everlytic

novation consulting

2020 POPIA Guide

How to Comply Without Killing Your List

Introduction

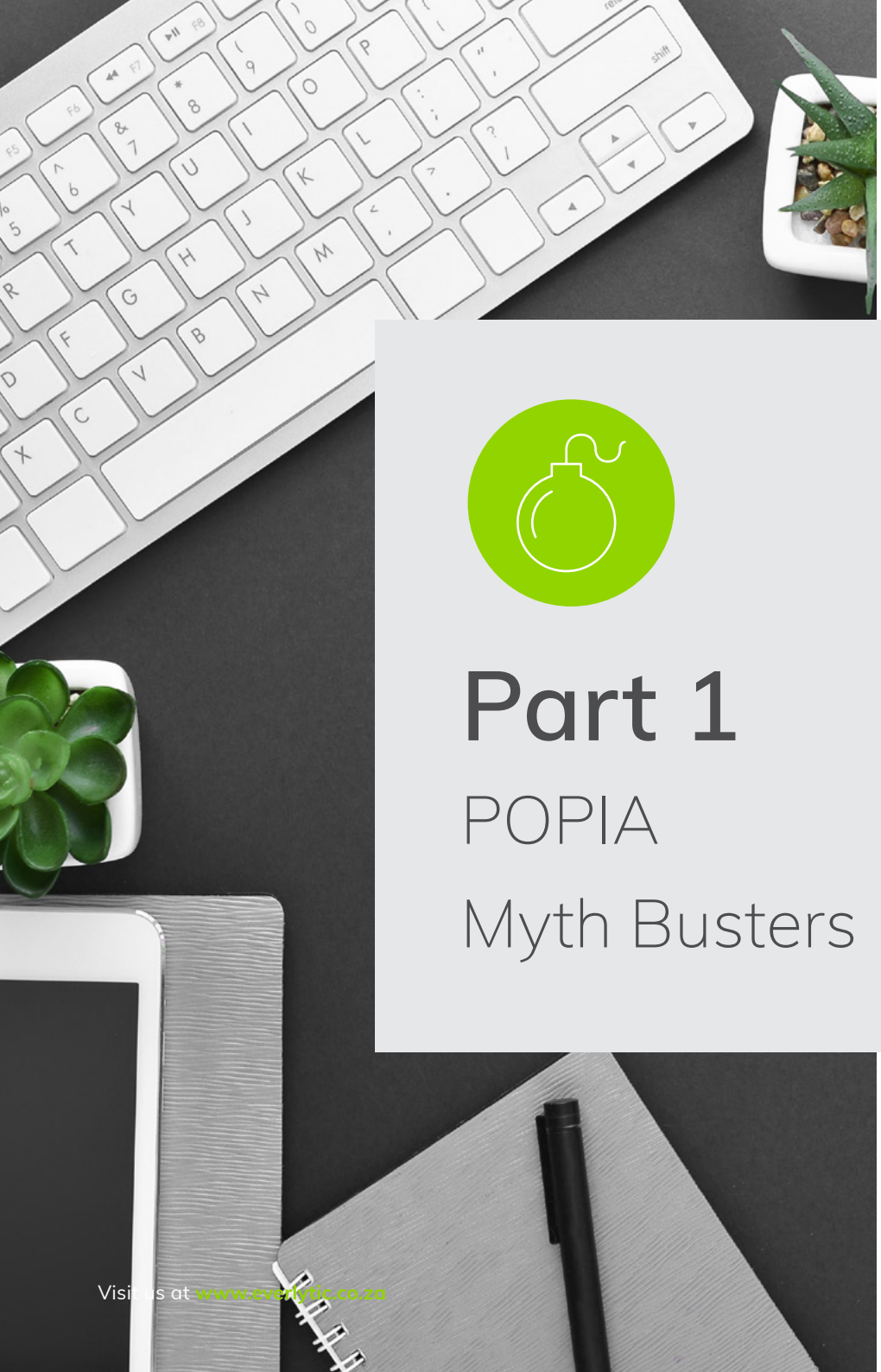
Welcome to the 2020 POPIA Guide: How to Comply Without Killing Your List. This simple, practical document summarises the content shared in **our three-part webinar** series hosted by Everlytic and POPIA expert, **Elizabeth de Stadler** from **Novation Consulting**.

In it, you'll learn what POPIA really says about direct marketing, what it doesn't say, and what you can do about it now – without killing your database. Importantly, this guide also explores why POPIA can even be an opportunity for your business in this changing landscape.

Disclaimer:

Context is king when applying POPIA. While this guide was created in partnership with an attorney, it is a poor substitute for formal legal advice. Why? Because POPIA is principles-based legislation and there are a lot of variables that could influence what is best for your business. Please remember this when reading this guide.

Contents



Part 1

POPIA Myth Busters

POPIA **isn't** What You Think it is

> ***"I don't think our death ray is working. I'm standing right in it and I'm not dead yet."***
>
> **- Jamie Hyneman, from the TV show Mythbusters**

The way people perceive POPIA is often like this – like it's a threat to all direct marketing. It isn't. Yes, it will affect some forms of marketing, but for the most part, it changes *how* we do things, not the fact that we *can*.

Simply put? POPI isn't the death ray – it won't kill your marketing. In fact, there are a lot of positive trends that have come out of similar legislation overseas. Embrace the change and you may be able to capitalise on it.

What POPIA **Doesn't Say**

- ✖ POPIA will stop spam and kill marketing
- ✖ POPIA doesn't apply to telemarketing
- ✖ You need opt-in consent before you do telemarketing
- ✖ Just put consent in your Ts & Cs and you're good to go

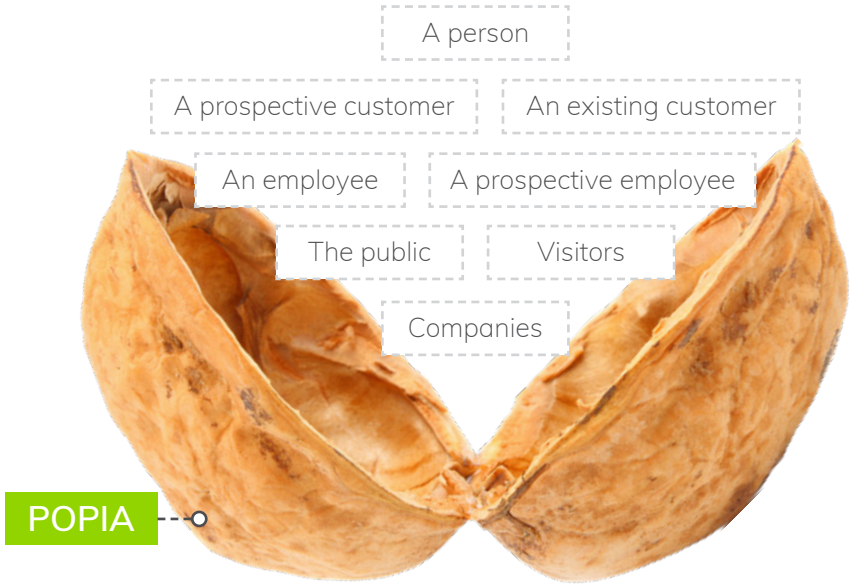
POPIA in a Nutshell

People underestimate the scope of POPIA. It doesn't just apply to direct marketing.

Why?

Because POPIA applies to any personal information you have on an identifiable individual or organisation.

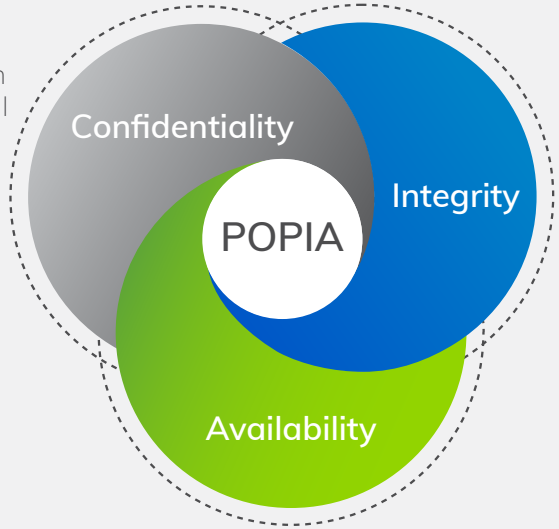
This can include:



The CIA Triad

POPIA also doesn't just apply to marketing activities. For instance, you have to make sure that any personal information you have is secure. Information security, is basically about three things:

Keep the information confidential



Make sure the information you have is accurate. E.g.: How sure are you that those cell-phone numbers and email addresses are correct? A lot of breaches happen because of integrity.

Protect information from loss, keep it accessible for the people in your organisation who use it, and ensure you don't accidentally destroy it.

Information security is not the only thing to worry about. POPIA has implications for every step in the information life cycle – from what information you collect and how you collect it, to how long you can keep it and how to get rid of it.

Direct Marketing & Promotions

What is **Direct Marketing?**

Direct marketing is any form of direct message that contains promotional information. This includes uploading a list of contacts to target on social media.

It does not include targeting unknown contacts on social media who meet a certain demographic, as you don't have their personal information.

What is a **Promotional Message?**

A promotional message is anything that directly or indirectly promotes a brand, even if it's just to raise awareness of that brand. It can promote a product or service directly or indirectly, like with inbound marketing where you create valuable content (newsletters, blog posts, guides like this, etc.) with the goal of converting a contact further down the line.

Tip: If your organisation can be identified and the content is being sent to identifiable individuals, the regulator will probably view it as direct marketing.

What POPIA Says About Marketing & Promotions

POPIA asks these questions:

1 **Where** did you get the information you're using?

You must get the information directly from the person to which it relates. You can also get it from a public record that's administrated by a public body. The internet is not a public record.

Buying and selling leads will still be legal, but in most cases you will need consent from the prospect for the sale to be legal. More about this in Part 2.

2 What **channel/s** are you using?

Electronic direct marketing (everything except telemarketing) requires consent before you send marketing.

Telemarketing: You can do it without consent, but if they opt out, you must listen.

3 Is this a **new prospect** or an **existing client**?

a. Did they contact you first?

   (e.g. they signed up for the newsletter, or you've sold similar products to them before via the same supplier)

b. Did you tell them that you'd be using their contact details for marketing?

c. Did you give them the opportunity to unsubscribe?

d. Do you unsubscribe them when they asked to be?

Wondering if you **need to reconsent your database?** Check out Part 2 of this guide.

What POPIA Says About Marketing & Promotions (cont.)

4 Say you **do need consent**. POPIA has very strict requirements you must meet for that consent to be valid.

Consent must be:

a. **Specific about the products and services** you're marketing

b. **Specific about the channels** you're using to send the marketing (email, SMS, social media, etc.)

c. **An opt-in request**. They must make an explicit, clear, and distinct request to receive your marketing communication (like via a form with a checkbox) before you can contact them. Do you unsubscribe them when they ask?

d. **Voluntary and separate from your services.** The fact that you're going to market to them can't be hidden in your Ts & Cs or be a requirement for use of your products and services.

See page 11 for more on this.

5 What happens if they **unsubscribe**?

You must have a good unsubscribe process – you're most likely to run into complaints if people can't unsubscribe.

6 How must I **manage** the information that I have?

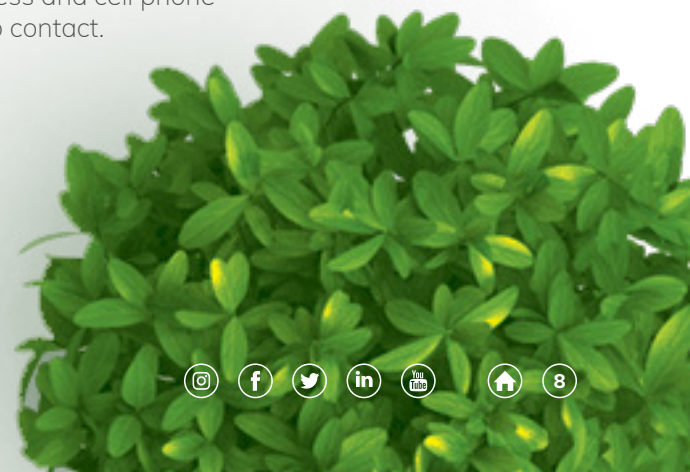
a. Manage all the information on your prospects in one place, so you can ensure it's always current and accurate.

b. Actively manage the information that you have in your database in real-time by automatically unsubscribing people who opt out and subscribing those who opt in.

If you manage your database properly, you're probably getting rid of most of the POPIA risks.

7 Can a person demand that I **delete** their information?

They can ask, but you'll have to keep some of their information (the information that's most relevant to their subscription, like their email address and cell phone number), so you know who *not* to contact.



Part 2

Building Your Mailing List

In this part of the guide you will learn:

- **What you can do** with your existing mailing list
- **What the rules are** regarding buying (or selling) leads
- **How to sign people up** for direct marketing
- How to **manage unsubscribes**

Leads & Where You Can Get Them

First-Party Leads

This is the best way to collect data – by getting people to connect with you authentically. Aka: inbound marketing.

Harvesting the Internet

You should, wherever possible, get information directly from the person – unless that person made the information deliberately public. But even if you get that information from a public place, like a person's website, you still have to contact them to explain where you got their information and ask for their consent before using it.

Buying Leads

You can still 'buy' leads. But the lead must have given their explicit permission for their data to be shared or sold to specific parties. So, the question is: can you trust the party selling the leads? If you're uncertain, you're going to need to contact the leads to confirm.

Selling Leads

Are the contacts aware that you have their information? Have they given you their explicit permission to sell it? If not, and you have their data, an option is to contact the person, let them know that you have their information, and give them a chance to opt out. However, until POPI is being actively enforced, it's an educated guess and may still carry risk.

Using Someone Else's Data

Some companies market to similar audiences, but this doesn't mean they can market to the same database. When requesting data, the requesting company will need to get explicit and specific third-party consent, listing the additional company by name (it can't be generic to apply to any company or department). Only if this is done can you share the database.

Cross-Selling

Some companies sell a variety of products; some of which are not in the same industry. Some clothing stores, for instance, may sell life insurance or credit.

In cases like these, your consent will only be valid for 'similar' products or services or if all of the products or services were listed. Clothing and life insurance, for example, are too far removed to be considered sensibly linked. Offering credit to buy clothes, like many clothing stores do, may have a link, but you'll need to be cautious.

Rule of thumb: The contact should not be surprised to be receiving marketing for this product or service from you.

Consent: When, How, What & Where

When **Do** You Need Consent?

- ✔ When the person doesn't know you or your business.
- ✔ When they know of you, but you didn't tell them you'd use their info for marketing.
- ✔ You got their information from someone else. For this, you may need two consents. The first is just to have the information, and the second is to market to them.
- ✔ You're selling something else now – something completely new or very different to the products you've marketed to that individual before.

When **Don't** You Need Consent?

When you can check all these boxes:

- You got their information in the context of a sale of a product or service – they know you, **and**
- You told them you were going to use their information for marketing of similar products / services, **and**
- You told them, when you collected their details and every time that you contacted them, that they could opt out of your marketing.

Many businesses haven't kept adequate records of where they got their data from.
This is a problem and may lead to you needing to reconsent your database to be 100% certain that you're compliant.

You May Not Need to Reconsent Your Database

Remember the rule of thumb:
Is this person going to be surprised to hear from me?

It's not always necessary to reconsent your database. Nowhere in the POPIA legislation does it say that you must reconsent your database. Additionally, some lawyers may not understand the impact reconsenting can have on your business unless you break it down for them.

For instance:

Reconsenting your database means that many people may not see or open your reconsent request, so many of your contacts will be lost – many against their will. This can lead to a drop in revenue and clients who are disgruntled for no longer receiving your messages.

When ***May*** You Need to Reconsent Your Database?

If the answer to any of the following questions is no, you may need to reconsent your database:

- Do you know where you got the personal information in your database?
- Do you have a record of exactly what they signed up for (the actual wording)?
- Have you ever contacted them for marketing before?
- Do you have a reliable unsubscribe process?
- Did you collect the information recently?

Smart Options if You Have to Reconsent

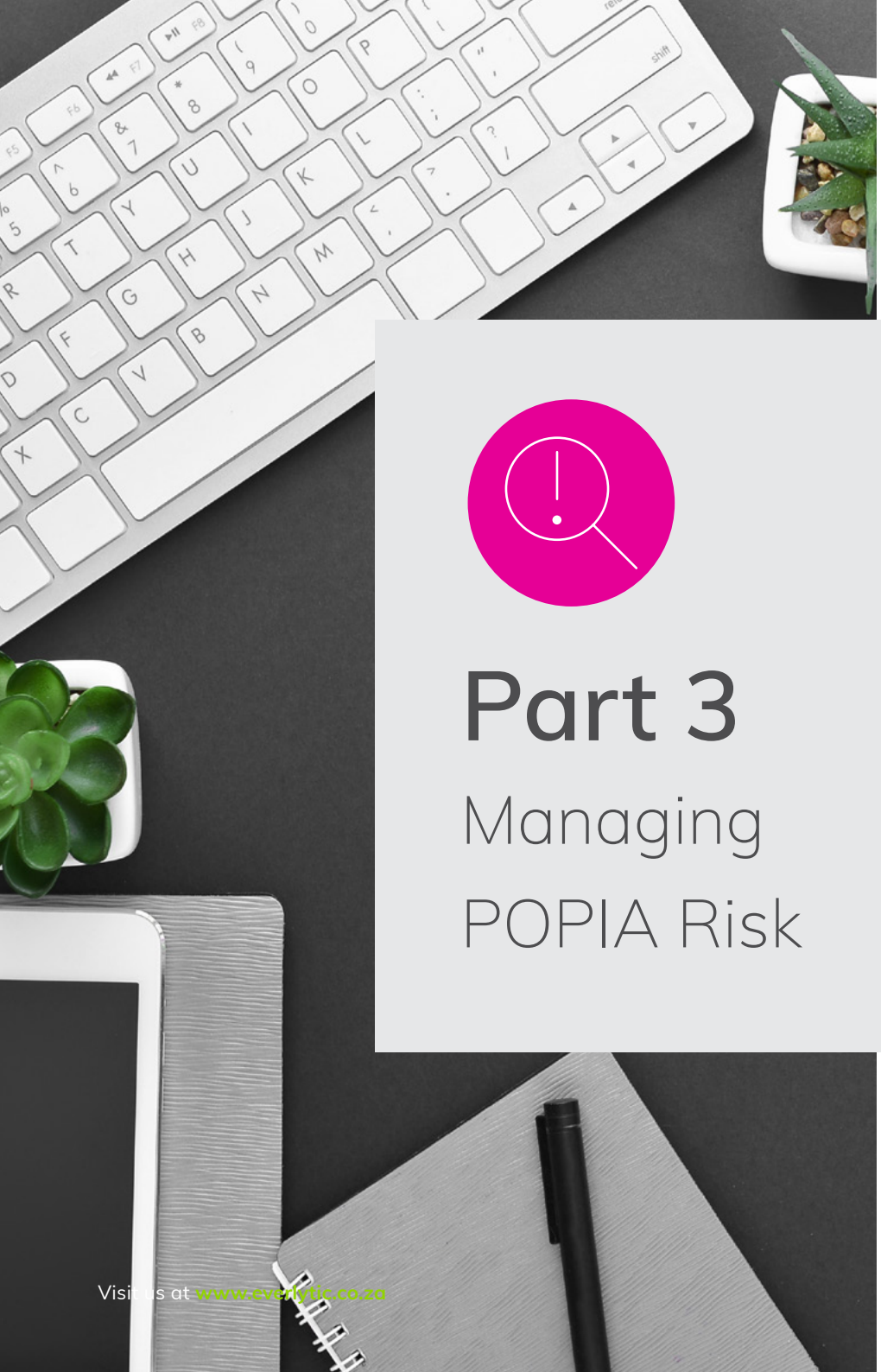
If you must reconsent your database, here are some smart, risk-based options to consider trying to lessen the business impact and improve compliance in the future:

- ✔ **Reconsent your database but use an opt-out.**
  i.e.: Not "Let us know if you want to receive our newsletter" – rather: "Let us know if you don't want to receive our newsletter."

> **Note:** This is not strictly compliant, so can carry risk. However, it may be less of a risk than not reconsenting at all. Knowing the ROI on your list may help you determine your appetite for risk.

- ✔ **Use friendly & open POPIA messaging.**
  Explain how you're protecting their data, why you're reconsenting, etc.
- ✔ **Dress up reconsent as an opportunity to update details – or opt out.**
  This puts the focus on updating their data – not opting out. Plus, it improves your data.
- ✔ **Incentivise staying or subscribing.**
- ✔ **Make unsubscribing fool proof.**
- ✔ **Manage complaints and enquiries like a boss – and plan for it.**

... All these things manage the risk of someone going to the Regulator.



Part 3

Managing POPIA Risk

In this part of the guide you will learn:

- **The 10 things** you can do now to improve your compliance
- Who the **'Privacy Actives'** are and why targeting them is beneficial for your business
- **Who to contact** for POPIA guidance and data-management technology

10 Things You Can Do Now

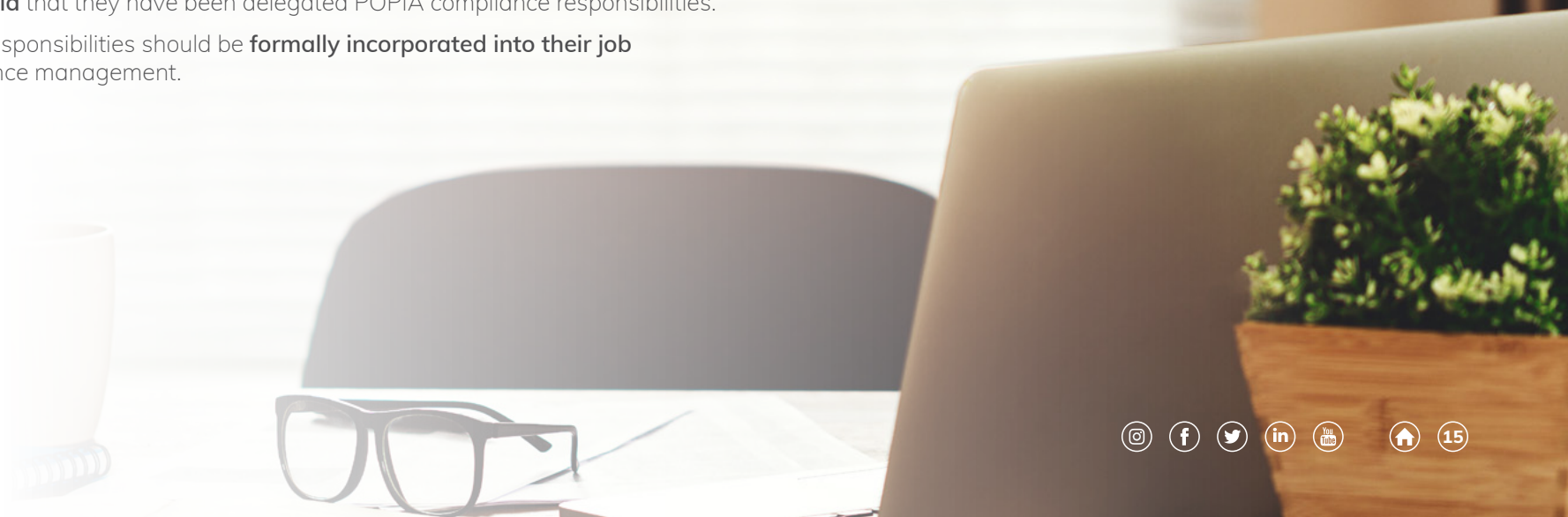
1 Figure Out Who is Responsible for Your POPIA Compliance

POPIA says that the person accountable for the day-to-day POPIA compliance in your organisation ('the information officer') is your CEO. But CEOs are busy people, so POPIA created the role of deputy information officers. Your CEO can therefore delegate the day-to-day responsibility for POPIA compliance to somebody else within your organisation.

What can you do about this? Be proactive. If nobody has been made responsible for POPIA compliance in your organisation yet, reach out to your CEO or your inhouse legal / compliance / risk team. Once you've decided who is responsible for day-to-day POPIA compliance, this needs to be documented as follows:

- The person **needs to be told** that they have been delegated POPIA compliance responsibilities.
- Their POPIA compliance responsibilities should be **formally incorporated into their job description** and performance management.

If nothing else, do these 10 essentials right now before 1 July 2021.



10 Things You Can Do Now (cont.)

2 Find Out Where You Got the Contact Data in Your Database & What They Signed Up For

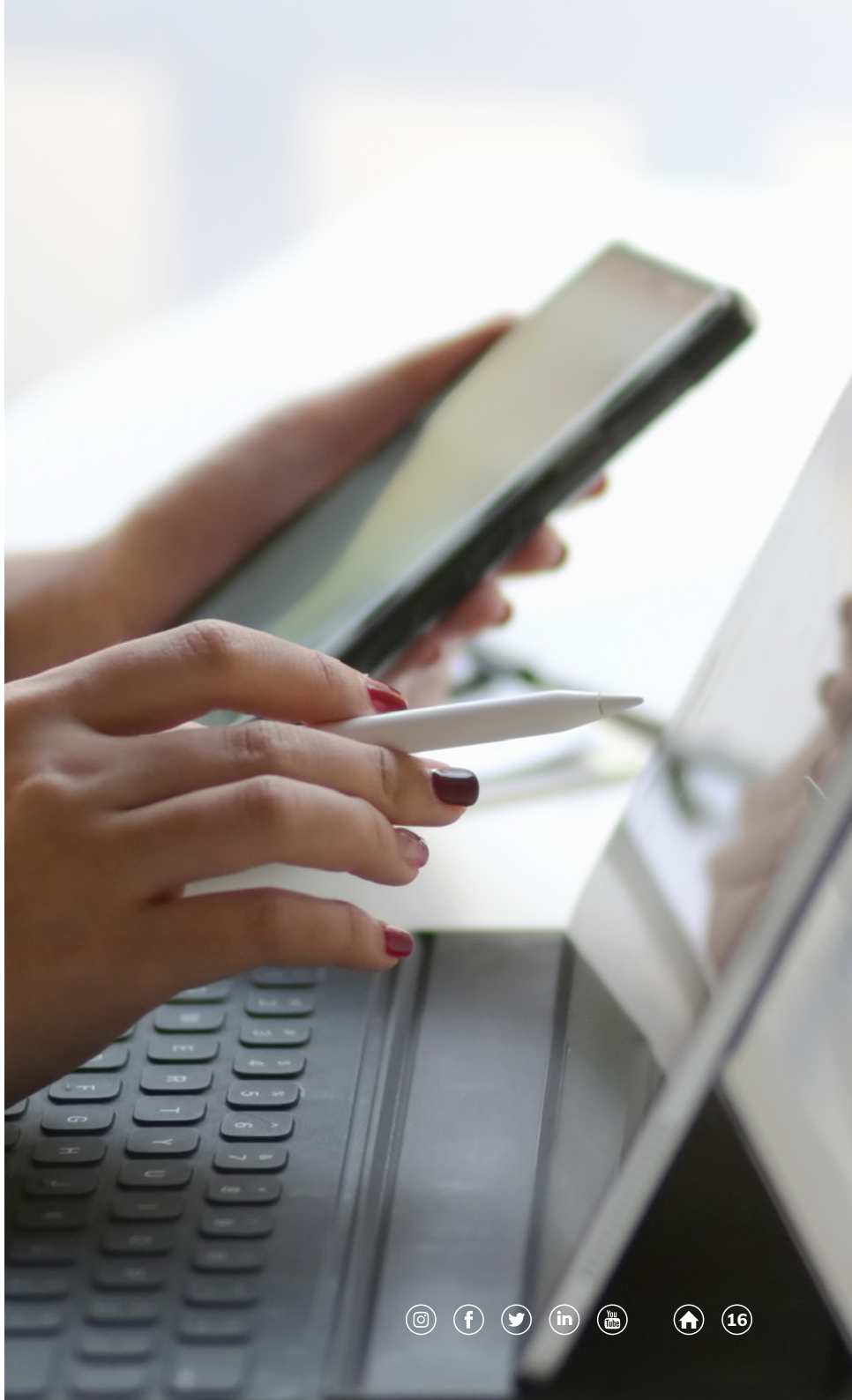
If you only do one thing from this list of 10 things – find out where you got the information on your current database. If you don't know, or you don't have any record, you may need to reconsent that database.

Try Data-Flow Mapping

A data-flow map is a picture that shows the flow of information throughout your organisation. To complete a data-flow map for your database, determine the following details about each contact:

- Where you got their information
- If they consented to receive direct marketing from your organisation
  - ✔ **If yes,** which specific brand / product did they consent to and on which communication channel?
  - ✖ **If no,** check if they unsubscribed.
- If you've given them the opportunity to unsubscribe on each direct marketing occasion
- If you've shared their personal information with any third party and why

Data-flow mapping has other benefits too. According to **this study by Cisco**, data-flow mapping allows organisations to discover operational efficiencies in their workflows and get actionable, real-time insight into customer behaviour.



10 Things You Can Do Now (cont.)

3 Know Your Database ROI & Decide What to Do with it

If you don't know where your data came from, think long and hard before you reconsent your database. Elizabeth from **Novation Consulting** recommends taking a risk-based approach when:

- Your marketing ROI to this base is high
- They gave you their personal information themselves for another reason (i.e. they know that you have their information)
- You've marketed to them before, so they know to expect marketing from you.
- You're sending them the same marketing as before; about products they expect to receive marketing about
- You've always given them the opportunity to unsubscribe easily, and you listen to them when they do
- You've shared your privacy notice with your contacts and have let them know that they can unsubscribe if they want
- No one has ever complained to you about having their personal information and using it for direct marketing

Technically, you may not comply with section 69(3) of POPIA and should have reconsented your base. Chances are that 99% of people who don't want your marketing will just unsubscribe. Worst-case scenario, someone complains to the Information Regulator and they may fine you... but if the ROI justifies the risk, it may be worth having the conversation to see if it's a risk you're willing to take.

10 Things You Can Do Now (cont.)

4 Ensure Your Consents are Valid

Under POPIA, if you're sending electronic communication to a person for the first time, you need to obtain consent. The consent must:

- ✔ Be a **voluntary, specific, and informed** expression of will
  - **Voluntary** means that the consent must be a genuine choice.
  - **Specific and informed** means that it must be clear what direct marketing the person is consenting to.
  - **Expression of will** means that the person must give consent through a clear, unambiguous, affirmative act. The use of pre-ticked opt-in boxes, or double negatives are not allowed.
- ✔ Be an **opt-in**, which means that, if the person does nothing (i.e. does not tick the box), the person will not receive marketing.
- ✔ Contain the **identity and contact information of the marketer**, as well as a person designated to act on behalf of the marketer (usually the information officer or the deputy information officer)
- ✔ Contain the **full name** of the person who gives consent
- ✔ Be **signed** in person or electronically
- ✔ Include:
  - the **date and location** where consent is given
  - the goods or services that will be marketed (in general terms or classes of goods)
  - the **method/s of communication** (e.g., email, SMS)

Some **important good news**: You don't need to use the Regulator's form 4 word-for-word when you draft your consent. Just make sure that the form you use is clear, understandable, and substantially similar.

Remember: Specific and informed consent is specific and informed. If a person has consented to receive direct marketing about apples, for example, it would be fine to send them direct marketing about oranges or other food because these are in the same or similar category of products.

Life insurance, on the other hand, is completely different. If you wanted to send this contact direct marketing about life insurance, you would need to get additional consent to do so.

10 Things You Can Do Now (cont.)

5 Do You Have A (Cool) Privacy Notice?

Section 18 of POPIA requires you to be transparent with people when you collect their information – you need to share a privacy notice. For this privacy notice to meet the POPIA requirements, it must:

- Be simple, written in plain language, and it must be prominent on your website
- Explain what information is being collected, how (and why) it is being used, and the data subject's rights in relation to their records
- Be used as a tool to inform customers that you treat their personal information with care and respect, and process their personal information ethically and responsibly

The UK's Information Commissioner's Office has **issued a code of practice on privacy notices** which is a great place to start and provides examples of good (and bad) privacy notices.

Also, have fun with it. Our favourite privacy notices include:

- **LinkedIn**, because it uses multi-media and graphic design elements and is really reader focused.
- This one by **August**, a digital marketing agency in Australia. It even has a fish in it.

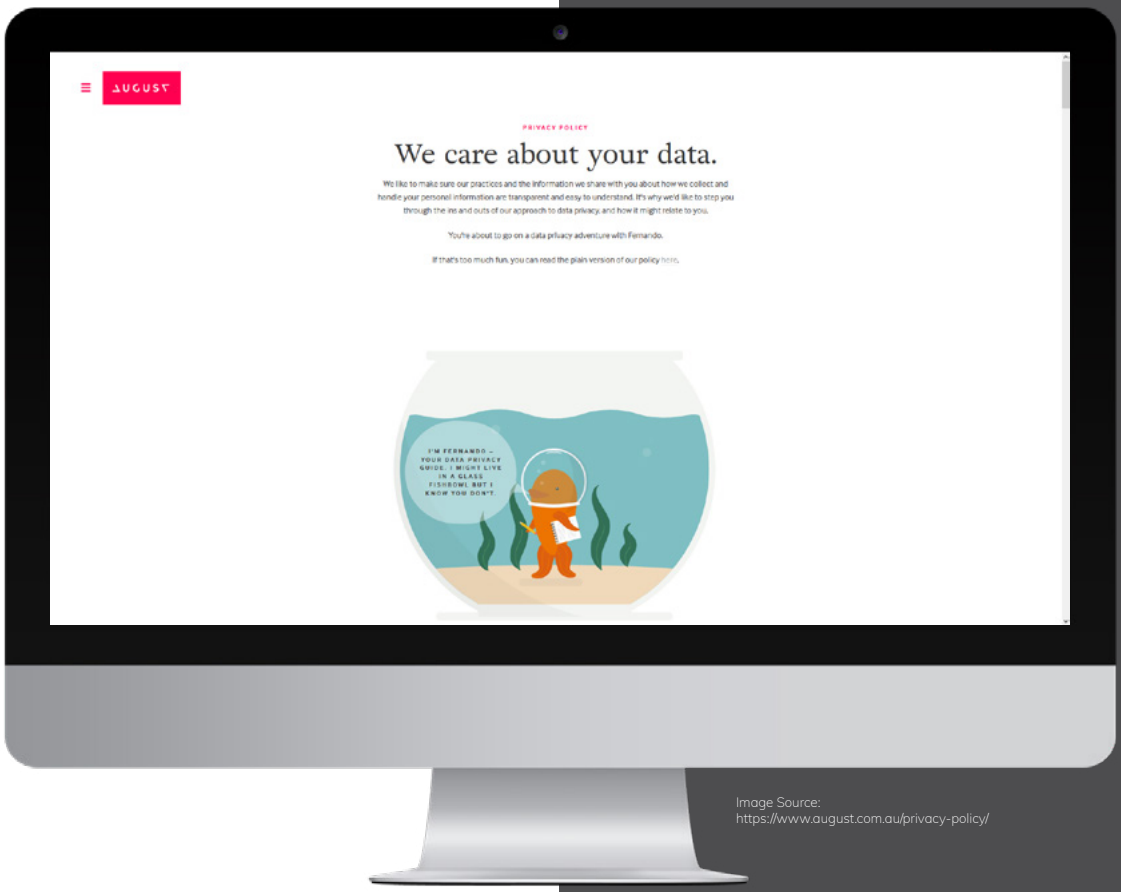


Image Source:
https://www.august.com.au/privacy-policy/

Novation Consulting loves some privacy notices so much, **they even wrote a blog about it**.

10 Things You Can Do Now (cont.)

6 Audit Your Unsubscribe Process

POPIA is all about the unsubscribe. Everyone you send direct marketing to must be given an ironclad way to unsubscribe from receiving direct marketing every. Single. Time.

For the unsubscribe process to be POPIA compliant, it must be clear, easy, free of any penalisation or cost, and in the same channel as the direct marketing communication.

For instance, if the sender sends direct marketing via an email, the opt-out process must also be email or internet-based – it isn't acceptable to ask them to send an SMS for this. The same goes for SMSs: opt-outs must be SMS-based. You must manage unsubscribes regularly and effectively to keep your database compliant with POPIA.

Then test your unsubscribe process. For all direct marketing channels. Sign-up and unsubscribe to make 100% sure it works.

10 Things You Can Do Now (cont.)

7 Audit Your Unsubscribe Process Again

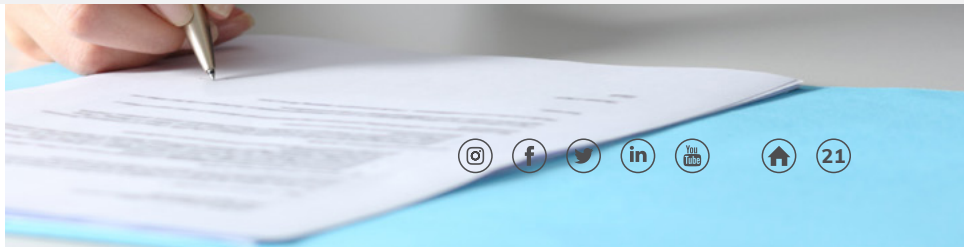
We cannot emphasise this enough. So many organisations don't practice Master Data Management – where a contact's master record is managed in one place. The problem with this is often, when a contact unsubscribes, the unsubscribe doesn't pull from one system to the other. This is the most common reason why people complain.

Many companies in Europe have been fined a lot of money under the GDPR for failing to process their unsubscribes properly. For example:

In October 2019,
a Greek telecommunications company was fined
€200,000
for contacting many customers via telemarketing – when all these customers had specifically opted out of receiving telemarketing from them. The unsubscribes had not been processed properly due to technical issues.

In March 2020,
a Romanian company was fined approximately
€3000
for sending a commercial message to **just one** customer who had already unsubscribed from receiving commercial messages from them.

Want to learn more about Master Data Management? Read this white paper from IBM.



10 Things You Can Do Now (cont.)

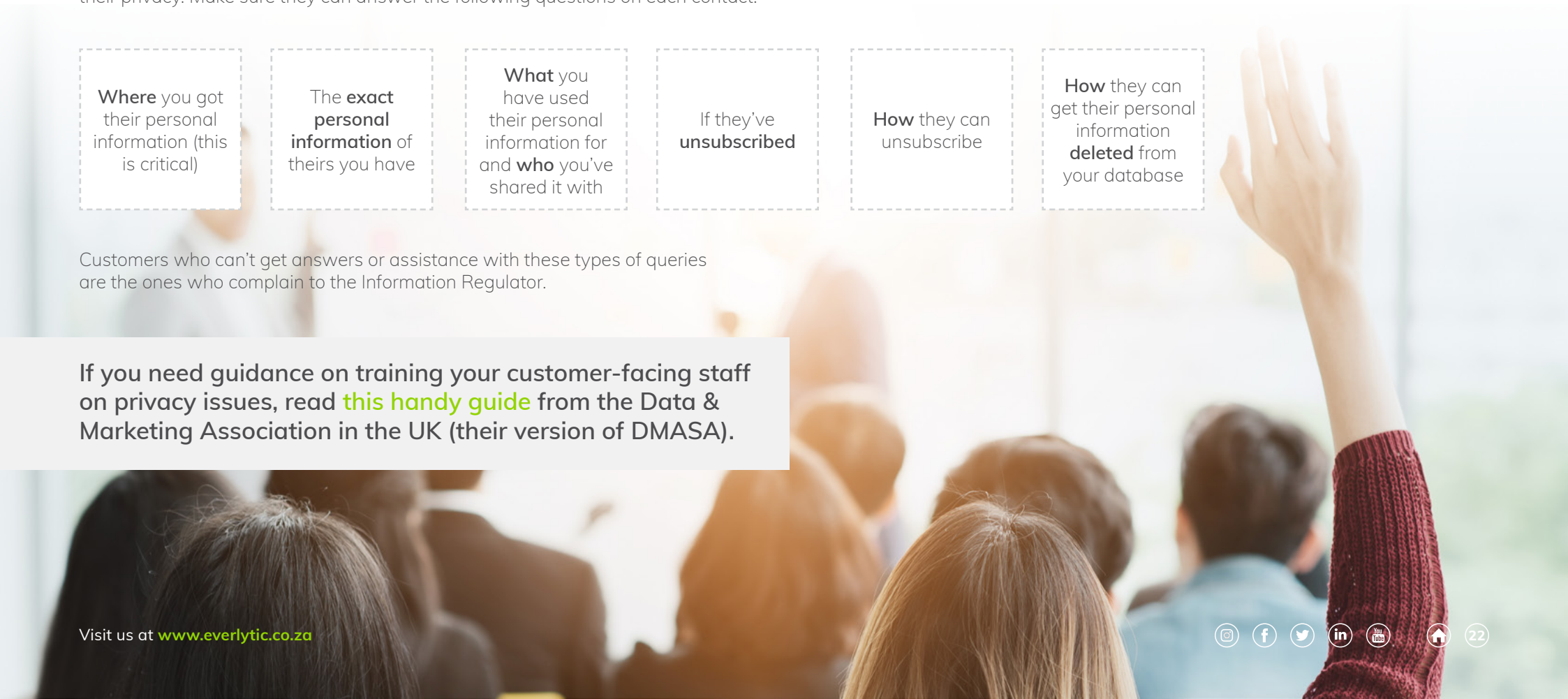
8 Train All Your Customer-Facing Teams

Your account managers and the staff in your call centres are the first point of call for ensuring your contacts feel like you're respecting their privacy. Make sure they can answer the following questions on each contact:

- **Where** you got their personal information (this is critical)
- The **exact personal information** of theirs you have
- **What** you have used their personal information for and **who** you've shared it with
- If they've **unsubscribed**
- **How** they can unsubscribe
- **How** they can get their personal information **deleted** from your database

Customers who can't get answers or assistance with these types of queries are the ones who complain to the Information Regulator.

If you need guidance on training your customer-facing staff on privacy issues, read this handy guide from the Data & Marketing Association in the UK (their version of DMASA).



10 Things You Can Do Now (cont.)

9 Make Sure Your Data is Ultra-Secure

Check your information security management. IBM's 2019 'Cost of a data breach' Report found that the average cost of a breach in 2019 was a whopping USD3.92 million. However, this report also found that organisations who had a thorough incident-response plan in place reduced the cost of a data breach by an average of USD1.23 million. It is worth it!

Under POPIA, you're also required to notify the Information Regulator and data subjects in question when you have reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person. POPIA requires that you have an incident response plan in place to deal with any personal information breaches and to inform the Information Regulator about what this plan entails.

For more guidance, read Novation Consulting's blog posts on formulating an incident response plan and who should be on your incident response team.

10 Things You Can Do Now (cont.)

10 Write Down the Rules You Make

There is no point in going to all this effort if you don't have evidence of it. Regulation 4 of the **2018 POPIA Regulations** requires your organisation to have certain documents and procedures in place to demonstrate your POPIA compliance.

Write down all the things you've done to be POPIA compliant, so if you need to deal with the Regulator, you can show them. Here's another **helpful blog post** about what you should include in these documents and procedures, and how to get your POPIA house in order.

Embrace The 'Privacy Actives'

According to **CISCO's Consumer Privacy Survey**, as much as 32% of the population fits into a new marketing segment called the 'Privacy Actives'. These people have already actively chosen new service providers based on how their data is protected.

These privacy actives are a very desirable marketing segment as they're:

- Young
- Early tech adopters
- Very active on social media

To embrace this growing group of people, get to know what your return is on your database, how you can protect the data in it, and how you can enhance it with POPIA. A good question to start asking yourself is:

How can we **embed privacy** in our marketing?

Another great CISCO report referred to in the webinars:

From Privacy to Profit: Achieving Positive Returns on Privacy Investments

Read it Here

Conclusion

POPIA is here to stay.

But that doesn't have to be a scary thing.
Embrace it and not only can you stay compliant – it may even be good for your business.

List-Friendly Compliance Requires a New Breed of Lawyer

Compliance can change minds. Increase sales. Reduce complaints. Add value.

It's also an integral part of doing ethical business. We'll help you do things right and grow your business.

www.novcon.co.za
elizabeth@novcon.co.za
083 342 6011

Contact Us

Better Communication Means Better Business

Get the all-in-one bulk email,
SMS, voice broadcasting,
and marketing automation software
to make it happen
- compliantly.

www.everlytic.co.za
sales@everlytic.com
011 447 6147

Get a Demo