requires the collection of personal information to be for an explicit, specific and legitimate purpose, and processing must be compatible with the purpose.[127] Thus, when personal information is collected for a specific purpose, for example, billing, it must not be used for other purposes such as marketing unless the data subject has approved it or if a lawful basis exists. The fourth duty requires the collection of personal information to be limited to what is necessary for the purpose for which it is processed.[128] The fifth duty requires that a valid explanation be provided before the collection of personal information relating to family or private affairs.[129]

117 CDPA (n 1) sec 9(1).
118 CDPA (n 1) sec 9(2).
119 CDPA (n 1) sec 10.
120 CDPA (n 1) sec 11.
121 CDPA (n 1) sec 12.
122 An example is GDPR (n 45) art 5.
123 CDPA (n 1 above) sec 13(a).
124 CDPA (n 1) sec 13(b).
125 Constitution of Zimbabwe (n 12) sec 68(1); Administrative Justice Act [Chapter 10:28] 12 of 2004 sec 3.
126 These include consent, legitimate interest, performance of a contract.
127 CDPA (n 1) sec 13(c).
128 CDPA (n 1) sec 13(d).
129 CDPA (n 1) sec 13(e).

The sixth duty requires personal information to be accurate and, where necessary, current. Reasonable steps must be taken to ensure that any inaccurate personal data is promptly erased or rectified.[130] This requires data controllers and processors to have mechanisms that ensure quick investigation, identification and action on any reported inaccuracies. Data controllers and processors must ensure that personal information is kept in a form identifying the data subject 'for no longer than is necessary for the purposes which it was collected'.[131] Thus, the duration for which personal information is kept by organisations should be given due regard and, where it is no longer necessary, organisations must ensure that they delete personal information.

4.6 Transparency of processing

To ensure transparency of processing, CDPA imposes disclosure obligations on controllers. When data is obtained directly from the data subject, they must be provided with information such as the name and address of the controller and the representative if any;[132] the purpose of the processing;[133] the existence of a right to object to the processing of data if it is obtained for direct marketing;[134] whether compliance with the request for information is compulsory; and consequences of non-compliance.[135] Supporting information may be provided in appropriate circumstances and includes recipients or categories of recipients of data, whether it is compulsory to reply, and the existence of the right to access and rectify data.[136] Similar obligations apply when data has not been collected directly from the data subject.[137] However, there are additional disclosure requirements when data is obtained from third parties for direct marketing. The data controller must first ensure that the data subject is notified of the right to object to the processing of data.[138]

POTRAZ may specify additional information to be provided when data is collected directly from a data subject.[139] No guidance or additional specification has to date been provided by POTRAZ. CDPA lacks comprehensive transparency requirements for data subjects, as there is no obligation to inform them of their right to complain to the DPA or of the period in which their personal information will be stored. Data controllers must also inform data subjects as to how they can exercise their rights, and the limitations on the rights. CDPA imposes transparency obligations on data controllers but they have a discretion

130 CDPA (n 1) sec 13(f).
131 As above.
132 CPDA (n 1) sec 15(1)(a).
133 CDPA (n 1) sec 15(1)(b).
134 CDPA (n 1) sec 15(1)(c).
135 CDPA (n 1) sec 15(1)(d).
136 CDPA (n 1) sec 15(1)(e).
137 CDPA (n 1) sec 16(1).
138 CDPA (n 1) sec 16(1)(d).
139 CDPA (n 1) sec 16(1)(f).

on compliance with disclosure obligations, with the most common method being privacy notices.[140] Most of the privacy notices, however, are complex to read.[141] Arguably, they simply ensure compliance with legal requirements as opposed to showing data subjects how their data is used.[142] Thus, more could have been done to ensure that disclosure is made more simply. Given that POTRAZ has the authority to issue guidance and regulate how disclosures can be made, there is room to ensure that privacy notices adopted using plain and simple language. POTRAZ can also require the use of machine-readable language by controllers as a way of ensuring greater transparency. Disclosure obligations, however, are not absolute. Data controllers are exempted from notifying the data subject when data has not been acquired from the subject if informing them would involve a disproportionate effort or is impossible.[143] Further exemptions apply when data is collected for statistical and research purposes or when it has been collected for medical examination to protect and promote public health.[144] Disclosure is also exempted when data is obtained from a third party or when it has been provided in terms of a law.[145]

Apart from disclosure obligations to data subjects, data controllers have disclosure obligations to POTRAZ. They must notify POTRAZ before carrying out any wholly or partly-automated operation or set of operations that intend to serve a single purpose or several related purposes.[146] However, an exception applies where the operations have the sole purpose of keeping a register intended to provide information to the public by law and that is accessible by the public.[147] POTRAZ may further exempt certain categories from notification where it has considered the data being processed and that there is no risk of infringement of data subjects' rights and freedoms.[148] POTRAZ must also be informed of the purposes of the processing, categories of data being processed, categories of data subjects, categories of recipients, and the retention period[149] for the exemption to apply. Furthermore, the data controller must appoint a data protection officer (DPO)[150] and POTRAZ must be notified of his appointment. POTRAZ

140 J Mohan, M Wasserman & V Chidambaram 'Analysing GDPR compliance through the lens of privacy policy' in V Gadepally and others (eds) *Heterogeneous data management, polystores, and analytics for healthcare* (2019) 82.

141 A Terpstra and others 'Improving privacy choice through design: How designing for reflection could

support privacy self-management' *First Monday* (2019), https://journals.uic.edu/ojs/index.php/fm/article/view/9358 (accessed 7 December 2021); S Jordan, S Narasimhan & J Hong 'Deficiencies in the disclosures of privacy policies and in user choice' *Social Science Research Network* (2021), https://papers.ssrn.com/abstract=3894548 (accessed 7 December 2021).

142 Mohan and others (n 140).

143 CPDA (n 1) sec 16(2)(a).

144 As above.

145 CPDA (n 1) sec 16(2)(b).

146 CPDA (n 1) sec 20(1).

147 CPDA (n 1) sec 20(2).

148 CPDA (n 1) sec 20(4)(a).

149 As above.

150 CPDA (n 1) sec 20(4)(b).

stipulates the minimum qualifications and functions of the DPO.[151] The CDA requires data controllers to ensure that the DPO is free to conduct its duties including ensuring compliance, dealing with requests made to the data controller, and working with POTRAZ.[152]

Where a data controller is not exempted from notifying POTRAZ, the notification must contain the date of notification and the law permitting the automatic processing,[153] full names, complete address, and registered office of the data controller and the representative where there is one.[154] The data controller must also inform the purpose of automatic processing, categories of data being processed including a detailed description of the sensitive data being processed; category or categories of data subjects; safeguards to be linked to disclosure of data to third parties; manner in which data subjects are informed and service providing a right to access and a measure taken to facilitate the right. POTRAZ must be notified of the period after the expiration of which data may no longer be stored; recourse to the data processor, if any; transfer to a third country and an assessment of whether security measures provided are adequate.[155] POTRAZ may prescribe other information that must be provided by the data controller.

4.7 Security of processing

CDPA requires that data controllers and processors or their representatives adopt appropriate technical and organisational measures protecting the data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or processing, or access.[156] The rationale for this is to safeguard the integrity, security and confidentiality of the data. The measures must ensure an appropriate level of security.[157] POTRAZ may issue standards it considers appropriate concerning information security for all or certain categories of processing.[158] POTRAZ is also empowered to inspect and assess the security and organisational measures before the commencement of processing or transfer of data where it formulates an opinion that processing or transfer of data by a data controller entails specific risk to the privacy or rights of data subjects.[159] Where a data controller seeks to appoint a data processor, they must ensure that the data processor can provide

151 POTRAZ in The Postal and Telecommunications Regulatory Authority of Zimbabwe [Public Notice on Data Protection Act Chapter 11:20] 5 of 2021. Public Notice Number 1 of 2022 provides for the qualification of a person with no less than an advanced level certificate of education.
152 CDPA (n 1) sec 20(6).
153 CPDA (n 1) sec 21(1)(a).
154 CPDA (n 1) sec 21(1)(b).
155 CPDA (n 1) sec 21(1).
156 CPDA (n 1) sec 18(1).
157 CPDA (n 1) sec 18(2).
158 CPDA (n 1) sec 18(3).
159 CPDA (n 1) sec 21(3).

sufficient guarantees regarding technical and organisational security measures to protect data.[160]

The data processor, therefore, may only process data following the instructions from the data controller.[161] The data processor and the data controller must enter into a written contract ensuring that the data processor maintains security measures on the data being processed.[162] Where there has been a security breach, the data controller is obliged to notify POTRAZ within 24 hours.[163] The notification period given to data controllers when a breach has occurred is insufficient. It could take controllers more than 24 hours to identify the exact scope of the breach. As a result, every security incident a data controller detects will be reported, potentially overwhelming POTRAZ. There is also a risk that security incidents will be downplayed and there will be underreporting to POTRAZ. Ideally, CDPA should have adopted the international standard period of 72 hours. While there is a requirement to notify POTRAZ of a data breach, there is no separate requirement to notify the data subject in circumstances of potentially high risk to the rights and freedoms of the data subject.

4.8 Accountability

Under CDPA data controllers must take all measures necessary to demonstrate compliance with the principles and obligations set out.[164] This often is referred to as the accountability principle. Data controllers must have internal mechanisms in place for demonstrating compliance to both data subjects and POTRAZ in the exercise of their powers. The accountability principle demands that there is a demonstration of compliance with all provisions of CDPA, and not only sections that might be framed as specific to data controllers.

4.9 Legal basis for the processing of data

CDPA provides several lawful bases for processing non-sensitive personal information. The first is with the consent of the data subject or a competent person where the data subject is a child.[165] Consent is the specific, unequivocal, freely given, informed expression of will by a data subject or their legal, judicial or legally-appointed representative to have their data processed.[166] Consent may be implied if the data subject is an adult or has a legal persona and full legal capacity to consent.[167] However, there is no mention of the circumstances where consent

160 CPDA (n 1) sec 18(4).
161 CPDA (n 1) sec 17.
162 CPDA (n 1) sec 18(5).
163 CPDA (n 1) sec 19.
164 CPDA (n 1) sec 18(3).
165 CPDA (n 1) sec 10(1).
166 CPDA (n 1) sec 3.
167 CPDA (n 1) sec 10(2).

may be implied from the data subject. This defeats the whole notion of consent as it is a mechanism of people exercising control over whom they decide to share their information with. This is more so when CDPA provides that personal information may only be processed where the data subject consents.[168]

Processing without consent is permissible where the data is key in proving an offence;[169] where the data controller must comply with an obligation to which the controller is subject or by law;[170] protecting the vital interests of the data subject;[171] or where the data controller is performing a task in the public interest or in the exercise of official authority vested in the controller or a third party to whom the data is disclosed.[172] Consent also is unnecessary where processing is meant to promote the legitimate interests of the controller or a third party to whom data is disclosed.[173] However, legitimate interest cannot be relied on where the legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject.[174] POTRAZ may specify conditions when legitimate interest is considered to have been met.[175]

Processing of sensitive data without the data subject's consent is prohibited.[176] Sensitive data is information or any opinion revealing the racial or ethnic origin, political opinions and affiliations, religious and philosophical beliefs of a data subject. It also includes membership of a professional or trade association; membership of a trade union; sex life; criminal, educational, financial or employment history; gender, age, marital status, family status; health information, genetic information; and any information presenting major risks to a data subject. Where a data subject consents to the processing of sensitive data, such consent may be withdrawn without explanation.[177] POTRAZ, however, can prohibit the processing of sensitive data even where the data subject consents.[178]

Where the processing of sensitive data may affect national security or the interests of the state, the minister responsible for cybersecurity may direct how sensitive information must be processed.[179] Written consent is unnecessary to process sensitive data where processing is required to carry out obligations and specific rights of a data controller in the field of employment law,[180] and where it is necessary to protect vital interests of the data subject where they are unable to

168 CPDA (n 1) sec 10(1).
169 CPDA (n 1) sec 10(3)(a).
170 CPDA (n 1) sec 10(3)(b).
171 CPDA (n 1) sec 10(3)(c).
172 CPDA (n 1) sec 10(3)(d).
173 CPDA (n 1) sec 10(3)(e).
174 As above.
175 CPDA (n 1) sec 10(4).
176 CPDA (n 1) sec 11(1).
177 CPDA (n 1) sec 11(2).
178 CPDA (n 1) sec 11(3).
179 CPDA (n 1) sec 11(4).
180 CPDA (n 1) sec 11(5)(a).

consent.[181] Written consent is unnecessary where processing is carried out during legitimate activities of a foundation, association or non-profit organisation.[182] The foundation or non-profit organisation must have a political, philosophical, religious, health insurance or trade union purpose. The processing must also relate solely to the members of the organisation or people who have regular contact with the organisation. The data controller must obtain the consent of the data subject before sharing sensitive data.

Sensitive data can be processed without consent if the processing is for compliance with national security laws;[183] is necessary for the establishment, exercise or defence of legal claims;[184] if it relates to data that has been made public by the data subject;[185] where processing is necessary for scientific research;[186] or if the processing is authorised by law or any regulation.[187] Data relating to sex life may be processed without consent by an association with a legal personality or by a public interest organisation whose main objective is the evaluation, guidance or treatment of a person of certain sexual conduct.[188] The organisation must be recognised by a competent public body as being responsible for the welfare of such persons. The objective of the processing by the organisation must consist of evaluation, guidance and treatment of persons.[189]

Genetic, biometric and health data must also be processed with the written consent of the data subject. The exceptions to this also apply to the processing of genetic data, biometric data and health data.[190] Health data, however, may only be processed under the responsibility of a healthcare professional.[191] Healthcare professionals and their agents are bound by the duty of professional secrecy.[192] An exception is if the data subject consents in writing, and it is necessary for the prevention of imminent danger or mitigation of a specific offence.

CDPA prohibits the collection of health data from other sources unless the data subject is incapable of providing the data.[193] Health-related data, however, must only be processed where a unique patient identifier is given to the patient. This patient identifier must be distinct from any other identification number issued by the public authority, for example, a national identity number or a passport number. The linking of the unique patient identifier with other identifiers that

181 CPDA (n 1) sec 11(5)(b).
182 CPDA (n 1) sec 11(5)(c).
183 CPDA (n 1) sec 11(5)(d).
184 CPDA (n 1) sec 11(5)(e).
185 CPDA (n 1) sec 11(5)(f).
186 CPDA (n 1) sec 11(5)(g).
187 CPDA (n 1) sec 11(5)(h).
188 CPDA (n 1) sec 11(5)(i).
189 CPDA (n 1) sec 11(5)(j).
190 CPDA (n 1) secs 12(3)(a)-(j).
191 CPDA (n 1) sec 12(4).
192 CPDA (n 1) sec 12(7).
193 CPDA (n 1) sec 12(6).

may result in the identification of the data subject is prohibited. An exception to this prohibition is when there has been express authorisation by POTRAZ.[194]

4.10 Incomplete obligations

CDPA is not explicit on some of the critical obligations on data controllers, which have become standard in data protection legislation around the world. GDPR, in particular, clearly articulates these principles.[195] This is a missed opportunity to strengthen the protection of personal information by CDPA. The first of such obligations is data protection by design. Data protection by design ensures that data protection principles are implemented, and the necessary safeguards are in place when an information technology system is designed.[196] At the core of data protection by design is the idea that data protection must be inscribed into the design of information technologies from the outset. The second modern principle is that data protection must be by default. This principle is assumed in the various CDPA provisions but is not explicitly stated.[197]

This ensures that only necessary data is collected and processed by data controllers. Data protection by design and default constitutes a shift to a proactive model of data protection aimed at preventing data protection issues instead of remedying them. The failure of CDPA to include an obligation of ensuring data protection by design and default means that CDPA adopts a reactive model to data protection as its provisions are meant to deal with issues of data breaches and other data protection-related matters when they occur. Closely related to the issue of data protection by design and default is the concept of privacy and data protection impact assessments. These are processes 'designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them'.[198] There is no requirement for controllers to carry out privacy and data protection impact assessments before releasing a product significantly involving the collection and processing of personal data.

Impact assessments enable controllers to rethink data processing. They provide controllers with an opportunity to comply with data protection legislation and

194 CPDA (n 1) sec 12(8).
195 GDPR arts 25(1) & (2)
196 European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020'.
197 The CDPA provides in secs 18(1)-(4) on security measures that data controllers can adopt. These measures take into account the state of technological development and the cost of implementing the measures, on the one hand, and the nature of the data to be protected. This provision is helpful but not sufficient, as a data controller has room to manoeuvre, especially using costs as a factor.
198 Article 29 Working Party 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' 4.

demonstrate appropriate measures taken to ensure legal compliance.[199] It is yet to be seen if POTRAZ with its broad powers to issue guidelines will make impact assessments mandatory. If POTRAZ seeks to make impact assessments mandatory, it should ideally compile lists inclusive of when it considers it necessary for a data controller to carry out an impact assessment and those circumstances that do not require impact assessments. An impact assessment would also enable controllers realising high risk to ensure that there is prior consultation with POTRAZ and data subjects to ensure that the processing does not result in an infringement of fundamental rights.

4.11 Rights of data subjects

CDPA provides for the rights of data subjects. The first is the right to be informed of how their personal information is used.[200] This must be done at the time of collection of data by the data controller.[201] The second is a right of access to personal information held by a data controller or data processor.[202] This right is exercised under the Freedom of Information Act (FOIA) as well, which is administered by a constitutional commission, and the timelines listed there might apply, but there might be conflicts between ZMC and POTRAZ on a request. However, there is no provision on the timeframe within which the data controller or data processor must comply with the request for access in CDPA and, therefore, provisions of FOIA apply. Furthermore, CDPA does not describe the nature and scope of the right. This means that it will be up to the POTRAZ to issue guidance on the nature of the right of access and what it entails. Other rights include a right to object to the processing of all or part of personal information;[203] a right to correction of false or misleading personal information;[204] and a right to deletion of false or misleading data about them.[205]

Data subjects have a right not to be subjected to a decision based solely on automated processing and profiling where the processing or profiling produces legal effects on the data subject and affect them.[206] Automated processing is permissible where the data subject consents or where the processing is premised on a provision established by law.[207] However, some data subject rights which have become standard in international data protection law are not provided for by CDPA. The first of such rights is the right to erasure, commonly known as the right to be forgotten. While there is a right to deletion in CDPA, it is limited to the deletion of false or misleading data and excludes correct personal information.

199 As above.
200 CPDA (n 1) sec 14(a).
201 CPDA (n 1) sec 15(1)(b).
202 CPDA (n 1) sec 14(b).
203 CPDA (n 1) sec 14(c).
204 CPDA (n 1) sec 14(d).
205 CPDA (n 1) sec 14(e).
206 CPDA (n 1) sec 25(1).
207 CPDA (n 1) sec 25(2).

The right to erasure constitutes a fundamental safeguard for the enforcement of data protection principles, especially the principle of data minimisation. The right to erasure is not absolute and usually has limited grounds upon which it can be invoked.[208] While the right itself is not without controversy and has been the subject of intense debate in Europe, the rationale for its existence was correctly underscored in *Google Spain*[209] where the Court held that the right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest in access to information. Thus, its absence from CDPA leaves a lot to be desired as there are circumstances where an individual's right to privacy will be greater than the public interest of access to information and commercial gain.

The second such right excluded from the Act is the right to data portability. The right allows a data subject to receive their data in a structured, common and machine-readable format. The importance of the right is to give more control over data to the subjects to allow for the free movement of data between providers. At a time when data sharing and reuse of data are becoming more mainstream in the digital economy, the absence of a right to data portability significantly hinders the ability of data subjects to move between service providers. The third right excluded from CDPA is the right to the protection of personal information or data. The Zimbabwean Constitution contains a right to privacy but not a right to the protection of personal information. While there is a relationship between privacy and the protection of personal information, the two rights are distinct.[210]

There is no consensus among scholars regarding what constitutes a right to privacy, but most definitions are framed in terms of information control.[211] Privacy is a 'claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others'.[212] A right to the protection of personal data seems to suffer a similar fate with some scholars arguing that the essence of the fundamental right to the protection of personal data is an elusive concept.[213] However, at its core, a right to protection of personal data enables people to check the accuracy and relevance of data concerning them, how personal data files should be properly set up and managed,

208 GDPR (n 45) art 17.
209 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317.
210 An examination of the distinction between the two rights is beyond the scope of this work. For a discussion of the difference between the two rights, see M Tzanou 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3 *International Data Privacy Law* 88-99. See also G González Fuster *The emergence of personal data protection as a fundamental right of the EU* (2014).
211 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 277.
212 As above.
213 M Brkan 'The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning' (2019) *German Law Journal* 878.

and legal sanctions for the misuse and abuse of personal data.[214] A right to data protection, therefore, is concerned with 'informational autonomy'.[215]

Despite their differences, the rights to privacy and protection of personal data interact in several ways.[216] In Zimbabwe, section 57 of the Constitution protects the right to privacy. It includes the right not to have possessions searched or seized, premises entered, communications infringed, and health data disclosed without authority. The right to privacy has been interpreted as being the right not to be subjected to the scrutiny of personal life or business.[217] The interpretation was premised on the interpretation of the right to privacy by the South African Constitutional Court in the case of *Gaertner & Others v Minister of Finance & Others*[218] in which it was held that '[t]he right to privacy embraces the right to be free from intrusions and interference by the state and others in one's personal life'.[219]

The Supreme Court of Zimbabwe in *Netone v Econet* interprets the essence of the right to privacy as being informational control. The right to privacy in the Zimbabwean Constitution, therefore, focuses predominantly on informational control. However, there is an element of informational autonomy derived from a reading of section 57(1)(e) of the Constitution, giving people a right not to have their health data disclosed. Nonetheless, informational autonomy is limited to health data. This means that the right to privacy as provided for in the Constitution does not cover informational autonomy, which is the essence of the right to data protection. Thus, the constitutional right to privacy on its own is inadequate to regulate issues of data protection.

Section 47 of the Constitution states that the rights contained in chapter 4 of the Constitution do not preclude the existence of other rights and freedoms that may be recognised or conferred by law, to the extent that they are consistent with the Constitution. CDPA, therefore, ought to have created a separate right to the protection of personal information to complement the constitutional right to privacy. This is because a right to protection of personal information would serve multiple interests potentially extending beyond the traditional concepts of privacy.[220] The view carried by CDPA that the protection of personal information essentially is privacy protection may obscure the realisation of the benefit of data

214 See the explanation of Hondius as to why there was a separate need for protection of personal data that differed from privacy and confidentiality. F Hondius 'A decade of international data protection' (1983) 30 *Netherlands International Law Review* 103-128.
215 Tzanou (n 210) 89.
216 A Rouvroy & Y Poullet 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' in S Gutwirth and others (eds) *Reinventing data protection*? (2009) 45.
217 *Netone Cellular (Private) Limited & Another v Econet Wireless (Private) Limited & Another* SC 47/18.
218 [2013] ZACC 38; 2014 (1) SA 442 (CC).
219 As above.
220 Bygrave (n 211).

protection to society as a whole and might ultimately hamper advocacy and the development and implementation of stronger data protection laws.

CDPA also lacks remedies for data subjects in the event of a breach. Data subjects, therefore, could use the law of delict to recover damages for data breaches or unlawful data processing causing harm. Whether the law of delict will provide recourse in the event of harm remains to be seen, given the rigidity of Zimbabwean courts in extending the applicability of the common law. The best approach, however, would be for a separate cause of action to be created targeting harm resulting from data breaches. Whether data subjects would succeed is one thing, but the absence of recourse leaves much to be desired.

4.12 Transfer of personal information outside Zimbabwe

CDPA prohibits the transfer of personal information to a third party in a foreign country or an international organisation unless an adequate level of protection is ensured in the country of receipt or recipient international organisation.[221] Adequacy is assessed considering all circumstances surrounding a data transfer operation, namely, the nature of the data; the purpose and duration of the proposed processing; the recipient third country or international organisation and professional rules; and security measures that are complied with within the third country or international organisation.[222] POTRAZ has exclusive authority to determine categories and circumstances in which the transfer of data to countries outside Zimbabwe is unauthorised. When a country has an adequacy decision and POTRAZ has made a list of data that is ineligible to be transferred outside Zimbabwe, data will not be able to leave Zimbabwe.[223] Whether such a provision will be consistent with the provisions of AfCFTA remains to be seen as this is not a standard clause in data protection legislation.

Transfers of data to a country devoid of an adequate level of protection can occur in six circumstances. The first is where the data subject has unambiguously consented.[224] The second is where the transfer is necessary for the performance of a contract between the data subject and the data controller or in the implementation of pre-contractual measures at the request of the data subject.[225] The third is where the transfer is necessary for the conclusion or performance of a contract that is concluded or is to be concluded by the data subject and the data controller.[226] The fourth is where the transfer is necessary on public interest grounds or for the establishment, exercise or defence of legal claims.[227] The fifth

221 CDPA (n 1) sec 28(1).
222 CDPA (n 1) sec 28(2).
223 CDPA (n 1) sec 28(3).
224 CDPA (n 1) sec 29 (1)(a).
225 CDPA (n 1) sec 29(1)(b).
226 CDPA (n 1) sec 29(1)(c).
227 CDPA (n 1) sec 29(1)(d).

is where a transfer is necessary to protect the data subject's vital interests.[228] The sixth is when the transfer is made from a register that is intended to provide information to the public and is open to the public in terms of an Act of Parliament or regulations.[229] There is no obligation of disclosure to the data subject when the controller intends to transfer personal data to a third country or international organisation and whether a decision of adequacy exists. Disclosure would only occur when the data controller seeks the data subjects' consent for such transfer.

4.13 Offences and penalties

CDPA provides for criminal penalties for violations of its provisions. The penalties may be imposed on data controllers, their representatives, agents or assignees when they violate the provisions relating to the processing of sensitive data; when they fail to fulfil duties in terms of section 13;[230] when they are not accountable as prescribed by section 24; when they transfer data outside Zimbabwe, against the provisions of section 28; and when they contravene the security requirements under section 18(4). Once found guilty, the data controller or their representatives will be liable to a fine not exceeding level 11[231] or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.[232] The court may also order the seizure of the media containing the data to which the offence relates or the deletion of the data. The computers themselves are not liable for seizure in terms of CDPA.[233]

Objects seized post-conviction must be destroyed, and the data controller shall be liable for the payment of the fines incurred by the agent or assignee. POTRAZ is not authorised to issue penalties or fines for violations of CDPA by data controllers and processors. Prosecution for violation of CDPA will be left to the NPA as violations are criminal offences that attract imprisonment, and it is the constitutional mandate of the NPA to prosecute criminal offences. This limits the enforcement capabilities of POTRAZ. Ideally, POTRAZ should be empowered to issue administrative fines and penalties for violations of CDPA.

228 CDPA (n 1) sec 29(1)(e).
229 CDPA (n 1) sec 29(1)(f).
230 CDPA (n 1) sec 13: 'Duties of data controller: Every data controller or data processor shall ensure that personal information is – (a) processed in accordance with the right to privacy of the data subject; (b) processed lawfully, fairly and in a transparent manner in relation to any data subject; (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required; (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.
231 For transgressions classified under level 11, the fine will not exceed US $1 000 in accordance with Statutory Instrument 14A of 2023.
232 CDPA (n 1) sec 33(2).
233 CDPA (n 1) sec 33(3).

These could include powers such as an order to stop processing or an order to delete data that is held by the data controller.

5 Conclusion

CDPA is a significant step towards protecting personal information in Zimbabwe, considering the absence of protection of personal information under common law and customary law. Private entities had no obligations to protect personal information under AIPPA. They are now obliged to protect personal information under CDPA. The protection of personal information is premised on the constitutional right to privacy. While CDPA reflects modern-day data protection law in most of its provisions, it has several weaknesses. These include using privacy as a premise for the protection of personal information rather than an independent right to data protection; the failure to include other data subject rights such as the right to be forgotten, the right to approach the courts for compensation for infringements of CDPA; the DPA lacking power to prescribe administration sanctions; as well as the absence of provisions guaranteeing the independence of the DPA and inadequate provisions on disclosure to data subjects.

CDPA also fails to address its relationship with the CPA, creating room for forum shopping and the possibility for divergent enforcement by two different DPAs. However, some of the weaknesses in CDPA can be rectified through statutory instruments issued in terms of CPDA or through guidance by POTRAZ. The regulations can lay down requirements for data controllers and processors to conduct impact assessments, and implement data protection by design and default. The regulations can also lay down rules on the nature of the right to access, circumstances when consent can be assumed, and requirements for data subjects to be notified of serious data breaches. It is also recommended that CDPA be amended to include other data subject rights such as the right to be forgotten as well as the right to data portability. This should be accompanied by remedies for data subjects when there have been violations of their rights. The supervisory function should be removed from POTRAZ and an independent authority established and given the status of a constitutional commission. These recommendations will act to further strengthen the significant inroads CDPA has made in ushering Zimbabwe into a new age of data protection.