Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the *Protection of Personal Information Act*

V Bronstein*

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed, open access online law publications

Author

Victoria Bronstein

Affiliation

University of the Witwatersrand, South Africa

Email

victoria.bronstein@wits.ac.za

Date Submitted

2 July 2021

Date Revised

15 August 2022

Date Accepted

15 August 2022

Date published

13 December 2022

Editor Mr M Laubscher

How to cite this article

Bronstein V "Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the *Protection of Personal Information Act*" *PER / PELJ* 2022(25) - DOI http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11661

DOI
http://dx.doi.org/10.17159/1727-3781/2022/v25i0a11661

Abstract

Although the *Protection of Personal Information Act* 4 of 2013 (POPIA) wholeheartedly adopts the command-and-control features of the EU *General Data Protection Regulation* (GDPR), POPIA does not include many of the collaborative governance mechanisms in the GDPR. POPIA dilutes the accountability requirements in the GDPR. It rarely requires responsible parties to generate or keep documentation and there is no equivalent of European Data Protection Impact Assessments in the South African Act. This affects the regulation of automated processing that involves profiling. The European system of certifications is also not included in POPIA. POPIA includes a system of codes of conduct but even they have a more peremptory nature. The absence of collaborative governance mechanisms in POPIA constitutes a missed opportunity to build a culture of enhanced data protection in South Africa. The Information Regulator has the task of giving many exemptions and prior approvals under the Act. The newly constituted Information Regulator will find itself exposed as it faces a particularly difficult mandate.

Keywords

Internet privacy; GDPR; data protection; POPIA; codes of conduct; data protection impact assessments; regulation; automated processing; profiling; command-and-control regulation; collaborative governance.

.....

1 Introduction

Both the South African *Protection of Personal Information Act* (POPIA)[1] and the EU *General Data Protection Regulation* (GDPR)[2] endeavour to safeguard fundamental foundations of democratic societies in an era of extraordinary technological change. These legislative instruments aim to foster the development of an ethical culture for the management of personal data.

The unregulated processing of personal data creates many high-profile dangers for data subjects. Ordinary people face multiple data security issues every day. "Automated processing of personal information" that includes profiling[3] creates risks for data subjects. In democratic countries, it may initially have seemed that the main danger was that computer algorithms were being used to nudge people, mainly for the purpose of selling consumer products and services to them.[4] It is apparent, however, that the risks are deeper. Controversy about artificial intelligence systems has abounded, from the Cambridge Analytica saga where Facebook's data were famously used to target specially identified individuals in order to influence a US election, to facial recognition systems that mis-identify arbitrary members of racial minorities.[5] The literature on these issues is abundant and it is unnecessary to review it here[6] save to say that multiple ethical issues arise with automated decision-making. Apart from algorithms potentially having a devastating effect on the rights of people, artificial intelligence (AI) systems are famously opaque. There is always a risk that things will take a totalitarian turn and propel us into a dystopian future. Current AI systems that are used in policing and national security

* Victoria Bronstein. BA (Hons) LLB (Wits) LLM (London). Associate Professor, School of Law, University of the Witwatersrand, Johannesburg, South Africa. E-mail: victoria.bronstein@wits.ac.za. ORCiD: https://orcid.org/0000-0002-5542-5466

1 *Protection of Personal Information Act* 4 of 2013 (hereafter POPIA).

2 *European Union General Data Protection Regulation*, 2016 (Regulation (EU) 2016/679) (hereafter GDPR).

3 Section 71(1) of POPIA.

4 Zuboff *Age of Surveillance Capitalism.*

5 See for example Amer and Noujaim *The Great Hack*; *R (on the Application of Edward Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058; Hao 2020 https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/.

6 But see for example references cited in Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 148-150; Roos "Data Privacy Law" 363-368.

foreshadow this outcome.[7] Internationally there is increased awareness of the risks of data processing and the need to protect data subjects:

> Seen in this light, contemporary data protection law can be understood as analogous to environmental regulation: it seeks to protect the democratic 'commons,' that is, the moral, democratic, and cultural environment, as opposed to the natural, physical environment.[8]

Data protection law aims to protect the foundations of liberal democracies. Although historically artificial intelligence systems were often seen as a powerful, objective ways of removing human failings from decision-making, there has been a shift in understanding which acknowledges that the computer systems that human beings create are laden with harmful possibilities that can multiply relentlessly through automated processing.[9]

The GDPR and POPIA are early attempts to mitigate these risks by creating a legal framework that protects the personal information of data subjects. These legislative instruments are very much in their infancy. Their aim is to effect positive cultural change among those that control and process data.

Although cyberspace seems impervious to regulation, the objective of effecting cultural change among those who process personal data is not as far-fetched as it may seem. Personal data protection already works effectively in many spheres. For example, most professionals are careful with the personal data of their clients or patients and many of them take extreme care. Professional bodies routinely apply codes of conduct that protect the privacy and confidentiality of data subjects. One of the aims of personal data protection legislation is to develop this ethos more generally among those who process personal data. In South Africa large institutions like the banks have invested significant resources in improving data protection and complying with POPIA.

Although on the surface there are deep similarities between the regulatory regime in the GDPR and that in POPIA, a second look shows that the systems are very different. This paper argues that POPIA has seamlessly adopted the command-and-control type aspects of the GDPR's approach to

---

7 Greenwald, MacAskill and Poitras 2013 https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

8 Yeung and Bygrave 2021 *Regulation and Governance*.

9 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 147-150; Constantinescu 2021 https://www.researchgate.net/publication/356612427_AI_moral_externalities_and_soft_regulation 4.

regulation. However, the GDPR contains many collaborative governance elements and most of those were not included in POPIA.

POPIA has been shaped by what is known as the "Brussels effect"[10] and consequently the legislation is based on the same principled foundation as the GDPR. The South African Information Regulator is an independent regulatory body that has functions under POPIA similar to those of the supervisory authorities that operate in the various European states. The Information Regulator is designed to deal with complaints about violations of data protection law and it has significant power to sanction wrongdoers. Like its European counterparts it also receives notifications of data breaches.

Although POPIA and the GDPR look similar, the collaborative governance features of the legal regime in the GDPR were not made part of the South African Act. The system of Data Protection Impact Assessments (DPIAs), which is an important pillar of the GDPR system, has no counterpart under POPIA. The DPIA system is backed by possible audits, which means that there is potential oversight of the data controllers' documentation by European supervisory authorities.

The GDPR contains other collaborative governance devices that are not part of POPIA. For example, POPIA does not provide for voluntary certification processes. Although POPIA does provide for codes of conduct which are an important collaborative governance feature, the South African enforcement mechanisms for codes of conduct have a strong command-and-control flavour that is not envisaged under the European legislation.

After exploring those features, this paper uses the legislative provisions that deal with the regulation of automated processing involving profiling as a lens into the different regulatory approaches under the GDPR and POPIA. Although the individualised remedies available for data subjects under the two regimes are similar, it is debatable how effective these remedies could be. The GDPR engages in systemic management of high-risk automated processing that involves profiling using a system of DPIAs. DPIAs aim to improve compliance and accountability and to put some brakes on automated processing. These mechanisms are not included in POPIA.

Unlike the GDPR, POPIA defines many circumstances in which responsible parties or data controllers need to get prior approval from the South African Information Regulator to commence processing. Some of these approvals

10 Bradford *The Brussels Effect*.

will be needed for automated processing that involves profiling (although multiple prior approvals are needed in other spheres as well). The newly constituted Information Regulator faces a particularly difficult mandate, which includes issuing prior approvals in a broad range of circumstances. Based on the experience of other supervisory authorities, it is difficult to be optimistic about the Regulator's ability to effectively fulfil these functions.

Ultimately POPIA will be effective only if a broad range of actors internalises the ethical principles in the Act and integrates them into everyday life. DPIAs and other collaborative governance mechanisms aim to recruit data controllers to assist in achieving this end. The South African legislature's omission of collaborative governance mechanisms constitutes a missed opportunity to effectively improve data protection culture in South Africa.

This paper starts by contrasting command-and-control approaches to regulation with strategies of collaborative governance. It analyses regulatory strategies that use prior approvals or licensing systems both generally and particularly in the context of the processing of personal information. Second, the paper illustrates that there are profound similarities between the GDPR and POPIA. Both regulatory systems are based on the same principled foundation and their regulators are constituted in similar ways. Third, the paper explores how the collaborative governance features in the GDPR were either excluded from or watered down in POPIA. DPIAs and certification systems are excluded from POPIA while the collaborative governance features of codes of conduct are watered down in the South African Act. Fourth, automated decisions that involve profiling provide a lens into the different regulatory regimes introduced by the GDPR and POPIA. Although the individualised remedies offered to data subjects are similar in Europe in South Africa, the more important systemic treatment of automated processing that involves profiling is very different under the two legal regimes. While the GDPR depends upon DPIAs to assist with risky processing, the South African Information Regulator presides over a complex patchwork of prior approvals and exemptions, including authorisations under sections 57 and 58 of POPIA. The penultimate section of the paper focusses on the role of the South African Information Regulator against the background of challenges faced by European supervisory authorities. The paper concludes that the omission of collaborative governance features and particularly DPIAs from POPIA constitutes a missed opportunity to improve data protection culture in South Africa.

2 Regulatory strategies

2.1 Command-and-control v collaborative governance

POPIA is more dependent on command-and-control type regulation than the GDPR. The GDPR incorporates a range of features associated with collaborative governance. Although the labels command-and-control and collaborative governance are inexact, they do help to distinguish different regulatory trends in modern industrial societies.

Collaborative governance strategies fit with the concept of "decentred regulation", which includes self-regulatory schemes and co-regulation.[11] In South Africa self-regulation is used to regulate the professions, advertising and broadcasting. Strategies which use third parties to monitor compliance, like auditors, inspectors, NGOs, standards councils or other technical committees, also fit within a conception of decentred regulation.[12]

The archetype of command-and-control regulation is based on Austin's theory of law which famously conceptualises law as the command of a sovereign backed by sanctions.[13] Models of regulation that are predominantly based on command-and-control are frequently criticised for being ineffectual and not cost effective.[14] These deficiencies stem from the central practical and theoretical problem with command-and-control regulation. If the "core regulatory problem" is how to influence others to change their behaviour,[15] then what motivates social actors to obey the law or to comply with a regulatory regime?

Although psychological studies show that the threat of sanctions may well deter individual actors, the deterrent effect only seems to work at scale when legal subjects view the probability of detection as being very high.[16] This leads to the conclusion that in order for command-and-control

---

11 See Black 2001 *CLP* 122. "The [UK] Regulators' Compliance Code stressed: the need for regulators to adopt a positive and proactive approach towards ensuring compliance by: • helping and encouraging regulated entities to understand and meet regulatory requirements more easily; and • responding proportionately to regulatory breaches". Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 21.

12 Black 2001 *CLP* 119.

13 Hart characterises this aspect of Austin's theory as the idea of the gunman writ large (Hart *Concept of Law* ch 2).

14 Gunningham and Sinclair date unknown https://www.oecd.org/env/outreach/33947759.pdf.

15 Black 2001 *CLP* 123.

16 Blanc *From Chasing Violations to Managing Risks* 145; Tyler "Psychology of Self-Regulation" 82-83.

strategies to be effective, huge resources would have to be committed to the deployment of sanctions.[17] The comprehensive large-scale use of sanctions is generally considered unfeasible in democratic societies.[18] Indeed most would agree that the chances of comprehensive sanctions being effectively deployed to achieve large-scale compliance in South Africa are negligible.

A recent series of articles edited by Peter Drahos[19] grapples with the question of what makes social actors comply with precepts contained in legislation. Tom Tyler explains that as the threat of sanctions is insufficient to achieve the legislator's objectives,[20] it is necessary to use other methods like "education, guidance [and] opinion forming" to achieve the desired results.[21] Other related strategies are advising and supporting legal subjects in ways that negotiate change.[22] These various hybrid strategies are frequently used by governments in order to facilitate behavioural change. They tend to be employed alongside sanctions, which can be used as a last resort.[23]

Christopher Hodges draws on the theory of HLA Hart and argues that by and large people comply with law because of an "internalized sense of duty".[24] Citizens are more likely to obey legal precepts because they view them as "right and just" than because they fear punishment.[25] Even in cases where legal subjects don't support a particular rule, they may well comply when the system is generally regarded as legitimate.[26] Consequently

17 Blanc *From Chasing Violations to Managing Risks* 145.

18 Blanc *From Chasing Violations to Managing Risks* 145; Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 28-29; Tyler "Psychology of Self-Regulation" 82.

19 Drahos *Regulatory Theory.*

20 Tyler "Psychology of Self-Regulation".

21 Blanc *From Chasing Violations to Managing Risks* 145.

22 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 21.

23 This hybrid approach has also become known as decentred regulation.

24 Hart *Concept of Law* ch 5 pt 2; Blanc *From Chasing Violations to Managing Risks* 147; Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 17. Hodges does not refer to nudging but see Blank who does (Blanc *From Chasing Violations to Managing Risks* 119); Murphy "Procedural Justice" 44.

25 Murphy "Procedural Justice" 44.

26 Procedural justice is important, and people should have the opportunity to voice their concerns. Murphy "Procedural Justice" 48. Another important finding is that good regulators that treat subjects fairly can "promote voluntary compliance behaviour" even in instances where the particular law is viewed as unjust. Murphy "Procedural Justice" 45-46; Tyler "Psychology of Self-Regulation" 90-93. See Donovan *Reconceptualising Corporate Compliance* in the context of compliance with tax regulation, illustrating that in democratic societies the quality of regulatory institutions matters in more ways than we might think.

regulators that prioritise procedural justice play a role in fostering "voluntary compliance".[27]

It follows that in order to be effective, regulation needs to shift its focus from providing and perfecting enforcement "to achieving behavioural change".[28] Hodges argues that the main aim of regulatory systems is to change the culture of those they aim to regulate.[29] "If safety and economic goals are to be effectively achieved" governments need to use "a collaborative approach to business and regulation, rather than a remote, adversarial and uncooperative approach".[30] In Hodges view public safety cannot be protected in the absence of increased self-regulation and co-regulation.[31] Hard enforcement should be resorted to only when a softer approach fails.[32]

There are other even more powerful drivers pointing towards collaborative governance mechanisms in the context of data protection. Most importantly it is simply not practical for governments to police the cyberworld. In the era of artificial intelligence and machine learning, government regulators always face a deficit of both information and expertise.[33] Black and Murray dissect the features of automatic processing, artificial intelligence and machine learning, which are characterised by

> … complexity, both conceptually and in terms of the actors and organisations involved; the fragmentation of power, capacities and responsibilities; the inevitable interdependencies between all actors within the system or network, not least regulators and regulatees; the inherent ungovernability of actors due to their ability to exercise agency and choice; and the rejection of a clear distinction between public and private in the performance of regulation …[34]

---

27 Murphy "Procedural Justice". Or see Blanc, who deals with the limitations of this perspective (Blanc *From Chasing Violations to Managing Risks* 145, 159, 311).

28 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 27. "[P]ersonal and group values of human actors and the ethical culture of their organisational groups" is fundamentally important (Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 24).

29 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 24-28. Also see Adamson "Importance of Culture in Driving Behaviours of Firms".

30 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 23.

31 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 23, 27, 28.

32 That supports the view that compliance "behaviour is affected by information, advice, support and reminders" which is consistent with psychological research (Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 19).

33 Finck 2017 http://eprints.lse.ac.uk/87568/1/Finck_Digital%20Co-Regulation_Author.pdf 19.

34 Black and Murray 2019 *EJLT*.

The fact that data flow freely over national boundaries without any technical barriers adds to this complexity.

Any attempt to control the virtual world needs to use hybrid regulatory strategies that engage both state and non-state actors.[35] In order for regulation to achieve its ultimate goal of influencing behaviour there will need to be "multiple points of accountability" and "accountability mechanisms".[36] Decentred regulation and collaborative governance are designed to provide these opportunities.

This is not to be naïve about potential problems with co-regulation or collaborative governance. Edelman and Talesh illustrate how businesses have used their co-regulatory or collaborative status to play an important role in influencing how they will be governed in the long term.[37] They argue that this trend had a particularly negative outcome in the 2008 financial crisis.[38] In the past, big business has used its co-regulatory status to influence how judges ultimately interpret the law.[39] Edelman and Talesh remind us that it will take vigilance to ensure that the democratic infrastructure of modern societies is not further undermined.

2.2 Licensing or prior approvals

Systems that require prior approvals or licensing are generally regarded as the "most interventionist of regulatory forms".[40] They fit within the ambit of command-and-control regulation. The general regulatory literature points out that prior approvals or licensing systems tend to be used to regulate spheres "that need to make use of centralised, scarce, or public resources, or which pose systemic risks or risks of 'deep regret', such as to life".[41] Consequently, licensing is traditionally used to register professionals like doctors or lawyers or to operate dangerous things like motor vehicles or firearms.

Different issues arise with prior approvals or licensing systems depending on the subject matter that they aim to regulate. For example, Black and Murray do not regard the use of prior approvals as a viable option for regulating AI and machine learning (ML). They argue: "It is too late for us to

35 Black and Murray 2019 *EJLT.*
36 Black and Murray 2019 *EJLT.*
37 Edelman and Talesh "To Comply or Not to Comply".
38 Edelman and Talesh "To Comply or Not to Comply" 115.
39 Edelman and Talesh "To Comply or Not to Comply" 105.
40 Ogus *Regulation* 9. On licensing generally see Bhagwat 1999 *Hastings LJ* 1279.
41 Black and Murray 2019 *EJLT.*

put AI and ML back into a box."[42] In modern democracies some types of AI are already regulated by systems of prior approval, for example in the medical field. But in general Black and Murray take the view that "there is little evidence that regulators have the necessary capacity properly to evaluate all the actual and potential uses of AI in their regulatory domains. Asymmetries of knowledge and skills are amplified in the highly technical area of AI".[43] Hence prior approvals are not viewed as a practical solution to the many varied problems caused by AI.

This view coheres with the regulatory approach in Europe. The GDPR does not require data controllers to get pre-approvals or licenses from supervisory authorities before risky processing can commence. Unlike the typical data protection regime in the EU (which can of course be varied by national legislatures in different member states), POPIA frequently requires responsible parties to apply for prior authorisations or exemptions to do particular types of processing. This is in stark contrast to the *ex post* approach under the GDPR:

> *Ex ante* regimes rely on a system of prior approval by a regulatory authority, while *ex post* regimes typically entail the legal promulgation of certain minimum standards that the regulated activity must meet, thereby allowing the activity to be undertaken without obtaining prior approval, provided that legally mandated standards are met. Although some early national data protection regimes in Europe entailed extensive licensing requirements, advance authorization is generally not required by the GDPR nor national data protection regimes within the EU.[44]

Under POPIA, responsible parties frequently must apply to the Information Regulator for pre-approvals, authorisations or exemptions before processing may commence. The South African Information Regulator must make individual decisions about applications and if necessary, gazette the outcomes. This places a heavy burden on the institution.[45]

Licensing systems present well-recognised problems in the regulatory literature. If one looks beyond the context of cyber-regulation, Blanc refers

---

42 Black and Murray 2019 *EJLT.*

43 Black and Murray 2019 *EJLT.* The proposed EU draft AI Regulation does not rely on licensing or pre-approvals to regulate any processing. If pre-approvals are to be deployed, it would only be for the most high-risk processing, for example remote facial recognition (Vale, Demetzou and Matheson 2022 https://fpf.org/wp-content/uploads/2022/03/FPF_Brussels_Privacy_Symposium-2021.pdf 12).

44 Yeung and Bygrave 2021 *Regulation and Governance*.

45 Regulators need to have the necessary capacity and skill to manage the system. Licensing is expensive and "might divert resources from areas of greater need" (Bronstein 2002 *SALJ* 477).

to numerous studies that review the use of regulatory prior approvals or licensing systems. He finds that the general picture is that licensing regimes are not associated with better regulatory outcomes. Conversely studies find that "stricter regulation of entry is associated with sharply higher levels of corruption, and a greater relative size of the unofficial economy".[46]

That is not to say that I anticipate that the South African Information regulator will become corrupt. Quasi-judicial bodies tend to be guided by a strong professional ethos in South Africa. The more likely problem is that the Information Regulator will be overwhelmed by the many demands on its limited resources. If the institution appears to provide a poor-quality service, then the new regulatory framework will become increasingly irrelevant and this will conduce to a culture of low levels of compliance with POPIA.

For these reasons legislators need to reflect about the extensive use of prior approvals in POPIA if they wish to achieve optimal results.

3 Comparing the regulatory strategies of POPIA and the GDPR

3.1 The Brussels effect - similarities between POPIA and the GDPR

POPIA adopts the values and principles in the GDPR that deal with the processing of the personal information of data subjects. These principles have been part of European law for more than two decades in the form of the *European Directive on the Protection of Individuals with Regard to the Processing of Personal Data*.[47] They are now enforced throughout the European Union as part of the GDPR. They are also encoded in International Agreements such as the Council of Europe's *Convention 108* and the *African Union Convention on Cyber Security and Personal Data Protection*.[48]

One of the functions of the GDPR is to protect European citizens from the abuse of their personal data globally. The most obvious mechanism for the export of the values in the GDPR is the requirement that other countries and/or foreign organisations including multinationals need to adopt proper data protection practices before EU data controllers are permitted to share

46 Blanc *From Chasing Violations to Managing Risks* 136.

47 *Directive 95/46/EC*, 1995 of the European Parliament and of the Council.

48 *Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1981); *African Union Convention on Cyber Security and Personal Data Protection* (2014).

personal data with them.[49] This impetus led to the adoption of data privacy legislation in important developing countries including South Africa.[50] European data protection principles have had a cascading impact globally and the formal standards in the GDPR have spread in a movement nicknamed the "Brussels effect".[51]

The GDPR is infused with general principles of responsible and ethical data processing and the legal regime is not explicitly or implicitly tied to any particular technology.[52] POPIA adopts the same model. The GDPR requires legal persons who process personal information (known as "data controllers" in Europe or "responsible parties" in South Africa) to play a major role in determining and applying principles of fair, transparent and lawful data processing. The scope of POPIA is wider than that of the GDPR as South African data subjects can be both natural and juristic persons.[53]

The eight value-based conditions that form the foundation of POPIA are derived from European data protection law. In abbreviated form they are known as accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation.[54] In addition to these principles, POPIA contains stricter standards for the processing of special personal information (*inter alia* data about race, religion, health or biometrics) and the personal data of children.[55] The intention is that data subjects will be exposed only to reasonable, lawful and transparent data processing (or to use the European Union formulation fair, lawful and transparent processing)

---

49 See for example European Commission date unknown https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en.

50 UNCTAD 2020 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. See Roos 2020 *CILSA* 4.

51 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 184-185. Another consequence of the Brussels effect is that countries that don't implement high standards of data protection, like the United States of America, find themselves under pressure. For an indication of how this pressure is felt, see Meltzer 2020 https://voxeu.org/article/impact-gdpr-data-flows-and-national-security.

52 "Although this was an intentional choice as the EU did not want to bind the GDPR to explicit technologies that would favour specific platforms and solutions, this technology agnostic approach may cause unforeseen complications to organisations attempting to adapt their internal processes to the GDPR's provisions" (Politou, Alepis and Patsakis 2018 *Journal of Cybersecurity* 15).

53 See the definition of personal information, s 1 of POPIA.

54 Section 4(1) of POPIA and ch 3, pt A of POPIA.

55 See pt B (special personal information) and pt C (children's personal information) of ch 3 of POPIA.

that does not infringe on their privacy.[56] The objective is that these values will become integrated into data processing law and practice.

The GDPR avoids a system of rules and focusses on "outcomes rather than process, meaning that public authorities define the objectives to be achieved through standards rather than precise legal rules, leaving platforms to decide how to best achieve them, encouraging flexibility and adaptability, and providing room for manoeuvre to platforms".[57] Both the GDPR and POPIA depend on the implementation of a body of principles rather than rules.[58] This principle-based system enables the GDPR to mesh with general ethical standards, an approach that has the potential to lead to cultural change in the community that controls data.

3.2 The regulatory architecture of POPIA and the Information Regulator

When one first reads POPIA one is struck by the similarities between the South African Information Regulator and European supervisory authorities. The South African Information Regulator is credibly constituted in the Act as an independent regulator.[59] The institution differs from European supervisory authorities as the South African regulator has important functions in the freedom of information field under the *Promotion of Access to Information Act*.[60] Although the access to information role of the regulator is very interesting, this paper limits itself to dealing with the Information Regulator's functions under POPIA.

South Africa has strong civil society organisations that operate in the context of a free society and this augurs well for the tenure and effectiveness of the Information Regulator.[61] On the other hand the institution will inevitably be short of resources, which will impact on its effectiveness.

The Information Regulator has impressive coercive powers that are similar to those of foreign regulators although our fines do not reach the scale of those that can be levied in the EU.[62] Like European regulators, the South

---

56 Section 9 of POPIA; Art 5(1) of the GDPR. For a general comparison of the GDPR and POPIA see Roos 2020 *CILSA*.

57 Finck 2017 http://eprints.lse.ac.uk/87568/1/Finck_Digital%20Co-Regulation_Author.pdf 19.

58 Dworkin *Law's Empire* generally.

59 Chapter 5 (pt A) of POPIA.

60 *Promotion of Access to Information Act* 2 of 2000. See Allan and Currie 2007 *SAJHR* 570-586.

61 Bronstein and Katzew 2018 *JML* 245-253.

62 Adams and Adeleke 2020 *IDPL* 154.

African regulator has a primary function of resolving complaints about the misuse of personal data. It also receives and deals with data breach notifications. Another similarity is that the South African regulator has many educative and advisory functions including a role in building international relationships.[63]

In other respects, the South African Information Regulator has a very different role from supervisory authorities in Europe.[64] POPIA requires the Information Regulator to grant frequent prior approvals and exemptions before certain processing can commence. On the other hand, the GDPR does not rely on systems of prior approval. Instead, it contains a range of self-regulatory or co-regulatory features that are not part of POPIA.

Although the regulatory structure of the GDPR has important collaborative governance aspects, it is not the intention of this paper to minimise the command-and-control aspects of the legal regime. Ultimately the European framework gains its force from strong command-and-control features. The colossal fines that can be levied by European supervisory authorities are among the most important reasons why European organisations are cautious about the GDPR.[65] On the other hand, the GDPR appears to recognise that a regulatory regime cannot work in the absence of a "compliance culture".[66] In a new area like data protection, compliance cultures need to be built and developed.[67]

---

63 See generally s 40 of POPIA.

64 Yeung and Bygrave explain the EU's regulatory approach, which combines command-and-control features with aspects of collaborative governance in a picturesque manner: "The GDPR's role in regulating the processing of personal data is far more nuanced and sophisticated than simply promulgating a series of commands to be complied with on pain of state-enforced punitive sanction for violation, revealing the fallacy of exclusively equating the law's role in regulation with "command-and-control" regimes as is commonly believed. … Although the EU data protection regime is both technical and complex, drawing upon a range of techniques that combine both ex ante and ex post approaches, there is an underlying method to its apparent madness, underpinned by an overarching orientation that is primarily preventative: seeking to anticipate and prevent the unlimited collection and repurposing of personal data in order to reduce the dangers that might arise in the absence of any up-front restrictions. Hildebrandt provides an apt metaphor for this endeavor, likening it to Odysseus's strategy of tying himself and his crew to the mast to prevent them responding to the Sirens' call, thereby enabling them to resist the [overwhelming] temptation to gather more and more data and use it for more and more intrusive purposes and applications that will ultimately lead to downfall and destruction". (Yeung and Bygrave 2021 *Regulation and Governance*).

65 Kaminski 2019 *S Cal L Rev* 1533.

66 Kaminski 2019 *S Cal L Rev* 1568.

67 Kaminski 2019 *S Cal L Rev* 1560, 1561,1594.

3.3 Collaborative features of the GDPR that are excluded from or watered down in POPIA

3.3.1 Data protection impact assessments and auditing

The GDPR involves data controllers (or what we in South Africa call responsible parties) in their own regulation. "Collaborative governance shifts from commanding private actors to structuring both collaboration with and delegation to them."[68] The European system of DPIAs, which is discussed in more detail below, is a good example of this. As part of their accountability obligations, data controllers are required to conduct DPIAs before engaging in high-risk processing. Possible audits, which include checks of DPIAs, are another collaborative governance mechanism that is a cornerstone of the GDPR's regulatory regime.[69]

Although the South African Information Regulator does have the power to demand information from responsible parties about their processing, this system differs from the European system of auditing. The GDPR provides some clarity about the documentary requirements that organisations need to fulfil in order to comply with their accountability obligations. These include DPIAs in cases of high-risk processing.[70]

Under POPIA there is no well-established data processing paper trail and when a responsible party is challenged, the Regulator starts off at a disadvantage. It is interesting to note that the South African Information Regulator has already shown awareness of this shortcoming and has unobtrusively attempted to introduce documentary requirements through the Regulator's Guidelines for Information Officers.[71]

3.3.2 Certification systems

---

68 Kaminski 2019 *S Cal L Rev* 1564.

69 Kaminski 2019 *S Cal L Rev* 1570.

70 "Organisations, and not data protection authorities, must demonstrate that they are compliant with the law. Such measures include: • Adequate documentation on what personal data is processed; • Documented processes and procedures aiming at tackling data protection issues at an early stage when building information systems or responding to a data breach…. This is the first step towards compliance with the GDPR's accountability principle, which requires organisations to demonstrate (and, in most cases, document) the ways in which they comply with data protection principles when transacting business." (Data Protection Commission date unknown https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation).

71 See Information Regulator 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf para 4.2.

Apart from potential audits and DPIAs the GDPR also provides for certification systems. Article 42(1) of the GDPR states:

> The Member States … shall encourage … the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation …

Article 42(3) of the GDPR states that the "certification shall be voluntary and available via a process that is transparent". POPIA never adopted the voluntary certification system model, and our Information Regulator is not involved with the certification of seals or marks.

3.3.3 Codes of conduct

It is necessary to acknowledge that codes of conduct which are an important pillar of collaborative governance are intended to be an integral part of POPIA. However, even in this area POPIA changes the emphasis and establishes much more of a command-and-control flavour than the GDPR. Although European regulators and the UK Information Commissioners Office have the capacity to accredit codes of conduct, the codes do not become binding documents in the sector. In other words, data controllers generally choose whether to subscribe to them or not. The implementation of codes of conduct tends to be independent of government.

POPIA provides that codes of conduct can be issued by the South African Information Regulator after an impressively representative and collaborative process that actively involves civil society.[72] Once the code is issued, it becomes "binding on every class or classes of body, industry, profession or vocation referred to" in the code.[73] Failure to comply with the code is then considered to be a breach of the Conditions in Chapter 3 of POPIA.[74]

Under the GDPR, codes of conduct are conceptualised as voluntary codes that protect data controllers.[75] (This approach, which has a particular logic, already works successfully in South Africa in self-regulatory spheres like broadcasting.)[76] The idea under the GDPR is that codes are intended to fulfil a normative role by creating a good data protection culture that facilitates compliance. For example, the UK Information Commissioner's

---

72 Chapter 7 of POPIA.

73 Section 62(2) of POPIA.

74 Section 62(2) read with s 68 of POPIA.

75 See Art 40 of the GDPR. On practical steps for the adoption of a code of conduct in Europe, see for example Kamocki *et al* "CLARIN Data Protection Code of Conduct" 51ff.

76 See BCCSA 2009 https://bccsa.co.za/wp-content/uploads/2015/12/BCCSA_Broadcasting_Code_NEW.pdf.

Office sees a "real benefit to developing" codes of conduct as they can help to "build public trust and confidence" in a sector's "ability to comply with data protection laws".[77] The general understanding of codes of conduct is that they allow for the collaborative regulation of a sector, which should build confidence. Participants in the sector are involved in developing codes of conduct which enhance the chances of compliance.[78] In Europe

> [i]ndustry groups are encouraged to prepare codes of conduct to clarify the application of the GDPR in sector-specific or even technology-specific areas. Codes of conduct act as safe harbors from the GDPR: once a code has been approved by the relevant government authority, a company that follows it can be assured it will not be held liable.[79]

There is a clear logic behind the collaborative approach in the GDPR. The calculation is that "involving the private sector in its own regulation may lead to greater buy-in and adherence to voluntary rules over time".[80]

This is different to the approach in POPIA where, if a code of conduct applies in a sector, that code immediately becomes law for the rest of the sector irrespective of the views of those subject to it. Once made, codes of conduct then become more comparable with subordinate legislation.

3.3.4 Comparing the collaborative governance features of POPIA with those of the GDPR – a synopsis

Apart from the adoption of codes of conduct, which is significant, POPIA never adopted important aspects of the system of collaborative governance modelled in the GDPR. POPIA does not include important documentary requirements for data controllers, including the system of DPIAs. The proposed certification systems that are used in the EU are also not part of POPIA. Hence, POPIA tends to exclude the collaborative governance features of the GDPR.

---

77 Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/.

78 Molnár-Gábor and Korbel advocate a code of conduct for sharing genomic data in Europe and note that "codes of conduct can be written with the help of researchers. Their participation increases the chance that data protection issues will be addressed according to the needs of the relevant sector, that is, genomic and health research. Equally, their involvement can help to increase the code's acceptance: Legally speaking, scientists' participation can strengthen a code's factual legitimacy." (Molnár-Gábor and Korbel 2020 *EMBO Molecular Medicine* 5).

79 Kaminski 2019 *S Cal L Rev* 1600.

80 Kaminski 2019 *S Cal L Rev* 1561.

4 Automated decision-making as a lens into the different regulatory strategies under POPIA and the GDPR

4.1 Individualised remedies for automated decision-making that involves profiling under s 71 of POPIA

There is no definition of automated decision-making in POPIA but Jennifer Cobbe[81] offers the following useful definition in the GDPR context. She uses the term to refer to

> … decision-making by systems which involve algorithmic processes, including machine learning, to automate human decision-making. In popular discussions these are often termed 'AI', and may also be discussed by reference to 'algorithms' or 'algorithmic decision-making'…. Machine learning is the process by which a computer system trains itself to spot patterns and correlations in (usually large) datasets and to infer information and make predictions based on those patterns and correlations without being specifically programmed to do so. This may involve a practice known as 'profiling'; the processing of personal data about an individual in order to evaluate personal characteristics relating to their health, economic situation, performance at work, preferences, behaviours, and so on.[82]

The GDPR and POPIA provide similar remedies that individuals can use to protect themselves from automated decision-making that involves profiling. (Section 71 of POPIA adopts the same structure as Article 22 of the GDPR).[83] On the other hand, as will be seen below, the GDPR and POPIA diverge sharply when it comes to measures that aim to improve the quality of automated decision-making that includes profiling on a systemic level.

Section 71(1) of POPIA provides a general rule that a data subject may not be subject to a decision that is based solely on the automated processing of personal information, which has a substantial effect on or results in legal consequences for that person.[84] This applies in cases where the processing is intended to provide a profile of the person. The profile could include "his

---

81 Cobbe 2019 *Legal Studies* 636-655.

82 Cobbe 2019 *Legal Studies* 637.

83 Article 22 of the GDPR needs to be read with the recitals and the guidelines set out by the Article 29 Data Protection Working Party (AWP29) on Automated Individual Decision-Making and Profiling. The latter is a softer law mechanism operating within the EU: AWP29 2017 https://ec.europa.eu/newsroom/article29/items/612053. See Arts 22(2)(1) and 22(2)(2) of the GDPR; Kaminski 2019 *S Cal L Rev* 1593; ss 71(2)(a), 71(2)(a)(ii), 71(3)(a) and 71(3)(b) of POPIA; AWP29 2017 https://ec.europa.eu/newsroom/article29/items/612053 27.

84 Also see s 5(g) of POPIA. S 60(4)(a)(ii) provides that for a code of conduct to be approved by the Regulator, the code of conduct must "specify appropriate measures for protecting the legitimate interests of data subjects insofar as automated decision making, as referred to in section 71, is concerned".

or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct".[85] Section 71 of POPIA provides that in certain circumstances data subjects are entitled to have automated processing explained to them by the data controller or responsible party. This aims to put them in a position to make representations and contest adverse automated decisions.[86]

Section 71 and Article 22 are not the main focus of this paper, and it is unnecessary to bog this text down in too much technical detail about their operation. Suffice it to say that the provisions do at least allow for some sensible dialogue with the data controller or responsible party. It is, however, fair to say that ultimately remedies of this type are likely to be disappointing. Casey, Farhangi, and Vogl argue that:

> Though transparency may often feel like a robust solution intuitively, explainable artificial intelligence—or 'XAI' as it is increasingly called—is especially unlikely to provide significant remedial utility to individuals in instances where the discrimination involved is only observable at the statistical scale.[87]

Paradoxically, opportunities to provide reasoned explanations may conceal other problems with the automated decision-making process.[88] Most importantly "the reliance on transparency as an individualized mechanism often places excessive burdens on resource-constrained users to seek out information about a system, interpret it, and determine its significance, only then to find out they have little power to change things anyway, being disconnected from power".[89]

If Casey, Farhangi, and Vogl are correct about the relative ineffectiveness of the individualised remedy, then it is fundamentally important that there should be other ways of regulating algorithmic decision-making.

---

85 Section 71(1) of POPIA. The latter part of the provision echoes Recital 71 to the GDPR. AWP29 2017 https://ec.europa.eu/newsroom/article29/items/612053, which gives authoritative guidance as to what the GDPR means by a decision "based solely on automated processing".

86 Section 71(2)(b) of POPIA. Codes of conduct can legitimate the automatic processing although the process of creating and approving codes of conduct is complex. See the development and possible adoption of the Code of Conduct from the Credit Bureau Association at Gen N 209 in GG 44459 of 16 April 2021.

87 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 180-181.

88 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 180-181.

89 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 180-181.

4.2 Systemic management of automated decision making under the GDPR

A potential strength of the GDPR is the way in which it goes beyond individualised remedies when it deals with automated processing that involves profiling.[90] Although the GDPR system is in its infancy, it provides a way of navigating this complex terrain, which has up to now been impervious to regulation.

Under the GDPR, in cases where automated decision making that involves profiling constitutes a high risk to data subjects, the data controller is required to conduct a DPIA.[91] The Article 29 Data Protection Working Party describes a DPIA as

> … a process for building and demonstrating compliance by systematically examining automated processing techniques to determine the measures necessary to manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.[92]

The GDPR allows data controllers a lot of flexibility about the form of their DPIAs. Article 35(7) of the GDPR provides that Data Processing Impact Assessments shall contain at least:

> (a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects… ; and (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

In addition to DPIAs the Article 29 guidelines recommend that companies

> … perform regular quality assurance checks of their systems to make sure that individuals are being treated fairly and not discriminated against …

---

90 "The GDPR comes closest to creating what Frank Pasquale has called 'qualified transparency': a system of targeted revelations of different degrees of depth and scope aimed at different recipients. Transparency in practice is not limited to revelations to the public. It includes putting in place internal company oversight, oversight by regulators, oversight by third parties, and communications to affected individuals. Each of these revelations may be of a different depth or kind; an oversight board might get access to the source code, while an individual instead might get clearly communicated summaries that she can understand." Kaminski 2019 *Berkeley Tech LJ* 210-211.

91 Article 35 of the GDPR (Data Protection Impact Assessments). Also see Arts 35(3)(a) and (c) of the GDPR.

92 Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 172.

> Companies should also perform algorithmic auditing, regularly testing algorithms to ensure they are not producing discriminatory, erroneous or unjustified results.[93]

Most companies that use algorithmic decision-making while processing personal data will have to appoint Data Protection Officers and comply with the documentary requirements under the GDPR.[94] The technical staff in organisations are required to describe and explain their systems when compiling DPIAs.[95] This is inevitably a reflexive process which is likely to conduce to more "informed decision making" by the data controller and may well protect the organisation against the "negative and unintended consequences" of their processing systems.[96] DPIAs can also demonstrate that data controllers have acted with "due diligence", which can potentially protect them from legal liability.[97]

Regulators or supervisory authorities are in a position to assess DPIAs in order to perform their functions.[98] The process of reviewing DPIAs has the potential to assist with rule-setting and the creation of industry-wide standards.[99]

DPIAS also assist in safeguarding "societal concerns".[100] Casey, Farhangi and Vogl argue that "system-wide audits of the type envisioned by DPIAs already have a well-documented track record of detecting and combatting algorithmic discrimination in otherwise opaque systems".[101] If DPIAs are executed in a transparent way then they can assist in building public confidence and show that organisations respect and comply with their legal, ethical and human rights obligations.[102] In cases where it is possible to get

---

93 Kaminski 2019 *S Cal L Rev* 1606.

94 Kaminski 2019 *S Cal L Rev* 1603. For a range of softer law mechanisms set out in recent guidelines, see generally AWP29 2017 https://ec.europa.eu/newsroom/article29/items/612053.

95 Kaminski 2019 *S Cal L Rev* 1603-1604.

96 Kloza *et al* 2017 https://www.prio.org/publications/10579 1-2.

97 Kloza *et al* 2017 https://www.prio.org/publications/10579 1-2.

98 Kloza *et al* 2017 https://www.prio.org/publications/10579 1-2.

99 Kaminski 2019 *S Cal L Rev* 1605.

100 Kloza *et al* 2017 https://www.prio.org/publications/10579 1-2.

101 Casey, Farhangi and Vogl 2019 *Berkeley Tech LJ* 182.

102 Kloza *et al* 2017 https://www.prio.org/publications/10579 1-2. The Working Party Report suggests a number of best practices. For example, it suggests that companies should consider publishing their Data Protection Impact Assessments (DPIAs) or parts of them in order to "help foster trust in the controller's processing operations, and demonstrate accountability and transparency" (Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ* 177).

access to DPIAs, there is potential for NGOs and other actors to mobilise teams with appropriate expertise in order to analyse documentation.

The recent UK Court of Appeals case *R (on the Application of Edward Bridges) v the Chief Constable of South Wales Police* (*Bridges*)[103] provides an example of a DPIA that recently came under scrutiny. (Even though policing is usually beyond the scope of the GDPR, computer systems for policing are specifically regulated under the UK *Data Protection Act* which requires DPIAs.)[104] *Bridges* dealt with the police use of a facial recognition software system on public streets and at public events. Facial recognition systems are notoriously contentious. This is partly because they are unreliable but it is also because of their dystopian potential. In *Bridges* the Court found that the use of facial recognition was unlawful because the DPIA revealed two impermissibly wide areas of discretion for police officers. First, the DPIA did not indicate how people were selected to be on police watch lists before they were pursued by the facial recognition system. Second, it did not indicate the locations in which the facial recognition system could be deployed.[105]

The Court was also concerned about the accuracy of the facial recognition system. The expert evidence indicated that the software had been trained to recognise faces based on a particular dataset that could potentially introduce training bias. (This remained an open question as the experts did not have access to the dataset.) The Court found that the police had not sought to satisfy themselves "either directly or by way of independent verification, that the software program … [did] not have an unacceptable bias on grounds of race or sex".[106] Although the judgment focussed on a specific statutory equality duty, a suitable DPIA would have revealed the same issues.[107]

---

103 *R (on the Application of Edward Bridges) v the Chief Constable of South Wales* Police [2020] EWCA Civ 1058.

104 *Data Protection Act*, 2018.

105 *R (on the Application of Edward Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058 para 152.

106 *R (on the Application of Edward Bridges) v the Chief Constable of South Wales Police* [2020] EWCA Civ 1058 para 199.

107 On what the DPIAs should be designed to do in these circumstances, see Information Commissioner's Office 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf 14. The UK Information Commissioner's Office has advised that a baseline figure for false facial recognition matches needs to be set out in the DPIA. The tolerance for false matches needs to be low. "The grounds for confidence that this baseline can be maintained should be included, as well as a description of steps to reduce it further where

The *Bridges* example illustrates how systemic approaches to data processing can potentially improve compliance and accountability and protect rights.[108] The European regulators are conscious of the need to build an ethical system for managing automated processing.[109] Even with the enormous GDPR fines at their disposal, European regulators will never have the capacity to regulate high-risk automated decision making by using sanctions on an individualised basis. The South African legislature has chosen a command-and-control approach to the regulation of personal data that eschews the internal documentary system that the GDPR has developed in order to foster compliance. More or less in its place, the South African legislature uses multiple pre-approvals which are to be granted on an individual basis by the Information Regulator.

4.3 Comparable provisions in our law - or are they comparable? power to authorise processing by the Regulator using exemptions, authorisations and pre-approvals

While automated processing that involves profiling would tend to amount to high-risk processing under the GDPR and require a DPIA,[110] there is no similar conceptual category under POPIA.[111] Automated processing that involves profiling might fit into one of following three categories under POPIA:

a) The automated processing might involve processing that falls within the parameters of the principles and exceptions within POPIA and be permitted.

b) The automated processing might fall outside the conditions in the Act and require either an exemption or an authorisation from the Regulator.

---

possible" (Information Commissioner's Office 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf 17).

108 On what the DPIAs should be designed to do in these circumstances, see Information Commissioner's Office 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf 17.

109 McDougall 2021 https://ico.org.uk/about-the-ico/media-centre/blog-what-s-next-for-data-ethics/.

110 Also see Art 35(3)(a) of the GDPR, which reads: "A data protection impact assessment … shall in particular be required in the case of: a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person."

111 Section 71(1) of POPIA.

c) The processing may require prior authorisation from the Regulator on the basis that it falls within the parameters of section 57 of POPIA.

The Information Regulator is called upon to provide a range of pre-approvals and exemptions under POPIA. These various legislative provisions form a complex patchwork that is briefly explored in the paragraphs below. The South African Information Regulator is tasked with giving frequent pre-approvals and exemptions, which is not an inevitable function of modern information regulators.

4.3.1 Exemptions and authorisations

If the prospective automated processing of personal information does not fall within the boundaries of POPIA,[112] the Regulator has the power to authorise particular processing in the public interest. These authorisations are called "exemptions" in the Act and the responsible party must apply to the Regulator for authorisation on a case-by-case basis.[113]

There is also a general principle in POPIA that processing special personal data (*inter alia* personal information dealing with race, religion or health) may not take place in the absence of a ground to be found in sections 27 to 33 of POPIA inclusive.[114] If the automatic processing is not covered by those sections then the processing can take place only with the consent of the Regulator.[115] The power to process the personal information of children is prohibited in terms of section 34 of POPIA unless there is a ground to be found in section 35(1) of the Act. In the absence of a section 35(1) ground,

112 Section 4 of POPIA.

113 "The Regulator may, by notice in the Gazette, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case- (a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or (b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing." S 37(1) of POPIA.

114 Specific authorisations concerning a data subject's religious or philosophical beliefs (s 28 of POPIA); race or ethnic origin (s 29); trade union membership (s 30); political persuasion (s 31); health or sex life (s 32); criminal behaviour or biometric information (s 33).

115 According to s 27(2) of POPIA the Regulator may authorise the processing if it is in the public interest and appropriate safeguards have been put in place to protect the personal information. The Regulator may impose reasonable conditions or safeguards for the processing.

it is necessary for the responsible party to apply to the Regulator for consent to the processing.[116]

The Regulator will need to look at requests for exemptions or authorisations on a case-by-case basis and determine if the processing is in the public interest and whether there are sufficient safeguards to protect data subjects.[117]

In contrast, the UK supervisory authority, which is called the UK Information Commissioner's Office, does not routinely conduct onerous pre-approvals on public interest grounds. A list of the public interest grounds for the processing of special personal information is set out in schedule 1 of the UK *Data Protection Act*, 2018, and data controllers are required to make their own assessment of whether or not the processing of special personal information fits within those parameters.[118] In cases of high-risk processing, data controllers are required to conduct DPIAs. Data controllers must consult with the UK supervisory authority about processing where they find that there is difficulty in mitigating the risks to data subjects.

4.3.2 Prior authorisations in terms of sections 57 and 58 of POPIA

There are other categories of processing that responsible parties cannot embark upon without prior authorisation from the South African Information Regulator in terms of section 57 of POPIA.[119] Section 57(1) of POPIA states:

> (1) The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing if that responsible party plans to-
>
> (a) process any unique identifiers of data subjects-

116 Children remain dependent until they are 18 years old under POPIA, which is often unrealistic. This may cause responsible parties to need authorisations from the Regulator in order to deal with older children. According to s 35(2) of POPIA the Regulator may authorise the processing of the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information. The Regulator may impose reasonable conditions in respect of the processing.

117 Section 35(2) of POPIA.

118 There are also indications of the meaning of the term "public interest" in the Irish *Data Protection Act*, 2018 which can be fleshed out by Regulations.

119 The list of categories in s 57(1) of POPIA can be extended by the Regulator to other processing that carries particular risks to the legitimate interests of data subjects (s 57(2)).

(i) for a purpose other than the one for which the identifier was specifically intended at collection; and

(ii) with the aim of linking the information together with information processed by other responsible parties;

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; or

(d) transfer special personal information, as referred to in section 26, or the personal information of children as referred to in section 34, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section 72.

If the processing falls into the categories in section 57(1) and the responsible party does not notify the Regulator then he, she or it is guilty of an offence and liable to a fine and/or imprisonment for a period not exceeding 12 months.[120]

In some cases, automated processing that involves profiling will intersect with the categories in section 57(1).[121] The procedure for receiving pre-

120 Section 107(b) of POPIA

121 First, the boundaries of s 57(1)(c) of POPIA, which requires prior approval when a responsible party wishes to "process information for the purposes of credit reporting", overlap with automated processing that uses profiling. Credit reporting is a very contentious area that affects all citizens. In the EU and the UK, the practices of credit agencies are regulated by legislation (*Credit Rating Agencies (Amendment etc.) (EU Exit) Regulations,* 2019 (SI 2019/266)). In South Africa there is a prospective code of conduct for credit bureaus which is under consideration by the Information Regulator (see Gen N 209 in GG 44459 of 16 April 2021). If this code of conduct is issued, then it will not be necessary for credit agencies to request prior approval for processing (s 57(3) of POPIA). One of the advantages of being in a sector that is subject to a code of conduct is that responsible parties are exempt from having to comply with the sometimes vague pre-authorisation provisions in ss 57 and 58 of POPIA (s 57(3) of POPIA). This will be one of the most powerful incentives for sectors to develop codes of conduct under POPIA. Second, in terms of s 57(1)(a) pre-approval needs to be sought for the processing of any unique identifiers of data subjects "(i) for a purpose other than the one for which the identifier was specifically intended at collection; and (ii) with the aim of linking the information together with information processed by other responsible parties" (ss 57(1)(a)(i) and (ii)). A unique identifier is defined in s 1 of the Act as "any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party". There are two aspects of s 57(1)(a) which narrow what at first glance appears to be an impossibly wide ambit. The easiest to spot is that the ground applies only when unique identifiers are going to be passed on to and processed by another responsible party or other responsible parties. If the responsible party or the

approval from the Regulator under sections 57 and 58 of POPIA is confusing. First, the point of the exercise is that the Regulator must decide in advance whether the processing is lawful. There is no discretion here. Hence it is not clear why the Regulator should be burdened with the role of effectively giving an authoritative legal opinion in each case. Second, the Act prescribes periods within which the Regulator must respond to pre-authorisation requests. If the prescribed time periods in POPIA lapse, then the Act provides that the processing is allowed by default.[122] This situation is completely unsatisfactory as in cases of delay responsibility for the processing appears to shift from the responsible party onto the Regulator.

There is no equivalent process to section 57 of POPIA under the GDPR. The closest provision is the European requirement that data controllers must conduct DPIAs in cases where processing threatens to expose data subjects to high risk.[123] DPIAs must be properly conducted and retained as part of the data controller's accountability responsibility. In cases where the

data controller remains the same, the subsection is not triggered and there is no need for pre-approval. Second, the ground is not triggered if the data were *specifically* intended for the particular processing at collection and that intention was made transparent to the data subject. (Although the word *specifically* does appear intended to narrow the ambit of the provision and widen the Regulator's role.) S 57(1) may include automated processing that involves profiling but only in cases where data is being consolidated from or by various data controllers. Compulsory notification is also necessary when a responsible party intends to "process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties" (s 57(1)(b)). Presumably the press is excluded from this provision. Prior authorisation is also required to transfer special personal information and the data of children to "a third party in a foreign country that does not provide an adequate level of protection for the processing" (s 57(1)(d)).

122 The responsible party must notify the Regulator of the processing. In the interim he, she or it may not process the personal information (s 58(2) of POPIA). The Regulator must decide whether it wishes to do a more detailed investigation and it must inform the responsible party of its intention within four weeks (s 58(3)). If the Regulator does not respond to the responsible party within the four-week period, the responsible party can assume a decision in its favour and continue with the processing (s 58(7)). In the event that the Regulator decides to conduct a more detailed investigation, it must tell the responsible party how long the investigation will take although that period may not take more than thirteen weeks (s 58(4)). After the conclusion of the investigation the Regulator must issue a statement ruling on whether the processing is lawful. If the responsible party does not receive the response within thirteen weeks (or debatably a shorter period if the Regulator committed itself to that shorter period) the responsible party can assume a decision in its favour and continue with the processing (s 58(7)).

123 Article 36(1) of the GDPR. On the meaning of high risk for the purpose of the UK Information Commissioner's Office, see Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/.

risks cannot be adequately mitigated, the data controller must consult with the data protection authority.

The UK Information Commissioner's Office states that where it is consulted about risky processing, it will provide a written response that "will make clear" what may or may not be done.[124] Although the intention is to resolve the situation, there are instances where the authority will issue a warning to the data controller or even "impose a limitation or ban" on the processing.[125] But the general theme is that controllers are required to manage their own processing while protecting the interests of data subjects. This system is largely self-regulatory, although Kaminski writes:

> For high-risk activity, the GDPR's impact assessment process could be characterized as a soft version of premarket approval: requiring a company to be in conversation with the government and to adjust its risk-management process before releasing automated decision-making on the public. Even for non-high-risk impact assessments, the government still plays a role in ensuring accountability because impact assessments are subject to retention and updating requirements and potentially to government disclosure.[126]

When in doubt, many data controllers are likely to err on the side of caution and consult the relevant supervisory authority because of the ethical and reputational risks along with the large fines that are possible under the GDPR.

This paper has demonstrated that the GDPR encapsulates an approach different from that of POPIA. The concept of high-risk processing in the GDPR is imperfect and creates uncertainty for data controllers. On the other hand, it provides some coherence in the sense that processing cannot escape scrutiny because it fits within a legislative loophole. European supervisory authorities are not conceptualised as arbiters of all complex processing on a case-by-case basis. This is a role that the South African legislature appears to contemplate for the Information Regulator and it will be interesting to see how effectively it can be performed.

---

124 Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/.

125 Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/.

126 Kaminski 2019 S Cal L Rev 1605.

5 The Regulator

I have argued that the South African regulator is required to give many exemptions, authorisations and pre-approvals in instances where the UK Information Commissioner's Office relies on data controllers to make decisions about processing in line with principles expressed in the GDPR and the UK *Data Protection Act*. As POPIA comes into operation fully, it is worth noting the challenging task that has been set for the South African Information Regulator.[127]

Erdos has examined the performance of regulators in the EU.[128] He argues that data protection authorities "are generally endowed with very limited resources but are confronted with regulating an almost unfathomable range of personal data processing across political, social and economic life".[129] As a result, regulators often pursue an "increasingly discretionary and selective approach" where a "small sub-set of issues get prioritised" and there is "strong emphasis on 'soft' promotional activities as opposed to 'hard' enforcement action such as administrative injunctions and sanctioning of infractions".[130]

There are other very challenging aspects of an information regulator's work. For example, the UK Information Commissioner's Office's workload has expanded exponentially. In December 2018 it was reported that the office had "received over 8,000 notifications of data breaches since the end of May 2018. That is compared with just 3,311 notifications between 1 April 2017 and 31 March 2018".[131] Viewed in this context, it will be interesting to see how our Regulator manages the varied and onerous demands that have been placed upon it.[132]

The general picture is that supervisory authorities rarely use their enforcement powers in the EU.[133] "High fines under the GDPR have been

127 On 11 June 2021 on the eve of POPIA's coming into force the Information Regulator postponed the date when it would be necessary to apply for pre-approvals under s 57 to 1 February 2022, indicating that it was not ready to receive them. See GN 560 in GG 44761 of 25 June 2021.

128 Erdos 2020 *EDPL* 444.

129 Erdos 2020 *EDPL* 447.

130 Erdos 2020 *EDPL* 446.

131 Graham and Hurst 2019 *IQ: The RIM Quarterly* 20.

132 See how the South African Human Rights Commission did not have the capacity to process information manuals under the *Promotion of Access to Information Act* 2 of 2000 when it was responsible for doing so in Adams and Adeleke 2020 *IDPL* 151.

133 Erdos focusses on the UK Information Commissioner's Office and points out that, according to the 2019-20 Annual Report, the number of complaints was 38 514, a number which almost doubled when compared to the previous year. Only around

few and far between."[134] The French Data Protection Agency (CNIL) fined Google €50 million "for lack of transparency, inadequate information, and lack of valid consent in relation to its use of personal data for the purposes of personalising advertisements".[135] However, that fine is an "outlier".[136] At the same time audits have become "an increasingly important weapon" in the armoury of Data Protection Authorities.[137] Regulators use audits "to assess whether an organisation has effective controls in place alongside fit-for-purpose policies and procedures to support its data protection obligations".[138] Effective auditing is best supported by proper documentary requirements. I have noted that the latter are absent from POPIA.

6 Conclusion

Although POPIA wholeheartedly adopts the command-and-control features of the GDPR, by and large it neglects the collaborative governance mechanisms in the Regulation. In particular, POPIA dilutes the accountability requirements in the GDPR.

Although a deeper analysis of how and why this occurred would require a systematic examination of the drafting history of POPIA, it might be that lawmakers did not want to expose South African firms to expensive new documentation requirements. However, documents that have the potential to provide accountability do not have to be masterpieces. They should simply explain the proposed processing and demonstrate that the responsible party has engaged with risks to data subjects in a meaningful way that considers the conditions and requirements in POPIA. (Cybersecurity is always one of these considerations and the added rigour might be economical in the end.) The elaborateness of the particular documentation should depend on the risks involved. For example, a firm wanting to set up facial recognition in a public area should trigger high levels of scrutiny, elaborate documentation and engagement with the regulator.

40% of cases "were closed on the basis of a finding of no specific need for further action". Fifteen fines were issued and there were only nineteen uses of other formal enforcement powers. Erdos 2020 *EDPL* 449.

134 Graham and Hurst 2019 *IQ: The RIM Quarterly* 23.

135 Graham and Hurst 2019 *IQ: The RIM Quarterly* 23.

136 Graham and Hurst 2019 *IQ: The RIM Quarterly* 23.

137 Graham and Hurst 2019 *IQ: The RIM Quarterly* 24. "[T]he Dutch DPA is particularly keen on exercising its power to audit." There are also an increasing number of audits in Germany.

138 Graham and Hurst 2019 *IQ: The RIM Quarterly* 24.

Responsible parties build awareness of data processing risks and ethics when they document and analyse their processing. This explicitness is valuable. Although Hodges does not refer directly to cyber-regulation, he argues that regulatory systems need to foster an ethical culture and "systems need to be designed to provide evidence on which trust can be based".[139] Better documentation is important for governance and transparency. (This is particularly true in South Africa, where Breckenridge links the weakness of the modern South African state to poor documentation and registration systems.)[140] Better documentation also creates a foundation for more transparency, which is a crucial tool in the global struggle for more responsible data processing.[141]

In the end, successful implementation of POPIA cannot be based squarely on the coercive power of the regulator. The legislative scheme needs to give the Information Regulator a realistic mandate. If the regulator is perceived as being unable to provide quality service, compliance with POPIA will suffer. For these reasons legislators need to reflect about the extensive use of prior approvals in POPIA.

The GDPR and POPIA aim to develop an ethos that protects data subjects while supporting the character of democratic societies that value openness, freedom and equality. These regulatory schemes are part of a global movement which aims to protect the freedoms that people in democratic countries enjoy. The omission of collaborative governance mechanisms from POPIA and accountability tools in particular constitutes a missed opportunity to effectively improve the data protection culture in South Africa. Seen in this way, POPIA needs to be adapted in order to take account of how the objectives in the Act can best be achieved.

---

139 Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 28-29.

140 Breckenridge *Biometric State* 218.

141 This coheres with the suggestion of Black and Murray, who propose transparency reports as a first step in trying to improve the regulation of AI. This is based upon a recommendation from the Communication and Digital Committee of the House of Lords and "recent consultation of the UK information commissioner on guidance on explaining AI based decisions" (Black and Murray 2019 *EJLT*). Also see European Parliament 2022 https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment; Myers 2022 https://www.nytimes.com/2022/04/21/technology/obama-stanford-tech-regulation.html.

Bibliography

Literature

Adams and Adeleke 2020 *IDPL*
Adams R and Adeleke F "Protecting Information Rights in South Africa: The Strategic Oversight Roles of the South African Human Rights Commission and the Information Regulator" 2020 *IDPL* 146-159

Adamson "Importance of Culture in Driving Behaviours of Firms"
Adamson C "The Importance of Culture in Driving Behaviours of Firms and How the FCA Will Assess This" Unpublished contribution delivered at the CFA Society UK *Professionalism Conference* (19 April 2013 Place unknown)

Allan and Currie 2007 *SAJHR*
Allan K and Currie I "Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa" 2007 *SAJHR* 570-586

Bhagwat 1999 *Hastings LJ*
Bhagwat A "Modes of Regulatory Enforcement and the Problem of Administrative Discretion" 1999 *Hastings LJ* 1275-1332

Black 2001 *CLP*
Black J "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" 2001 *CLP* 103-146

Black and Murray 2019 *EJLT*
Black J and Murray A "Regulating AI and Machine Learning: Setting the Regulatory Agenda" 2019 *EJLT* 1-21

Blanc *From Chasing Violations to Managing Risks*
Blanc FOM *From Chasing Violations to Managing Risks: Origins, Challenges and Evolutions in Regulatory Inspections* (Doctoral Dissertation Leiden University 2016)

Bradford *The Brussels Effect*
Bradford A *The Brussels Effect: How the European Union Rules the World* (Oxford University Press New York 2020)

Breckenridge *Biometric State*
Breckenridge K *Biometric State* (Cambridge University Press Cambridge 2014)

Bronstein 2002 *SALJ*
Bronstein V "Drowning in the Hole of the Doughnut: Regulatory Overbreadth, Discretionary Licensing and the Rule of Law" 2002 *SALJ* 471-483

Bronstein and Katzew 2018 *JML*
Bronstein V and Katzew J "Safeguarding the South African Public Broadcaster: Governance, Civil Society and the SABC" 2018 *JML* 244-272

Casey, Farhangi, and Vogl 2019 *Berkeley Tech LJ*
Casey B, Farhangi A and Vogl R "Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise" 2019 *Berkeley Tech LJ* 143-188

Cobbe 2019 *Legal Studies*
Cobbe J "Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making" 2019 *Legal Studies* 636-655

Donovan *Reconceptualising Corporate Compliance*
Donovan A *Reconceptualising Corporate Compliance: Responsibility, Freedom and the Law* (Hart Oxford 2021)

Drahos *Regulatory Theory*
Drahos P *Regulatory Theory: Foundations and Applications* (Australian National University Press Acton 2017)

Dworkin *Law's Empire*
Dworkin R *Law's Empire* (Harvard University Press Cambridge MA 1986)

Edelman and Talesh "To Comply or Not to Comply"
Edelman LB and Talesh SA "To Comply or Not to Comply - That Isn't the Question: How Organizations Construct the Meaning of Compliance" in Parker C and Nielsen VL (eds) *Explaining Compliance: Business Responses to Regulation* (Edward Elgar Cheltenham 2011) 103-122

Erdos 2020 *EDPL*
Erdos D "Ensuring Legal Accountability of the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?" 2020 *EDPL* 444-454

Graham and Hurst 2019 *IQ: The RIM Quarterly*
Graham G and Hurst A "GDPR Enforcement: How are EU Regulators Flexing their Muscles?" 2019 *IQ: The RIM Quarterly* 20-24

Hart *Concept of Law*
Hart HLA *The Concept of Law* (Clarendon Press Oxford 1961)

Kaminski 2019 *Berkeley Tech LJ*
Kaminski M E "The Right to Explanation, Explained" 2019 *Berkeley Tech LJ* 189-218

Kaminski 2019 *S Cal L Rev*
Kaminski M E "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability" 2018 *S Cal L Rev* 1529-1616

Kamocki *et al* "CLARIN Data Protection Code of Conduct"
Kamocki P *et al* "Toward a CLARIN Data Protection Code of Conduct" in CLARIN *Annual Conference Proceedings* (CLARIN Utrecht 2018) 49-52

Molnár-Gábor and Korbel 2020 *EMBO Molecular Medicine*
Molnár-Gábor F and Korbel JO "Genomic Data Sharing in Europe is Stumbling: Could a Code of Conduct Prevent Its Fall?" 2020 *EMBO Molecular Medicine* 1-7

Murphy "Procedural Justice"
Murphy K "Procedural Justice and Its Role in Promoting Voluntary Compliance" in Drahos P *Regulatory Theory: Foundations and Applications* (Australian National University Press Acton 2017) 43-58

Ogus *Regulation*
Ogus AI *Regulation: Legal Form and Economic Theory* (Hart Oxford 1994)

Politou, Alepis and Patsakis 2018 *Journal of Cybersecurity*
Politou E, Alepis E and Patsakis C "Forgetting Personal Data and Revoking Consent Under the GDPR: Challenges and Proposed Solutions" 2018 *Journal of Cybersecurity* 1-20

Roos 2020 *CILSA*
Roos A "The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'" 2020 *CILSA* 1-37

Roos "Data Privacy Law"
Roos A "Data Privacy Law" in Van der Merwe DP *et al* (eds) *Information and Communications Technology Law* (LexisNexis Durban 2016) 363-487

Tyler "Psychology of Self-Regulation"
Tyler TR "The Psychology of Self-Regulation: Normative Motivations for Compliance" in Parker C and Nielsen VL (eds) *Explaining Compliance: Business Responses to Regulation* (Edward Elgar Cheltenham 2011) ch 4

Yeung and Bygrave 2021 *Regulation and Governance*
Yeung K and Bygrave LA "Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship" 2021 *Regulation and Governance* 137-155

Zuboff *Age of Surveillance Capitalism*
Zuboff S *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books London 2019)

Film

Amer and Noujaim *The Great Hack*

Amer K and Noujaim J (directors) *The Great Hack* (The Others 2019)

Case law

R (on the Application of Edward Bridges) v the Chief Constable of South Wales Police [2020] EWCA Civ 1058

Legislation

European Union

European Union General Data Protection Regulation, 2016 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1)

Directive 95/46/EC, 1995 (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data)

South Africa

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

United Kingdom

Credit Rating Agencies (Amendment etc.) (EU Exit) Regulations, 2019 (SI 2019/266)

Data Protection Act, 2018 (Ireland)

Data Protection Act, 2018 (UK)

Government publications

Gen N 209 in GG 44459 of 16 April 2021

GN 560 in GG 44761 of 25 June 2021

International instruments

African Union Convention on Cyber Security and Personal Data Protection (2014)

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981)

Internet sources

AWP29 2017 https://ec.europa.eu/newsroom/article29/items/612053
Article 29 Data Protection Working Party 2017 *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679* https://ec.europa.eu/newsroom/article29/items/612053 accessed 23 July 2022

BCCSA 2009 https://bccsa.co.za/wp-content/uploads/2015/12/BCCSA_Broadcasting_Code_NEW.pdf

Broadcasting Complaints Commission of South Africa 2009 *Free-to-Air Code of Conduct for Broadcasting Services Licensees* https://bccsa.co.za/wp-content/uploads/2015/12/BCCSA_Broadcasting_Code_NEW.pdf accessed 25 April 2022

Constantinescu 2021 https://www.researchgate.net/publication/356612427_AI_moral_externalities_and_soft_regulation
Constantinescu M 2021 *AI, Moral Externalities, and Soft Regulation (Preprint)* https://www.researchgate.net/publication/356612427_AI_moral_externalities_and_soft_regulation accessed 23 April 2022

Data Protection Commission date unknown https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation
Data Protection Commission (Ireland) date unknown *Accountability Obligation* https://www.dataprotection.ie/en/organisations/know-your-obligations/accountability-obligation accessed 29 June 2021

European Commission date unknown https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en
European Commission date unknown *What Rules Apply If My Organisation Transfers Data Outside the EU?* https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en accessed 29 June 2021

European Parliament 2022 https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment
European Parliament 2022 *Press Release: Digital Services Act: Agreement for a Transparent and Safe Online Environment* https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment accessed 25 April 2022

Finck 2017 http://eprints.lse.ac.uk/87568/1/Finck_Digital%20Co-Regulation_Author.pdf
Finck M 2017 *Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy - LSE Law, Society and Economy Working Papers 15/2017* http://eprints.lse.ac.uk/87568/1/Finck_Digital%20Co-Regulation_Author.pdf

Greenwald, MacAskill and Poitras 2013 https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
Greenwald G, MacAskill E and Poitras L 2013 *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations* https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance accessed 30 June 2021

Gunningham and Sinclair date unknown https://www.oecd.org/env/outreach/33947759.pdf
Gunningham N and Sinclair D date unknown *Designing Smart Regulation* https://www.oecd.org/env/outreach/33947759.pdf accessed 23 April 2022

Hao 2020 https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/
Hao K 2020 *We Read the Paper that Forced Timnit Gebru out of Google. Here's What It Says* https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/ accessed 22 July 2022

Hodges 2015 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961
Hodges C 2015 *Corporate Behaviour: Enforcement, Support or Ethical Culture? Oxford Legal Studies Research Paper No. 19/2015* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2599961 accessed 23 July 2022

Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/
Information Commissioner's Office (UK) date unknown *Codes of Conduct* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/ accessed 29 June 2021

Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/
Information Commissioner's Office (UK) date unknown *Do We Need to Consult the ICO?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/do-we-need-to-consult-the-ico/ accessed 29 June 2021

Information Commissioner's Office date unknown https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/
Information Commissioner's Office (UK) date unknown *When Do We Need to Do a DPIA?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/ accessed 29 June 2021

Information Commissioner's Office 2019 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf
Information Commissioner's Office (UK) 2019 *Opinion on the Use of Live Facial Recognition Technology by Law Enforcement in Public Places* https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf accessed 29 June 2022

Information Regulator 2021 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf
Information Regulator (South Africa) 2021 *Guidance Note on Information Officers and Deputy Information Officers* https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-IO-DIO-20210401.pdf accessed 1 August 2022

Kloza *et al* 2017 https://www.prio.org/publications/10579
Kloza D *et al* 2017 *Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework Towards a More Robust Protection of Individuals* https://www.prio.org/publications/10579 accessed 23 July 2022

Meltzer 2020 https://voxeu.org/article/impact-gdpr-data-flows-and-national-security
Meltzer JP 2020 *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security* https://voxeu.org/article/impact-gdpr-data-flows-and-national-security accessed 23 July 2022

McDougall 2021 https://ico.org.uk/about-the-ico/media-centre/blog-what-s-next-for-data-ethics/
McDougall S 2021 *Blog: What's Next for Data Ethics?* https://ico.org.uk/about-the-ico/media-centre/blog-what-s-next-for-data-ethics/ accessed 30 June 2021

Myers 2022 https://www.nytimes.com/2022/04/21/technology/obama-stanford-tech-regulation.html
Myers SL 2022 *Obama Calls for More Regulatory Oversight of Social Media Giants* https://www.nytimes.com/2022/04/21/technology/obama-stanford-tech-regulation.html accessed 2 July 2022

UNCTAD 2020 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
United Nations Conference on Trade and Development 2020 *Data Protection and Privacy Legislation Worldwide* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide accessed 29 June 2021

Vale, Demetzou and Matheson 2022 https://fpf.org/wp-content/uploads/2022/03/FPF_Brussels_Privacy_Symposium-2021.pdf
Vale SB, Demetzou K and Matheson L 2022 *Brussels Privacy Symposium 2021: The Age of AI Regulation: Global Strategic Directions - Symposium Report* https://fpf.org/wp-content/uploads/2022/03/FPF_Brussels_Privacy_Symposium-2021.pdf accessed 23 July 2022

List of abbreviations

AI	artificial intelligence
AWP29	Article 29 Data Protection Working Party
BCCSA	Broadcasting Complaints Commission of South Africa
Berkeley Tech LJ	Berkeley Technology Law Journal
CILSA	Comparative and International Law Journal of Southern Africa
CLP	Current Legal Problems

DPIA	Data Protection Impact Assessment
EJLT	European Journal of Law and Technology
EDPL	European Data Protection Law Review
EU	European Union
GDPR	European Union General Data Protection Regulation, 2016 (Regulation (EU) 2016/679)
Hastings LJ	Hastings Law Journal
IDPL	International Data Privacy Law
JML	Journal of Media Law
ML	machine learning
NGO	non-governmental organisation
POPIA	Protection of Personal Information Act 4 of 2013
S Cal L Rev	Southern California Law Review
SAJHR	South African Journal on Human Rights
SALJ	South African Law Journal
Seton Hall L Rev	Seton Hall Law Review
UNCTAD	United Nations Conference on Trade and Development