AUTHORS:
Lee Swales[1]
Donrich Thaldar[1]
Dusty-Lee Donnelly[1]

AFFILIATION:
[1]School of Law, University of KwaZulu-Natal, Durban, South Africa

CORRESPONDENCE TO:
Donrich Thaldar

EMAIL:
ThaldarD@ukzn.ac.za

HOW TO CITE:
Swales L, Thaldar D, Donnelly D-L. Why research institutions should indemnify researchers against POPIA civil liability. S Afr J Sci. 2022;118(3/4), Art. #13205. https://doi.org/10.17159/sajs.2022/13205

ARTICLE INCLUDES:
☒ Peer review
☐ Supplementary material

KEYWORDS:
Code of Conduct for Research, indemnification, liability, POPIA, responsible party

FUNDING:
US National Institute of Mental Health, US National Institutes of Health (award number U01MH127690)

PUBLISHED:
7 March 2022

Why research institutions should indemnify researchers against POPIA civil liability

Significance:

In the research context, a 'responsible party' as contemplated in terms of POPIA is typically the research institution as well as the individual researcher involved. Given the potential civil liability that individual researchers could face, we suggest that the Code of Conduct for Research should place a duty on research institutions to indemnify their researchers from civil liability. While this measure will limit individual researchers' personal financial risk in the extra-institutional legal sphere, it will in no way shield individual researchers from intra-institutional accountability and disciplinary action. Accordingly, we suggest that this measure strikes a fair balance.

Introduction and background

The research community eagerly awaits the publication of a draft Code of Conduct for Research (the Code) in terms of the *Protection of Personal Information Act* (POPIA).[1] The Code should provide researchers with practical guidance and animate the provisions of POPIA which are largely principles-based. With predominantly principles-based legislation, as opposed to a strictly rules-based approach, there is often room to interpret certain principles – depending on how the various provisions and concepts are phrased. Although a Code cannot re-define concepts (this would be *ultra vires*), it will play a particularly important role in providing guidance on how terms are to be applied and understood, especially in the context of scientific research.

One of the essential foundational definitions in POPIA – as a general concept, and in the context of duties and potential liability – relates to the person that controls and directs the processing of personal information: a 'responsible party'.[1] Accordingly, the purpose of this Commentary is to analyse this concept and outline certain areas in relation thereto that the Code ought to provide clarity and guidance on.

The definition of a 'responsible party'

POPIA, in section 1 thereof, defines 'responsible party' as 'a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information'[1].

Importantly, the definition does not restrict a responsible party to juristic persons (the research institutions under whose auspices the research is being conducted). The words 'any other person'[1] includes any natural person. The definition is certainly wide enough to encompass both an individual researcher, and the research institution as a responsible party. Further, the phrase 'alone or in conjunction with others'[1] indicates that more than one person may be considered a responsible party. In addition, if one considers POPIA's definition of 'operator', which is 'a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party'[1], an employee is specifically excluded from the ambit thereof, while the definition of 'responsible party' makes no such exclusion. An employee is by definition a person who is 'under the direct authority' of an employer. Therefore, an employee cannot be defined as an 'operator', but may well be considered a 'responsible party' if in fact the employee 'determines the purpose of and means for processing personal information'[1] (as per the definition of 'responsible party'). With this being the case, it is clear from the definition of 'responsible party' that multiple persons may, depending on the circumstances, jointly qualify as responsible parties for a single act of processing personal information.

How does one determine who the responsible party will be in each situation? This is a factual question that ought to be determined on a case-by-case basis. In the research context, typically, there will always be at least two responsible parties. Firstly, the research institution, acting through its organs, such as a research unit or an individual researcher, that determines the purpose of and means for processing personal information, and, secondly, a natural person in the form of the researcher who, as an employee of the institution, determines the purpose of and means for processing personal information. While it is conceivable that a researcher who does independent research may be the sole responsible party, researchers are typically employed or contracted by research institutions, in which case the research institution is likely to be the joint responsible party. As a result, research institutions must appoint an information officer, and that person must ensure that the organisation has a policy on how employees should implement the conditions of lawful processing set out in POPIA, and conduct training and monitoring.[2] Researchers employed or contracted by the institution must therefore take decisions on data protection in consultation with their institution's information officer and in compliance with all applicable policies. While employees generally act as an agent only, employees are not exonerated from personal liability in all circumstances. It is well established in South African law that in cases of wrongful breach of a duty of care or criminal misconduct, personal liability may follow. Therefore, we regard it as prudent for individual researchers to regard themselves as potentially joint responsible parties in line with the definition in POPIA, and to act accordingly.

In many instances, particularly in larger organisations, there will be multiple joint responsible parties. In some research projects, it is possible that the principal investigator, as well as the co-investigators or even technicians may determine the purpose of or means for processing personal information, hence making them all responsible parties. Furthermore, in the context of research consortia, all the research institutions may qualify as responsible parties. The decisive consideration is determining, objectively, who decides the purpose of or means for processing

personal information. As pointed out above, there is no hard-and-fast rule here – it is a determination that must be made on a case-by-case basis.

Consequences for a responsible party of non-compliance with POPIA

Whenever there is non-compliance with the provisions of POPIA, data subjects (research participants) will have recourse against the non-complaint responsible party or parties – i.e. the individual researchers and/or research institutions involved. Accordingly, we provide a brief overview of the consequences of non-compliance. We also make recommendations, where appropriate, of what the Code should do to protect individual researchers, who are more vulnerable to lawsuits than research institutions.

POPIA's enforcement mechanisms

In the event of non-compliance with POPIA, data subjects (research participants) can lay a complaint with the Information Regulator. Chapter 10 of POPIA regulates enforcement, and sections 73 and 74 provide that where there has been 'interference with the protection of the personal information of a data subject'[1], the data subject may make a complaint, in writing, in the prescribed manner and form, to the Information Regulator. In terms of section 76, the Regulator is required to conduct a pre-investigation, act as conciliator where appropriate, decide on whether a full investigation is required, and, where necessary, refer the matter to its Enforcement Committee. The Regulator is given wide and expansive powers in Chapter 10 and may summon and enforce the appearance of witnesses, administer oaths, receive evidence, conduct interviews, apply to a judge or magistrate for a search and seizure warrant, and enter and search any premises occupied by a responsible party (where a warrant is granted).

Where a breach of POPIA leads to an investigation and ultimately a referral to the Regulator's Enforcement Committee, section 93 provides that the Enforcement Committee may make any recommendation to the Regulator against the responsible party or an information officer of a responsible party. These recommendations, as set out in section 95, will include an order for the responsible party and/or information officer to take certain steps within a period specified, or to refrain from taking such steps. A responsible party may, in terms of section 97, appeal any decision of the Regulator to a High Court to set aside or vary any order.

Thwarting POPIA's enforcement mechanisms by, for example, obstructing the Regulator, or failing to comply with an enforcement notice, could lead to criminal prosecution and administrative fines. The sanctions are potentially severe, with fines up to ZAR10 million, and prison sentences for a period not exceeding 10 years.

Private remedies for data subjects

The thrust of section 99 is that a data subject, or the Information Regulator on the data subject's behalf, may initiate civil action to claim damages against a responsible party where the responsible party has breached a provision of POPIA (for example, a breach of the conditions for the lawful processing of personal information) or for breach of the provisions of a code of conduct for research approved and issued by the Regulator in terms of section 60. Generally, in South African law, plaintiffs in civil actions for damages caused by wrongful acts (called 'delicts' in South Africa and 'torts' in the USA and UK) must prove that the defendants acted with fault, which is either intent or negligence. However, the new *sui generis* delictual action created by POPIA explicitly excludes the requirement of fault. As such, responsible parties can be held delictually liable by data subjects even if the responsible parties did not act intentionally or negligently. This is referred to as 'no-fault liability' or 'strict liability', and other examples exist in South African law, such as (strict) product liability of a manufacturer under the *Consumer Protection Act*, and the (strict) liability of the owner of a domesticated animal for damage caused by such animal in terms of the ancient Roman *actio de pauperie*. Strict liability clearly benefits plaintiffs in delictual actions, as it significantly lessens their evidentiary burden. In the research context, research participants only need to prove that their personal data were unlawfully processed by one or more researchers (and vicariously by their research institutions) and that they have suffered damages as a result. The mental state (intention or lack thereof) of the researcher or researchers involved is not relevant.

In delictual actions, plaintiffs are entitled to choose their defendant or defendants from a group of potential wrongdoers.[3] To use the language employed by the Durban High Court in *Parekh v Shah Jehan Cinemas (Pty) Ltd,* the plaintiff may 'select his target'.[4] In the research context, this means that research participants whose personal information has been processed unlawfully and who intend to sue in terms of section 99 have the right to select their target from *all the persons who qualify as responsible parties* in terms of POPIA's definition of responsible party (and who fulfil the other criteria of section 99).

The most likely scenario would be that potential plaintiffs would cite the research institution and the researchers involved as defendants. In the alternative, for whatever strategic reason, the plaintiffs may choose to cite only the research institution or only one of the researchers involved – this is an election the plaintiffs are free to make in their own discretion.

While research institutions would have resources to defend themselves against legal action, individual researchers are unlikely to have the resources to do so. Accordingly, we recommend that the Code should place a duty on research institutions to, on condition that the research project has been approved by the research institution's ethics committees, indemnify the researchers in their employ against section 99 claims. This indemnification should be stated in ethics clearance letters. There should also be a procedure provided for in the Code for researchers who are sued in terms of section 99 to notify the relevant research institution and for the research institution to immediately intervene as a further defendant in the action and cover the costs of the legal defence of itself and its employees. In the event that a researcher who is sued in terms of section 99 notifies the research institution, but the research institution fails to intervene, the researcher can force the research institution to become a co-defendant based on the indemnification statement in the ethics clearance letter. This would be accomplished by serving a third-party notice on the research institution in terms of Rule 13 of the Uniform Rules of Court.

To ensure that the indemnification is not misinterpreted by researchers as a free pass to ignore POPIA subsequent to ethics clearance, institutions can require researchers, when filing applications for ethics clearance, to specifically declare that they (a) know the data protection requirements of POPIA and (b) will uphold such requirements. In the event of non-compliance with POPIA by a researcher, the research institution can investigate and take disciplinary action against such researcher. Although such a declaration is important, it should be integrated within the context of a more comprehensive POPIA-compliance awareness and training programme by a research institution. Institutions should ensure that their researchers know how to fully comply with POPIA, and that although the institution would shield them from personal financial risk in the extra-institutional legal sphere – the indemnification that we propose – this would in no way shield individual researchers from intra-institutional accountability and disciplinary action.

Joint liability?

As we set out above, it is possible that in any given research situation, there may be *more than one* responsible party. How does POPIA deal with this? In simple terms, it does not. It may be interpreted as meaning that where there are multiple responsible parties[5]:

> *they are jointly and severally liable for any processing which is carried out jointly (that is to say, where both the purposes and means of processing are shared), but are individually liable for any processing which is carried out separately for their own purposes, and by their own means.*

Joint and several liability, which applies to delictual wrongdoers under the common law, entails that each party can be held liable for the whole

of the damages. This is wider than 'joint' liability where multiple parties are each only liable for a proportionate share of a joint debt.[6]

However, where there is partial overlap of either the purposes or means of processing, the position is less clear. In its ordinary meaning, the phrase 'in conjunction with' used in the definition of responsible party refers to 'the situation in which events or conditions combine or happen together'[7]. It thus includes, but is somewhat wider than, the adjective 'joint' or 'jointly', which means 'belonging to or shared between two or more people'[8]. Thus again, each case would have to be dealt with on its own facts, but the point of departure in our view is that it is only where parties did act jointly in the latter sense that there can be joint and several liability. This accords with the view expressed by the Court of Justice of the European Union in two cases (albeit decided in the context of online services rather than research) that responsibility as joint controllers does not imply 'equal' responsibility.[9] The level of responsibility would be determined in accordance with the individual circumstances of each case.[9,10]

It is worth noting that POPIA's definition of 'responsible party' is drawn from Article 2(d) of the Data Protection Directive[11], which is in all material respects identical to Article 4(7) of the General Data Protection Regulation[12] (GDPR) (although the European data protection regime uses the term 'controller' rather than 'responsible party', the definitions are similar and the principles the same). One caveat in this regard: although there are striking similarities between POPIA and the GDPR, Article 26 of the GDPR makes specific provision for joint responsibility, enjoining parties to 'determine their respective responsibilities for compliance'[12]. POPIA does not have a similar provision, and it is hoped that the Code will suggest – on a similar basis to Article 26 – that responsible parties make suitable arrangements and make same available to the data subject. However, it should be noted that even if joint-responsible parties conclude an agreement regarding their respective responsibilities for compliance with POPIA, this will not be binding on the data subject, who can still select their target in the event of section 99 civil liability litigation – joint-responsible parties may well have indemnity provisions between themselves in the underlying agreement, but these are not binding on the data subject, who will still in theory have a choice of whom to litigate against.

Conclusion

The Code should clarify, using practical examples, who qualifies as a 'responsible party'. That said, POPIA does not provide that codes of conduct can limit the rights of data subjects in any way. In light of our analysis of plaintiffs' right to select their target in delictual actions from the entire pool of wrongdoers, it means that the Code cannot define 'responsible party' narrower than in POPIA itself. Stated differently, the Code cannot prescribe to data subjects who to sue and who not to sue. This is the prerogative of the data subjects. What the Code can and should do, is to arrange for research institutions to indemnify individual researchers. Furthermore, to ensure that researchers who work in consortia do not just assume that somebody else will take responsibility for POPIA compliance, the Code should provide guidance regarding suitable POPIA compliance arrangements between research consortium partners.

Acknowledgements

We acknowledge the support by the US National Institute of Mental Health and the US National Institutes of Health (award number U01MH127690). The content of this article is solely our responsibility and does not necessarily represent the official views of the US National Institute of Mental Health or the US National Institutes of Health. We thank Michaela Steytler for her assistance with the technical formatting. All errors are the authors alone.

Competing interests

We have no competing interests to declare.

References

1. Protection of Personal Information Act 4 of 2013, South Africa.
2. Information Regulator. Guidance note on Information Officers and Deputy Information Officers, 1 April 2021, South Africa.
3. Myeni v Organisation Undoing Tax Abuse NPC (15996/2017) [2019] ZAGPPHC 565. Available from: http://www.saflii.org/za/cases/ZAGPPHC/2019/565.html#_ftnref32
4. Parekh v Shah Jehan Cinemas (Pty) Ltd 1982 (3) SA 618 (D) at 622E.
5. Donnelly D. Privacy by (re)design: A comparative study of the protection of personal information in the mobile applications ecosystem under United States, European Union and South African law [thesis]. Durban: University of KwaZulu-Natal; 2020.
6. De Pass v The Colonial Govt (1886) 4 SC 283 at 390 per De Villiers CJ.
7. Cambridge English Dictionary [online]. Cambridge: Cambridge University Press; 2021. Conjunction [cited 2020 Mar 30]. Available from: https://dictionary.cambridge.org/dictionary/english/conjunction
8. Cambridge English Dictionary [online]. Cambridge: Cambridge University Press; 2021. Joint [cited 2020 Mar 30]. Available from: https://dictionary.cambridge.org/dictionary/english/joint
9. Wirtschaftsakademie Schleswig-Holstein (C-210/16) ECLI:EU:C:2018:388 para 43.
10. Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17) ECLI:EU:C:2019:629 para 75–76.
11. Data Protection Directive 95/46/EC, European Union.
12. General Data Protection Regulation (EU) 2016/679, European Union.