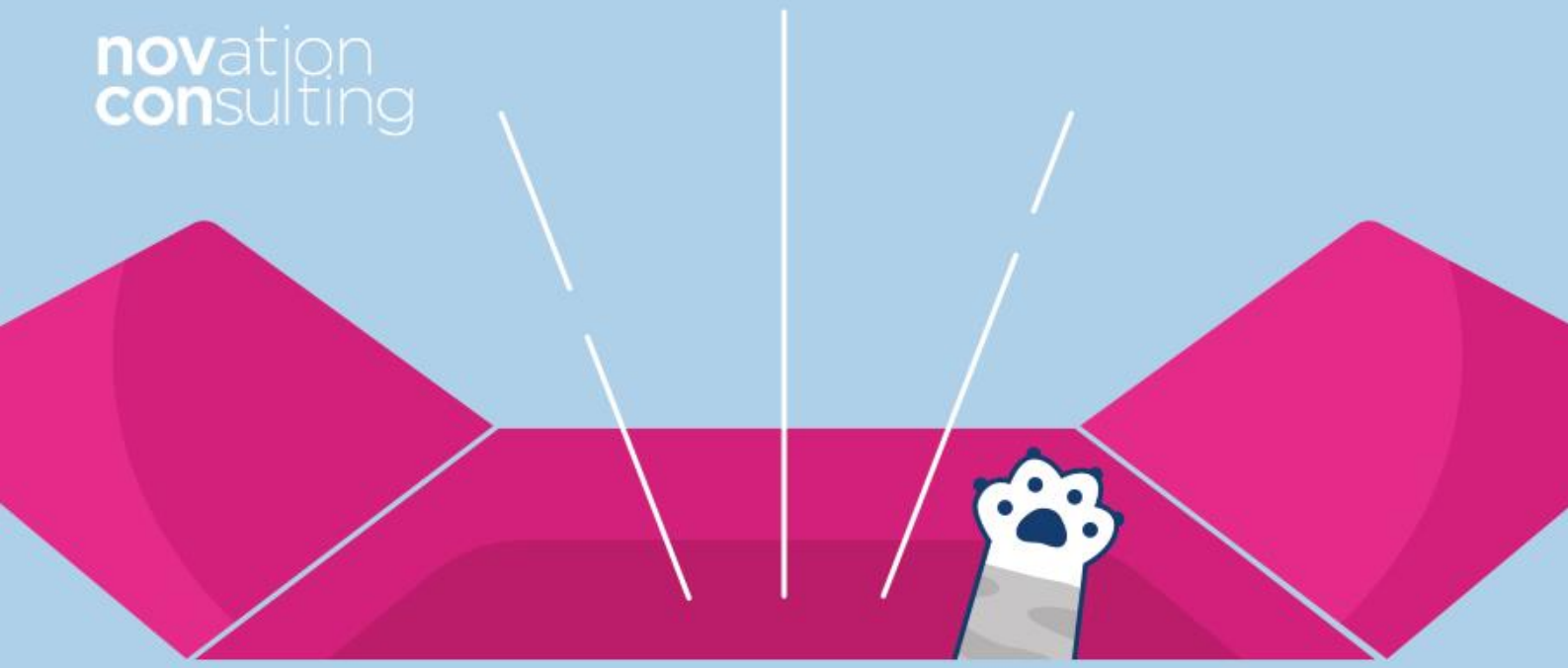
novation consulting



A GUIDE TO THE PROTECTION OF PERSONAL INFORMATION ACT

(for advertisers)

3 March 2022

Our aim with this article is to:

- introduce the Protection of Personal Information Act (POPIA) and unlock some of its key terminology;
- share our approach to navigating the differences and similarities between POPIA and the EU GDPR; and
- correct some of the most common misunderstandings about POPIA.

Remember, context is king, so always ask for legal advice on your specific activities.

1. ANOTHER DAY, ANOTHER PRIVACY REGULATION

With the recent explosion in privacy regulations around the world, South Africa could not afford to be left behind. Luckily,[1] on 1 July 2021, POPIA, came into force.

Curiosity killed the cat: Did you know that POPIA is new, but also really old? The first draft of the Act appeared back in 2009 and was based on privacy regulations like the European Union's Data Protection Directive and New Zealand's 1993 Privacy Act. Both have since been updated. The Directive has been replaced by POPIA's more famous, but younger sibling, the European Union's General Data Protection Regulation (EU GDPR). New Zealand's Privacy Act got a facelift in 2020. Why are we telling you this? Nothing about POPIA is new, you just need to know where to look.[2] But mostly, so we can joke about being copycats[3].

While POPIA protects the constitutional right to privacy that all South Africans already have,[4] its purpose is not to protect privacy at all costs. It is to balance the right to privacy with the right of organisations to market and sell their products and services.[5]

---

[1] Yes, we said luckily. If South Africa does not keep up with data protection regulation, we will miss out on the global information economy and the fourth industrial revolution, because organisations in other countries would not trust South African organisations with personal information.

[2] **For the lawyers:** You can find out all about the birth of POPIA in the South African Law Reform Commission Project 124 on Privacy and Data Protection that is comprised of a 2005 Discussion Paper (available at https://www.justice.gov.za/salrc/dpapers/dp109.pdf) and their 2009 Report (available at https://www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf).

[3] If you're wondering why all the cat references, check out our white paper: Lifting the Lid on POPIA.

[4] **For the lawyers:** Section 14 of the Constitution contains the right to privacy. The preamble to POPIA states that 'the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information'.

[5] **For the lawyers:** Section 44(1)*(b)* of POPIA provides that the Information Regulator must take the interests of public and private bodies in achieving their objectives in an efficient way into account when enforcing POPIA.

What does POPIA protect us from? People often think that data protection and privacy is just about data breaches, identity theft and fraud, but it's also about:

- not secretly watching people and gathering information behind their backs;
- respecting people's anonymity;
- giving people control over what their personal information is used for;
- not discriminating against certain categories of people when making decisions about them, such as who to market to; and
- respecting people's right not to be disturbed.

An interesting read: In his *Taxonomy of Privacy* Dan Solove talks about different privacy problems. **Here** is an adaptation of his work.

How does POPIA prevent privacy problems from happening?

POPIA has rules about…	**What you do with information**
What information advertisers may **collect or create**	You **collect or create** information when you: • learn about consumers by monitoring and tracking their behaviour online and offline; • infer things about who consumers are and their preferences from their behaviour; • share and combine information about consumers from different sources; and • ask consumers about themselves.
What advertisers may **use** this information for	You typically **use** information to: • identify potential consumers; • display targeted advertising about products and services to consumers; • make suggestions to consumers; • make decisions about consumers like whether they qualify for a product or service or whether to send them marketing; • contact consumers for direct marketing; • sell products and services to consumers; and • improve websites, products, and services.

Whether an advertiser may **keep** information	You want to keep information about consumers: • for historical, research or statistical purposes (e.g., to determine what your return on investment was on previous marketing campaigns); • to prove that you complied with POPIA (and other laws); and • to market to consumers some more (i.e., remarketing).
Whether advertisers may **reuse** information	You reuse information to reconnect with consumers who previously interacted with you.
During all these activities, POPIA requires **transparency** and that you respect the new rights POPIA gives consumers (called **data subjects' rights**) to have a say in what advertisers do with their personal information.	

2. WHEN DOES POPIA APPLY?

POPIA applies when an organisation (1) processes (2) personal information (3) in South Africa. Sounds simple? When a law(yer) is involved, it's never simple.[6]

All three activities must be true for POPIA to apply, so we'll unpack each of these important concepts, namely, processing, personal information, and when it is done in South Africa.

2.1. What is processing?

Processing covers all activities that involve personal information – from collection to destruction. When you collect, use, disseminate (transmit, distribute or make available), merge, link, restrict, degrade, erase or destroy personal information, you are processing it.[7] There is hardly a verb, or an activity left on the board.

2.2. What is personal information?

What advertisers are asking:

Q: What is personal information?

[6] **For the lawyers:** Sit with that for a moment.

[7] **For the lawyers:** Processing is defined in section 1 of POPIA.

A: Personal information is all information that can be linked to an identifiable living individual or existing organisation.

Here are some examples of 'personal information':[8]

- email addresses
- mailing addresses
- phone numbers
- precise locations
- full names or usernames
- likes, dislikes, preferences and opinions
- browsing and shopping history
- inferences about a consumer's life or health

Curiosity killed the cat: Did you know that South Africa is one of the only countries in the world that also protects the personal information of organisations? Yup, as far as we know it's just us, Columbia and Laos.

So, when is personal information not personal information? If the person or organisation cannot be identified. This brings us to online identifiers like IP addresses, cookie identifiers, radio frequency identification (RFID) tags, tracking pixels, device fingerprints, MAC addresses, advertising IDs, and account handles. Cookies are used to collect these types of personal information, but is this information really *personal*?

POPIA will only apply if you collect:

- enough personal information to identify the consumer;
- information that can be linked by a reasonably foreseeable method to other information that identifies the consumer; or
- information that can be used or manipulated by a reasonably foreseeable … aw &^%$@!, say what now?

The bottom line is if you know who these identifiers belong to or if there is a legal way for you to find out, then this information is personal and POPIA applies (even before you take the step to find out who the consumer is).[9]

---

[8] These are not air quotes; the term is defined in POPIA in section 1.

[9] **For the lawyers:** See the definition of 'personal information' along with the definition of 'de-identification' in POPIA. This will leave you with the question 'What does identifiable and "reasonably foreseeable method" mean?' Don't reinvent the wheel, the EU GDPR has a very similar definition for personal data and de-identification. Go and read recitals 26 and 30 of the GDPR. Then go and read the 2016 judgment of the European Court of Justice in *Patrick Breyer v Germany*, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=en&mode. Lastly, go and read the Article 29 Data Protection Working Paper *Opinion 05/2014 on Anonymisation Techniques*, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

2.3. When is personal information processed in South Africa?

Personal information doesn't exactly respect borders. It travels around the world in a flash and at a very low cost. So, regulating data protection country by country is like herding cats. But here we are … still using geography to determine which data protection law applies.

POPIA applies to all South African organisations. Not sure if your organisation is South African (it happens)? A shortcut is to ask whether you pay tax here.[10] Whether the consumer is a citizen of South Africa or located in South Africa does not matter. In other words, POPIA also protects foreigners when their personal information is processed by a South African organisation.

Curiosity killed the cat: Did you know that POPIA also applies to foreign organisations? Yup, if the foreign organisation processes personal information in South Africa. A foreign organisation processes personal information in South Africa if it uses equipment or a service provider in South Africa to process personal information. For instance, if a website that deploys cookies is hosted and managed in South Africa, or if an advertiser has employees in South Africa who process consumer information.

3. HOW DOES POPIA COMPARE TO EU GDPR?

What advertisers are asking:

Q: Can we just use cookie banners and cookie notices that European companies use?

A: Yes and no. When European organisations or organisations that target consumers who are in Europe, use cookies they are subject to the EU GDPR and the ePrivacy Directive. POPIA copied parts of the EU GDPR and the ePrivacy Directive, but not all of it, so POPIA is actually less strict when it comes to cookies. If an organisation uses an EU law compliant cookie notice and cookie banner, they will have done more than POPIA requires. So, if over-complying is your thing, go for it.

---

[10] **For the lawyers:** When POPIA applies is determined by section 3(1). Organisations who are domiciled in South Africa, must comply. We use the definition of tax residency in section 1 of the Income Tax Act 25 of 2002 to determine when this is the case. Section 3(1)*(b)* determines when POPIA will apply to a foreign organisation. They must use 'automated' or 'non-automated' means in South Africa. 'Automated means' is defined as 'any equipment'. However, POPIA will not apply if the means is only used to 'forward personal information through' South Africa. For more information on how this clause should be interpreted, read Article 29 of the Data Protection Working Party's *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp56_en.pdf.

There are four scenarios:

- **where POPIA is silent or more lenient than the EU laws**, for instance, POPIA does not contain any specific provisions on the use of cookies and other tracking technologies, whereas the ePrivacy Directive does;
- **where POPIA is virtually identical to the EU laws,** for instance, where POPIA copied the ePrivacy Directive verbatim for us to safely rely on the lessons learnt in Europe, such as with direct marketing;
- **where the concept is the same, but the wording is different,** for instance, on profiling and automated decisions, POPIA is very similar to the EU laws, but there are wording differences (this is the hardest one); and
- **where POPIA introduces a principle that is not in the EU laws,** for instance, POPIA introduces the principle that personal information must be collected directly from the data subject, unless certain exemptions apply.

Our approach is to carefully compare POPIA to the EU approach, but to pay attention to the differences.

What advertisers are asking:

Q: If we are EU GDPR compliant are we also POPIA compliant?

A: As far as cookie banners and cookie notices are concerned, yes, because in addition to the GDPR, European organisations must comply with the ePrivacy Directive. If you're a South African advertiser and you comply with the GDPR and ePrivacy Directive, you will have done more than you need to for POPIA purposes.[11]

4. WHAT IF THE INFORMATION REGULATOR DOES NOT AGREE?

POPIA has never been tested, which begs the question, 'What if the Information Regulator does not agree?' Let's test this with a scenario – one of many (very) educated guesses you'll find in this document:

Spoiler alert: We don't think a South African advertiser needs consent to do targeted advertising. We think they can choose between asking for consent or allowing consumers to opt out.

If we get it wrong, and you're left non-compliant, here's what could happen:

- The Regulator will warn you that they will investigate an alleged infringement.

[11] **For the lawyers:** This statement is true for cookie banners and notices, but there are some very important differences between POPIA and the EU GDPR. Sometimes POPIA is stricter than the EU GDPR. For instance, POPIA also protects the personal information of organisations.

- Once the Regulator completed their investigation, they will issue an enforcement notice in which they could tell you to start asking for consent to do targeted advertising.
- If you do not agree with their finding, you can challenge the enforcement notice in court.
- You will only get fined or imprisoned if you ignore an enforcement notice.

But you know what they say: a cat in gloves catches no mice. So, we think it makes sense to wait until the Information Regulator tells us that consent is required, before switching from the opt-out (legitimate interest) approach. However, it is also perfectly fine if you want to play it safe and get opt-in consent for targeted advertising.

Curiosity killed the cat: Did you know that the belief that a cat has nine lives goes back to ancient Egypt, when killing a cat was punishable by death? Egypt got its first standalone data protection law in 2020. #justsayin'.

5. WHAT PERSONAL INFORMATION IS ADVERTISERS ALLOWED TO COLLECT OR CREATE?

Curiosity killed the cat: Did you know that POPIA allows for the collection of personal information from a variety of sources?[12]

There have been rumours that POPIA bans so-called 'data mining', third-party cookies and other methods of collecting information about a data subject from third parties. This is not true.

These are common examples of instances when advertisers can collect information about consumers from other sources:

- Advertisers are allowed to collect personal information that the consumer has deliberately made public (e.g., published themselves, on the internet).
- Advertisers can argue that obtaining personal information from a third party (e.g., through third-party cookies) is in the (legitimate) interest of their organisation. When this is the case, collection can continue, but the consumers must be made aware of the collection and they must be given the right to object against it. Think of the right to object as opting out – if the

[12] **For the lawyers:** We are talking about section 12, which creates the default rule that personal information must be collected from the data subject directly. What? But that would be the end of third-party cookies! Don't panic, section 12(2) contains a long list of exceptions. The ones we have listed are most used in the context of marketing. Section 12 is one of the handful of sections that did not come from the EU GDPR, and why you will not easily find a lot of discussion about it. Instead, it comes from the 1993 New Zealand Privacy Act.

consumer says nothing, you can carry on collecting their personal information.

- Advertisers could get the consumer's consent to collect their personal information from another source. To be valid, the consent must be a voluntary, informed, specific expression of will. This means the consumer must give opt-in consent – if the consumer says nothing, you cannot collect their personal information from the third party.

Ask your lawyer whether the organisation should ask for consent to collect personal information from a third party, or whether you can rely on legitimate interest (and the right to object). To answer the question, the lawyer should do a legitimate interest assessment. We talk about those here.

6. WHAT ARE ADVERTISERS ALLOWED TO USE PERSONAL INFORMATION FOR?

Curiosity killed the cat: Did you know that POPIA does not always require consent to collect and use personal information? One of the hardiest myths about POPIA is that you must have consent to do anything with personal information. Nothing could be further from the truth. POPIA is about balancing the right to privacy with the right of organisations to market and sell their products and services.[13] One of the ways in which POPIA balances these rights is to recognise that consent is often not practical and will prevent organisations from going about their business.

There are six different legal justifications for processing ordinary personal information. Here they are along with some notes on the context in which they might (or might not) apply.

When can an advertiser use personal information?	**How this *might* apply to you**, but to be sure, ask your lawyer.
When it is in the legitimate interest of the advertiser or a third party	This is the justification we would use for most marketing and advertising activities. It is in your legitimate interest to: • identify consumers who may be interested in your products through profiling based on third-party information;

[13] **For the lawyers:** Section 44(1)*(b)* of POPIA provides that the Information Regulator must take the interests of public and private bodies in achieving their objectives in an efficient way into account, when enforcing POPIA.

	• serve consumers advertising (targeted or behavioural advertising); and • measure the effectiveness and return on investment of your campaigns and websites. **For the lawyers:** Do you always need opt-in consent for marketing cookies? Not in South Africa. This means that most of the time, we can rely on the advertiser's legitimate interest if the data subject is well-informed (cookie notice) and given the opportunity to object (opt-out). You also do not need consent for targeted or behavioural advertising, because it is not considered 'electronic communication'. POPIA requires consent for 'unsolicited direct marketing by means of electronic communications'. Targeted and behavioural advertising is not considered 'electronic communications' because the message is not stored in the network or in the data subject's terminal equipment until it is retrieved.[14] For non-electronic communications, advertisers can rely on legitimate interest, if the data subject is well-informed (cookie notice) and given the opportunity to object (opt-out).
When the advertiser contracts with the consumer	You can collect information you need to enter into a contract. This applies once a lead has indicated that they are interested by ordering or starting to complete an application form. It also means that you can screen leads to determine whether they qualify for your product (e.g., qualifying for a loan).
When the advertiser meets contractual obligations	You can collect and use personal information to meet contractual obligations. For example,

[14] POPIA defines 'electronic communications' as any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

	when a data subject provides a physical address to an e-commerce platform for the delivery of their order the e-commerce platform does not need consent to deliver it; they need the delivery address to meet their contractual obligations.
When the advertiser complies with the law	You can collect and use personal information to comply with the law. For example, FICA requires that some advertisers monitor for money laundering. To do a FICA search of a client is allowed in terms of POPIA.
If it is in the legitimate interest of the consumer	You can collect and use personal information if it is in the legitimate interest of the consumer, such as in emergencies and 'once-off' processing activities. (It's not really relevant here, but we thought we would mention it nonetheless.)
If the advertiser is a public body, performing a public law duty	You can collect and use personal information if you are a public body performing a public law duty, for example, governments often use this to justify screening people for social benefits if they want to distribute information about social benefits or other forms of government assistance. So, it might be relevant if you are in the public sector.
If the advertiser has consent	If none of the other legal justifications apply, you may need consent. For marketing activities, it will often come down to choosing between consent and legitimate interest, which is what we discuss next. You might also need consent if you are reusing personal information for a completely new purpose. We discuss this in CAN ADVERTISERS REUSE PERSONAL INFORMATION?

6.1. How to choose between consent and legitimate interest

When you use personal information for marketing, the legal justification will either be your legitimate interest or consent. So how do you choose which one to apply?

It's better for business to rely on legitimate interest rather than consent because you can continue with the processing activity until the consumer objects (opts out).

6.2. Do a legitimate interest assessment

So, when can you rely on 'legitimate interest'? If your interest in efficiently achieving your objective (i.e., sell stuff) outweighs the infringement of the consumer's privacy. Another test is to ask whether the consumer would expect that their personal information will be processed. Sound complicated? That's because it is.

Ask your lawyer: Ask your lawyers to do a legitimate interest assessment. To rely on your legitimate interest depends on what personal information you collect, who the information is shared with and what that personal information is going to be used for. The UK Information Commissioner's Office produced a helpful guideline for responsible parties to perform a legitimate interest assessment.

Here is an example of a legitimate interest assessment of targeted advertising that was published by CIPL (a global privacy and data policy think tank), adapted ever so slightly for South Africa.[15]

Targeted advertising that is clearly part of the services provided	
Legitimate interests of the responsible party, third parties or the consumer	**Consumers' rights, freedoms and reasonable expectations**
Organisations have legitimate interests in providing targeted advertising when it underpins their business model and where it is clearly part of services provided. Consumers may have a legitimate interest in receiving targeted advertising when they believe they benefit from discovering new products and services and that receiving advertising was clearly part of the services requested.	Consumers expect to see targeted advertising where they use services that are offered in a way where targeted advertising is clearly part of the offering.

[15] **For the lawyers:** You will find commentary stating that legitimate interest cannot be used as a legal basis (e.g., the European Data Protection Board in their Guidelines 8/2020 on the targeting of social media users, paragraphs 71 and 72). Be careful, because their opinion is informed by the fact that this form of tracking is also governed by the ePrivacy Directive, which requires consent. South Africa does not have the equivalent of the ePrivacy Directive, so the legal position is a bit more relaxed.

Mitigating measures:

- Making it easy for consumers to object.
- Providing enhanced transparency such as just-in-time notices when the consumer sees the advertisement.
- Ensuring that the targeted advertising is not discriminatory.
- Providing detailed and meaningful controls to consumers concerning advertisements and the use of their personal information.

Curiosity killed the cat: Did you know that POPIA does not require an opt-in consent for targeted advertising? POPIA only requires consent for unsolicited, electronic direct marketing (e.g., email, SMS, sending DMs or robocalls). Targeted advertising is not electronic direct marketing, even though it is targeted. The reason for that is a bit technical, but it means that the advertiser can rely on their legitimate interest if the consumer is given the opportunity to object. [16]

6.3. If you fail the legitimate interest assessment, then it's consent

When legitimate interest is not appropriate, you will have to rely on consent.

To be valid, consent must be:

Voluntary	It must be a genuine choice. The consumer must be able to say no and still continue with the activity (e.g., to purchase a product or browse a website) without being penalised. The consent should also not be bundled with terms and conditions – the consumer must have the freedom to withhold consent, but still accept the terms and conditions. In other words, no 'fit in or fork-off' consents. Consumers must be free to withdraw consent without effort and without any detrimental effects such as an increase in cost, unavailability of services or a decrease in service levels.
Specific	The consent must always relate to a specific, well-articulated purpose. A blanket consent covering all purposes for which

[16] **For the lawyers:** POPIA defines 'electronic communications' as any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient. This means that personalised (targeted and behavioural) advertising is not considered 'electronic communications' because the message is not stored in the network or in the data subject's terminal equipment until it is retrieved. Telemarketing is not electronic direct marketing for the same reason.

	personal information is processed will be too vague to be valid. Instead, the consent must be detailed.
Informed	The consent must be worded in such a way that the consumer can make an informed decision. This means that the consumer must understand the facts of the situation and the implications of giving or withholding consent. According to the European Data Protection Board a consent is valid if the following information is provided: • the identity of all the responsible parties who will rely on the consent; • the purpose of each processing operation for which consent is asked; • the type of personal information that will be collected and used; • that the consumer can withdraw consent; and • whether the information will be used for automated decision-making. Advertisers must take the target audience (also referred to as a market segment) into account when writing consents. For instance, if the audience has lower levels of literacy, responsible parties must use simpler language.
Expression of will	The consent must be explicit, which means that it must be given by means of a clear, unambiguous, affirmative act. It cannot be given by default and silence. Inactivity cannot be taken as consent. To avoid ambiguity, the action of giving consent must also be distinct from other actions, such as agreeing to terms and conditions.[17] So, if you are relying on consent, it must be an opt in. If the consumer does nothing, there must be no processing of personal information.

This is a tall order. Which is why we recommend that you only rely on consent when you absolutely have to.

[17] **An interesting read:** So much has been written about valid consents. The European Data Protection Board's *Guidelines 05/2020 on consent under Regulation 2016/679* 18, is just one example and is available at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf TL;DR? Here is a blog on the C-word.

7. CAN ADVERTISERS KEEP PERSONAL INFORMATION?

What advertisers are asking:

Q: For how long can we keep personal information?

A: The short answer? You can keep personal information for as long as you need it.

You may keep personal information[18] if:

- a law requires that you keep the personal information;

Curiosity killed the cat: Did you know that you must keep personal information to show that you complied with POPIA? We discuss consumer requests later but answering them requires a meticulous record of what personal information you collected, how, from where, and what you used it for.

- you need the personal information for your functions or activities;
- you retain the personal information for historical, statistical or research purposes (e.g., conducting campaign analytics or research);
- a contract requires that you keep the personal information;
- the data subject gave consent (the c-word again) that their personal information may be retained for a longer period; or
- if you used the personal information to make a decision about the data subject (e.g., personalising advertising based on a profile of a consumer) *and* that decision will have a substantial impact on the consumer, the consumer has the right to make representations. In this case you must keep the information long enough to afford the consumer a reasonable chance to request access to the information. We discuss this some more under RESPECTING DATA SUBJECT RIGHTS. Not to worry, we don't think that personalising advertising has a substantial impact.

Ask your lawyer: Does your organisation have a records retention schedule for marketing-related information? A records retention schedule is a document that sets out what kind of information you must keep and for how long. Each organisation should have one to comply with POPIA.[19]

8. CAN ADVERTISERS REUSE PERSONAL INFORMATION?

8.1. What is reusing personal information (or 'further processing')?

Further processing happens when a responsible party uses personal information for a purpose that is different from the purpose for which the information was originally

[18] **For the lawyers:** What personal information can be retained is determined by section 14 of POPIA.

[19] Specifically, section 14.

intended. Shifting purposes may introduce new privacy risks, and so POPIA places restrictions on the reuse of personal information.

When can you reuse information? Here are some of the justifications most often used for marketing-related processing: [20]

- If the personal information is available in or derived from a public record.
- If the data subject deliberately made the personal information public.
- If the personal information is being (re)used for historical, statistical or research purposes and it will not be published in an identifiable form.
- If the purpose for which the personal information will be (re)used is still compatible with the original purpose for which the personal information was being used.
- If you have the consumer's consent.

An easy test? Ask yourself whether the consumer would be surprised to learn that you are using their personal information in this way. And 'If they come to know about it, would they be upset?' If you answer yes to either of these questions, tread lightly.

What advertisers are asking:

Q: Does POPIA allow for 'remarketing'?

A: The question is really whether you need consumers' consent to do remarketing. Remarketing happens when advertisers serve ads to consumers who have visited their website, or a specific web page. It is an effective way of targeting consumers who have already shown some interest in your product or brand. If the personal information used in the remarketing was originally collected for that purpose, then you are not further processing. Then, as we previously discussed, you should ask your lawyer to perform a legitimate interest assessment to determine whether you need consent.

Here are some activities for which you may need consent:

- When you merge personally identifiable information with information previously collected as non-personally identifiable information.
- When you link information a service provider collected with offline personal information that you collected for another purpose (e.g., sales data).

[20] **For the lawyers:** Further processing is regulated by section 15 of POPIA. Section 15(2) gives guidelines on how to determine if the purpose for which an organisation is (re)using the personal information is compatible with the original purpose. Section 15(3) lists some instances where it will automatically be compatible. An organisation must comply with section 15(2) *or* section 15(3), not both. In the EU GDPR 'further processing' is regulated under their purpose limitation section. The Article 29 Working Party wrote an Opinion on Purpose Limitation which is useful, but tread carefully, because the wording is quite different to that of POPIA.

Ask your lawyer: If you want to merge or link personal information that was previously collected for another purpose, you should ask your lawyer to consider whether you need consent.

8.2. When advertisers may need prior authorisation

For some processing activities the responsible party must first apply for authorisation from the Information Regulator because the processing activities are considered to infringe on data subjects' privacy. POPIA lists the activities that you'll need authorisation for, such as processing consumers' unique identifiers to link to information held by other responsible parties, where the linking activity constitutes further processing that is incompatible with the original purpose for which the unique identifier was collected or created. [21]

What are unique identifiers? According to the Information Regulator, unique identifiers include 'bank account numbers or any account number, policy number, identity number, employee number, student number, telephone or cell phone number, or reference number'.[22] We expect that client IDs, user IDs and other tags also fall within the definition of a unique identifier.[23]

If you use client and user identifiers to merge or link your own dataset with a service provider's dataset to do something that differs from the original purpose for collection, then the processing activity might be seen as further processing. In that case, you may have to apply for prior authorisation from the Information Regulator.

However, if you have the opt-in consent of the consumer to merge or link the datasets, you might not need prior authorisation.[24]

Ask your lawyer: You should ask your lawyers whether prior authorisation is required in terms of section 57(1)*(a)* when you link personal information in your possession with someone else's information.

---

[21] Section 57(1)(*a*).

[22] **Interesting read:** See the Information Regulator's *Guidance note on applications for prior authorisation*, available at https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PriorAuthorisation-20210311.pdf.

[23] **For the lawyers:** POPIA defines a unique identifier 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.

[24] **For the lawyers:** Section 57(1)*(a)* applies if the linking activity is not the purpose 'for which the identifier was intended at collection'. We interpret that to mean that the linking must be 'further processing' in terms of section 15. Section 15(3)*(a)* states that if the data subject gave their consent, the processing is automatically compatible.

9. POPIA REQUIRES TRANSPARENCY

Transparency is the cornerstone of data protection. Consumers cannot exercise their rights if they don't know what personal information is being collected about them and how it is used. We discuss these rights in the next section.

Here, the rule of thumb is that consumers should not be surprised to learn what their personal information is used for.

Curiosity killed the cat: Did you know that researchers at Carnegie Mellon found that it would take the average internet user 76 working days to read the privacy notices they encounter on the internet in a year. That is about 304 cat days.[25]

POPIA requires that advertisers must notify consumers of, amongst others:[26]

- the personal information being collected;
- the sources from which the information is collected if it is not collected directly from the consumer;
- the purpose for which the information is collected;
- whether or not the supply of the information is mandatory or voluntary (i.e., can the consumer opt out?);
- the consequences of failure to provide the information;
- whether the responsible party intends to transfer the information to a foreign country or international organisation, and the level of protection afforded to the information by that country or international organisation; and
- the consumer's right to object to the processing when the advertiser is relying on legitimate interest as a legal justification.

The notification cannot be hidden behind an obscure URL in the farthest corners of the website. You must take 'reasonably practicable steps' to bring the information to the attention of the consumer.

What advertisers are asking:

Q: Do we need a cookie banner and notice?

A: The short answer is yes. It doesn't matter whether you call it a cookie notice, a website privacy policy, a privacy notice, a cat, a dog, or a bus, consumers must be made aware of the use of cookies to collect personal information. The cookie

---

[25] **For the lawyers:** We over-simplified this and we know how much you hate that. Here is a useful article about cat years: https://www.pumpkin.care/blog/cat-age-chart/.

[26] **For the lawyers:** POPIA's transparency requirements are in section 18.

banner is how you bring the cookie notice to the attention of the consumer. What should be in the cookie notice? We discuss that in our white paper 'Lifting the Lid on POPIA: Answering your AdTech and MarTech questions'.

10. ADVERTISERS MUST RESPECT DATA SUBJECT RIGHTS

10.1. Consumers have more privacy rights now

A cat may look at a king![27] Data subject rights are POPIA's way of giving consumers control over what their personal information is used for.

POPIA gives consumers the right to:

- access their information (e.g., consumers can ask if you have their personal information, what you know about them, and which third parties have access to their personal information);[28]
- correct or delete their information (e.g., correct or update incorrect personal information or delete personal information that is no longer relevant);[29]
- object to having their personal information processed (e.g., a consumer can object to the processing of their personal information if you are processing their personal information for your own legitimate interests);[30]

For the lawyers: A consumer has the right to object to the processing of their personal information if you use legitimate interest as your legal basis for serving them targeted advertising or tracking them through third-party cookies.

- withdraw consent previously given;[31]

For the lawyers: A consumer may withdraw consent if you rely on consent as your legal basis for serving them targeted advertising or tracking them through third-party cookies.

- complain to the Information Regulator; and

[27] **For the grammar nerd:** Even a person of low status or importance has rights.

[28] **For the lawyers:** Check out section 23 of POPIA.

[29] **For the lawyers:** Check out section 24 of POPIA.

[30] **For the lawyers:** Section 5(*d*) of POPIA read with section 11(3)(*a*) of POPIA.

[31] **For the lawyers:** Regulation 3 and Form 2 of the Regulations Relating to the Protection of Personal Information, No. R. 1383, 14 December 2018. The Information Regulator has published draft updates to the regulations that are available here: https://www.inforegulator.org.za/legal/20211012-InfoRegSA-InvtieToComment-RegulationsAmendment.pdf.

- not be subject to a decision based solely on automated processing of their personal information profiles.[32]

Not respecting consumer's rights is one of the easiest ways to get into trouble under POPIA. Think about it. A consumer who are trying to exercise their rights is already like a cat on a hot tin roof. Ignoring them will guarantee a complaint!

The easiest way to avoid a caterwauling is by:

- informing consumers in a user-friendly way about their rights and how to exercise them (see how the Information Regulator did this in their privacy notice);[33] and
- having an internal procedure to deal with consumer requests in an acceptable and timeous way (i.e., a data subject request procedure).

Ask your lawyer: Ask your lawyer for advice on developing and implementing an internal data subject request procedure.

For the lawyers: What is a reasonable time period within which to respond to a data subject request? Because PAIA also covers data subject access requests, you should consider the timelines provided by PAIA. The default period in PAIA is 30 days.[34] If an information officer misses the deadlines referred to in PAIA, it is seen as a refusal of the request.[35]

What about other data subject rights? It is probably not a good idea to adopt 30 days as the standard for what is reasonable. Responsible parties should test their data subject requests procedures and define a standard for different types of requests.

10.2. A special word on making automated decisions

Using automated processing (e.g., an algorithm) to make important decisions about consumers is dangerous. In some instances, it is outright forbidden, while in others,

---

[32] **For the lawyers**: Section 71 of POPIA.

[33] We are kidding, *whispers* it is not particularly user-friendly. **Interesting read:** We quite like Jurro's privacy notice and cookie notice. And it is opensource. Fernando is our favourite privacy fish. When looking around for inspiration, just be sure you're comparing cookies with cookies!

[34] **For the lawyers:** See section 25 (in respect of public bodies) and section 56 (in respect of private bodies) of PAIA. There are exceptions to the default rule or instances when it can be extended.

[35] **For the lawyers:** See sections 27 and 58 of PAIA.

POPIA imposes additional rules, like giving the data subject an opportunity to make representations about any decision that was taken about them.[36]

Automated processing (like personalising advertising based on a consumer's profile) is only 'automated decision-making' if it has a substantial impact on the consumer. This might be the case where you use profiling to make automated decisions that:

- have a prolonged or permanent impact;
- affect the behaviour and choices of data subjects;
- lead to discrimination or exclusion of individuals;
- affect their financial circumstances (e.g., their eligibility for credit);
- affect their access to health care;
- deny someone an employment opportunity or put them at a serious disadvantage; and
- affect their access to education (e.g., university admission).

And there you have it. If you have any questions, you know where to find us. May the odds be ever in your favour.

11. ABOUT NOVATION CONSULTING

We're a unique interdisciplinary gang of rehabilitated lawyers, change managers, design thinkers, information designers, risk managers, chaos pilots and troublemakers. We combine our powers to design legal, compliance and risk management solutions that make sense. We turn compliance on its head, shake the nonsense out of its pockets and present it in a fresh and exciting way.

Here is what we spend most of our time on:

- We create **customer terms & conditions** that people actually want to read. In the process, we make sure that organisations treat their customers fairly.
- We help organisations to manage their **commercial contracts** and to build relationships that are based on trust and understanding (and a little bit of tenderness). We create awesome templates, negotiation and drafting playbooks with a light sprinkling of appropriate tech.

[36] **For the lawyers:** Automated decision-making is regulated by section 71 of POPIA. Much of what we have to say about it comes from the Article 29 Data Protection Working Group *Guidelines on Automated individual decision-making and Profiling*. Available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

- We ♥ **policies**. Done well they can increase efficiency, improve teamwork, establish culture and protect everybody. What's the point of shelling out vast amounts of money on a set of policies, procedures or guidelines only to have them gather dust in a drawer somewhere? If it's not read, it's dead, we say.
- We do legal, risk and compliance interventions. Are you wondering why people hate legal, compliance and risk management? We can help diagnose the problem and fix it. We refer to this as our **#complianoscopy service**. It's a thing.
- **Information governance and data protection** is our passion. It involves many things we love, like improving processes, getting the most out of your data and big, hairy change management problems. From getting buy-in, to policy development and kick-ass training. We do it all.

Connect with @Novcon on LinkedIn, or check out www.novcon.co.za.