NOT ANOTHER POPIA WHITE PAPER:

novation consulting

10 years: 10 lessons. 25 June 2020

JUTA

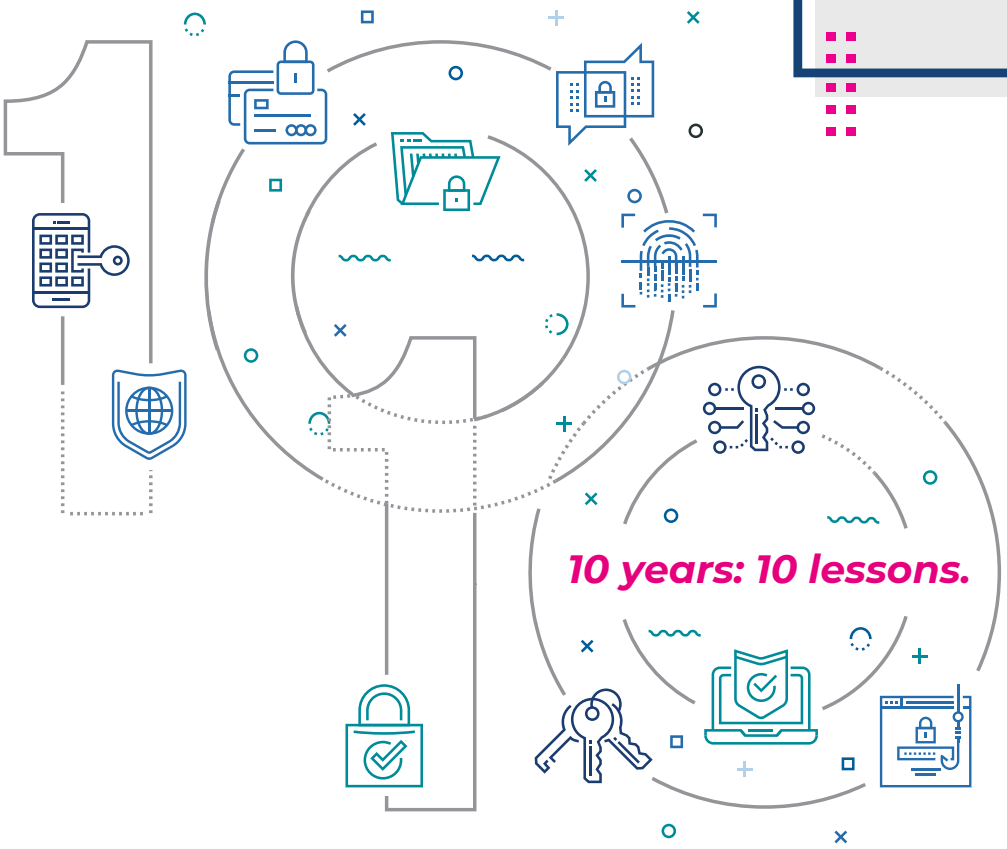
NOT ANOTHER POPIA WHITE PAPER: 10 YEARS: 10 LESSONS.

It has been a decade since talk of the Protection of Personal Information Act started. Ten. Years. And finally we have an effective date. It is 1 July 2020. That's right; it means that we have until 30 June 2021 to become compliant.

We've been talking about it for so long that, understandably, many people are suffering from POPIA fatigue. This white paper is our attempt at getting you excited about compliance with the POPIA (yup, it's absolutely possible!). It is a collection of lessons we have learnt over the years by asking why so many POPIA programmes fail.

WHAT DOES 'FAIL' MEAN? FOR US, A FAILED PROGRAMME IS WHEN WE COME BACK THREE YEARS LATER, AND WE FIND SIGNIFICANT LEVELS OF NON-COMPLIANCE. OR WORSE, UNKNOWN LEVELS OF NON-COMPLIANCE.

So how does that happen? And how can you avoid it?



01. STOP WORRYING ABOUT THE POPIA – AND WHAT YOU SHOULD FOCUS ON INSTEAD

Lesson #1

Don't make it about POPIA compliance.

No organisation has compliance as one of its strategic objectives. It is perceived as a pain, not a gain. So how do you get boards to get behind a POPIA programme? You speak their language – money.

"IF YOU CAN'T MAKE SOMETHING IMPORTANT INTERESTING, THAT'S YOUR OWN FAULT."

– Ezra Klein, Editor-in-Chief for Vox.

It's all about the numbers

Let's start with some astonishing numbers and see if we can't convince even the most jaded board member that privacy is important, with or without the POPIA.

- Maybe the next 'must-have' market will be the 'privacy actives'. Roughly 32% of people have already switched companies or providers over their data policies or data sharing activities. This demographic is an important one, because they are younger, they do more of their shopping online, they see themselves as early tech adopters and they are frequent users of social media. According to Harvard Business Review, you can put these findings to work by including privacy as part of the overall 'customer experience', fixing the transparency gap and engaging 'privacy actives' as you explore new ways to use data.
- As important as making money, is saving it. Privacy has you covered by reducing sales delays, mitigating losses caused by data breaches, and achieving operational efficiency through data controls. A recent study by Cisco showed that, on average, for every dollar spent on privacy, organisations received $2.70 in benefits.

'IF YOU THINK COMPLIANCE IS EXPENSIVE, TRY NON-COMPLIANCE.'

– General Paul McNulty, former US Deputy Attorney General

- In 2019 IBM and the Ponemon Institute calculated the average cost of a data breach at $3.9 million. But, the good news is that having an incident response plan and team, and testing them from time to time, will likely save you $1.23 million.
- Like keeping up with the Joneses? At the height of the GDPR implementation in 2016/2017, organisations were spending $354 per employee per year on privacy. This cost has settled at a cool(er) $128 in 2019.

INTERESTED IN FURTHER READING?

- This IAPP report is an excellent place to start reading about Getting to the ROI of Privacy, even though it is a bit old.
- For the latest on Privacy RIO, take a look at this report by CISCO.
- Learn about the cost of a data breach from IBM and the Ponemon Institute.
- This IAPP-EY Annual Privacy Governance Report tells you what other organisations are doing and spending.

02. MIND THE GAP: DON'T START WITH A GAP ANALYSIS

Lesson #2

Don't start with a gap analysis. You know you are non-compliant, most of us are. The only exception to this rule is if data protection is not new to your organisation. E.g. you have been subject to the GDPR.

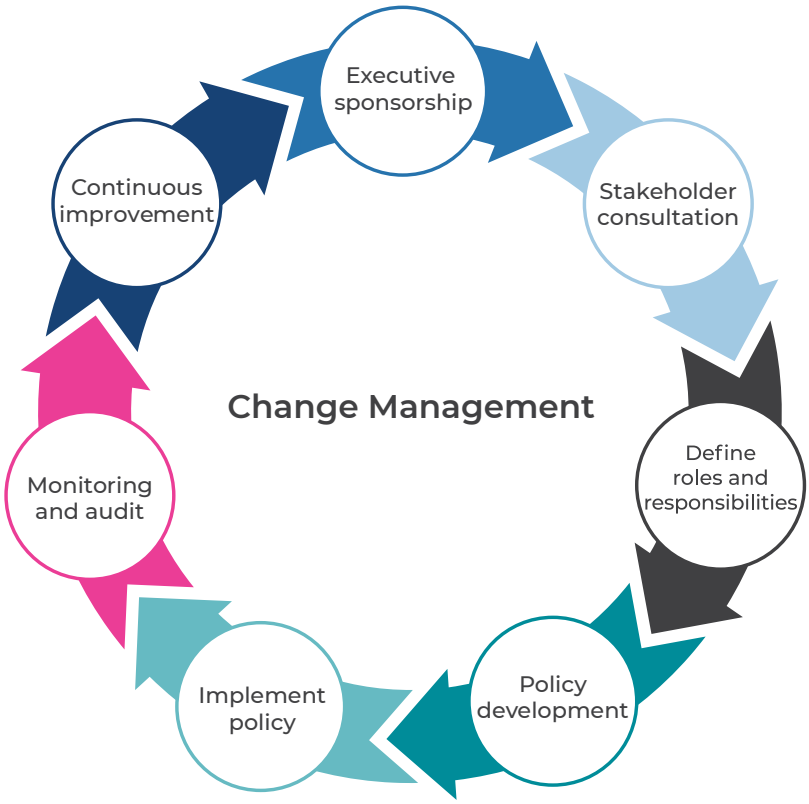
Most POPIA tenders or RFPs ask for proposals for a 'gap analysis'. We have learnt that this is putting the cart before the horses, particularly if it is the organisation's first foray into data privacy.

First, the words 'reasonable' or 'reasonably' appears in the POPIA 78 times. We checked. That is not surprising, because the POPIA is an example of principle-based legislation. Organisations must exercise sound judgment and do what is fair and sensible under the circumstances. Each organisation must consider the principles in the legislation and decide what would be fair and sensible for the organisation given (for instance), what personal information is processed, why it is processed, the nature and scope of the processing, the size of the organisation, the industry it operates in. For us, this means creating policies, standards, procedures and guidelines for that specific organisation.

Second, it doesn't make sense to spend money on a gap analysis if you already know that you don't comply with the POPIA. All you will get is 200 pages of problems and no way to solve them.

Again, if you already have some data privacy controls in place, and you want to know what else you should do, a gap analysis may be useful.

So where should you start? This is our roadmap to creating a sustainable POPIA programme:



02. (continued)

- **Executive sponsorship:** See lesson #1 about setting the tone at the top. If you can't convince your board that privacy is essential, it isn't. Find something else to do.

> **'STAKEHOLDERS ARE ANYONE IN AN ORGANISATION WHO WILL KILL A GOOD IDEA OUT OF SPITE OR POLITICAL ILL WILL.'**
>
> – Unsuck-it.com

- **Stakeholder consultation:** Find the decision-makers, the people whose input you will need, the people who will be affected and the people whose support you need to make all this happen.
- **Define roles and responsibilities:** Who is responsible for ensuring POPIA compliance? Who will be doing what to whom? Lesson #5.
- **Policy development:** Create policies, procedures, standards and guidelines in which the organisation records what they are going to do and how they are going to do it.
- **Implement policy:** No, this does not mean 'email the policy to everybody'. See lesson #8.
- **Monitor and audit:** Because, if you do not measure compliance with policies, you are not managing it. This is the gap you should be minding.
- **Continuous improvement:** The result of your monitoring and auditing should be change (unless the audit was perfect). Audit findings should mean something – this is the hallmark of a sustainable POPIA programme.
- **Change management:** Effectively prepare and support people through change. We do not see change management as a phase in this process. It is integral to each stage. More about this in lesson #9.

If you are hellbent on starting with an assessment of some kind, start by assessing what POPIA-related policies you already have and how well they have been implemented. More about that in lesson #3.

03. THINKING 'THE POPIA IS COMING, LOOK BUSY' IS A MISTAKE. HOW TO CALM DOWN AND MAKE THE MOST OF THE TIME YOU HAVE LEFT.

Lesson #3

Becoming POPIA compliant takes more than a year. Maybe a COVID-19 year. They are 19 times longer than standard years.

POPIA programmes take long to establish. Exactly how long depends on the nature and size of the organisation, but mostly it depends on something we call information governance maturity. If the way in which information (*all* information, not just personal information) is governed is not well established and effective, the organisation must fix that first, before moving onto the POPIA. And, just like that, a year is no time at all.

> **'PRIVACY IS EASIEST WHEN IT IS THE ORGANISATION'S STANDARD MODE OF OPERATION AND MONITORING IS MAINSTREAMED THROUGH EXISTING GOVERNANCE MECHANISMS SUCH AS THE BOARD, EXECUTIVE OR SENIOR MANAGEMENT MEETINGS. MONITORING AND REVIEW CAN BE ACHIEVED THROUGH EXISTING MECHANISMS SUCH AS THE AUDIT AND RISK COMMITTEE OR CUSTOMER OR OTHER ADVISORY COMMITTEES.'**
>
> – Dr Elizabeth Coombs, NSW Privacy Commissioner

Why are we talking about information governance now? With all the hype around the POPIA and data protection, organisations are forgetting that personal information is not the only class of information that is essential for doing business. For many organisations, personal information won't even be the most valuable information they use. Measured in Rands and cents, their intellectual property may be more valuable.

Here are some other forms of information:

- all intellectual property (trademarks, designs, inventions, trade secrets, know-how, content or publications the organisation created, technical documents);
- information on the organisation's website;
- financial information;
- contracts and information about contract negotiations;
- strategies and plans;
- policies and procedures;
- internal memoranda, minutes of meetings and agendas;
- emails;
- research and statistics; and
- personal information of customers and prospective customers (leads), employees and employment candidates, suppliers and service providers.

TOOL TIP

Information governance maturity assessments help organisations to spot areas of information governance that need to be improved. We also use the maturity assessment to determine whether an organisation is ready for a POPIA project. Here is the one we use. It is adapted from the ARMA International Information Governance Maturity Model.

We've also written a blog that will help you interpret the results. Spoiler alert, the blog even shares which projects we think may be more useful to your organisation than a POPIA programme.

04. KNOW YOUR BLIND SPOTS. ATTORNEYS AND COMPLIANCE OFFICERS ARE NOT TRAINED FOR THE POPIA.

Lesson #4

Lawyers stick to what they know. The POPIA is about so much more than an updated privacy notice or a template data protection clause.

Many requests for assistance start with 'draft a records management policy, give me a retention schedule, draft a privacy notice, an operator clause template or a non-disclosure agreement'. As lawyers, we focus on the legal documents. It is what we know, but it is a fraction of what the POPIA entails.

'INFORMATION GOVERNANCE (IG) IS A NEW AND DEVELOPING HYBRID "SUPER DISCIPLINE" THAT CROSSES MULTIPLE FUNCTIONAL BOUNDARIES, PRINCIPALLY RECORDS MANAGEMENT, INFORMATION SECURITY, RISK MANAGEMENT, LEGAL AND E-DISCOVERY ISSUES, INFORMATION TECHNOLOGY (IT), BIG DATA ANALYTICS, PRIVACY, AND MORE.'

– Robert Smallwood.

A complete POPIA programme includes several disciplines that are way beyond what lawyers were trained to do, for instance:

- Data security
- Data quality
- Reference and master data management
- Metadata management
- You know... 'IT stuff'

The problem with being out of our depth is that we will naturally prefer tasks that are familiar to us, instead of prioritising tasks based on how important they are.

How do we combat this? The first step is to understand our blind spots. The second is to find people who do know how to tackle these areas, which we are not equipped to handle. Which brings us to lesson #5.

05. POPIA COMPLIANCE IS A TEAM SPORT – WHO YOU SHOULD PICK

Lesson #5

Compliance, Risk, Legal, IT... no one can go it alone. The POPIA involves the entire organisation.

The sheer scope of the POPIA breaks lawyers and compliance officers. Complying with the POPIA often requires that everyone in an organisation changes the way they work. We must go back to compliance and risk management basics: the three lines of defence.

What is the role of the three lines in POPIA compliance?

01 Management:
The organisation owns and manages the risk (not you)

It is their responsibility to manage the personal information that is processed in their area. They own the risks that could impact the processing of personal information. They must decide whether to do something about the risk or not.

02 Compliance:
Monitor, challenge, advise, and report (this is you)

Information officers and their deputies, information security officers and other people with 'information' in their title perform a compliance and risk management function. It is their job to interpret the POPIA, develop policies, standards, procedures and guidelines, to advise the organisation and to monitor and report on compliance with the POPIA. They poke and prod.

03 Independent assurance:
Marks everybody's homework (not you)

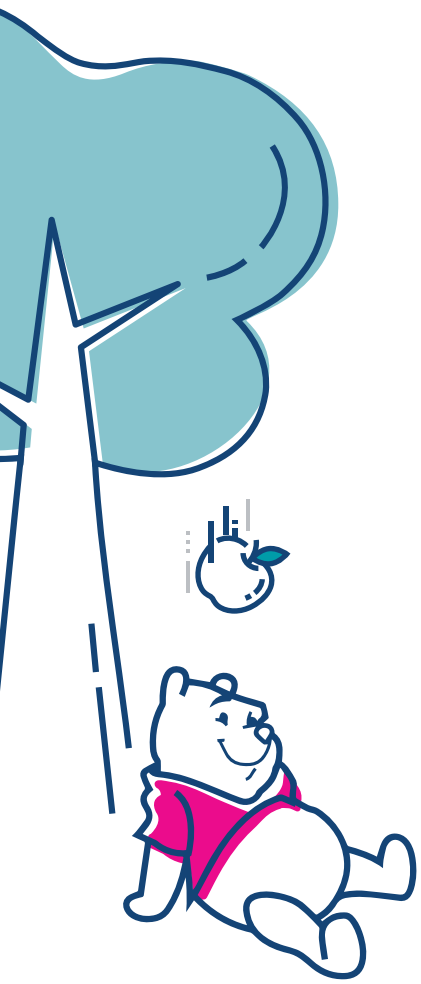
They mark the other two lines' homework. Internal and external audits are used to uncover POPIA compliance issues and to avoid surprises.

So, who is on the POPIA team? In a sense, everybody.

06. THE LEADING EXPERT ON RISK MANAGEMENT IS WINNIE THE POOH

Lesson #6

If you don't take a risk-based approach, you will succumb to analysis paralysis.



POPIA programmes often get stuck in exceedingly long phases of project planning, risk identification and analysis, which creates little or no value. Teams often spend so much time trying to decide what to do first, that they end up exhausting the available time and budget.

> *"Supposing a tree fell down, Pooh, when we were underneath it?"*
>
> *"Supposing it didn't," said Pooh after careful thought. Piglet was comforted by this.*

Avoid this analysis paralysis by going back to risk management basics and prioritising existential risks or mindblowing opportunities over the small stuff.

Need to hone your skills?

The Institute of Risk Management South Africa – they are great on LinkedIn.

Many risk frameworks are based on ISO 31000. The information security management standard is ISO 27001. Here is an article about both, and here is a critical analysis of the standard.

We need to get better at doing a root cause analysis of risks to avoid risk management groundhog day. Here is an excellent guide to the questions you should ask to break the cycle and get to the root of the problem. It was drafted for information security risks but works well with other types of risks too.

'ONE OF THE MAIN CYBER-RISKS IS TO THINK THEY DON'T EXIST. THE OTHER IS TO TRY AND TREAT ALL POTENTIAL RISKS. FIX THE BASICS, PROTECT FIRST WHAT MATTERS FOR YOUR BUSINESS AND BE READY TO REACT TO PERTINENT THREATS.'

– Stephane Nappo, Global Chief Information Security Officer, 2018 Global CISO of the year

06. (continued)

How we manage risk

We apply the 80/20 principle. In POPIA terms, this means identifying those activities that will address 80% of the risk, and to prioritise those.

This led us to:

THE POPIA TOP 5

(5 THINGS TO DO, IF YOU DON'T DO ANYTHING ELSE)

INCIDENT RESPONSE:

Get an incident response team and a grip on what your plan is for when the POPIA strikes the fan

IMPLEMENT A DATA PROTECTION IMPACT ASSESSMENT:

Whether you call them personal information assessments or privacy impact assessments, they stop you from introducing new POPIA risks into your organisation

ACCESS CONTROL:

No, everybody should not have access to everything

REVIEW YOUR FORMS:

Make sure you know why you ask what you ask and that you are transparent about what you use the information for

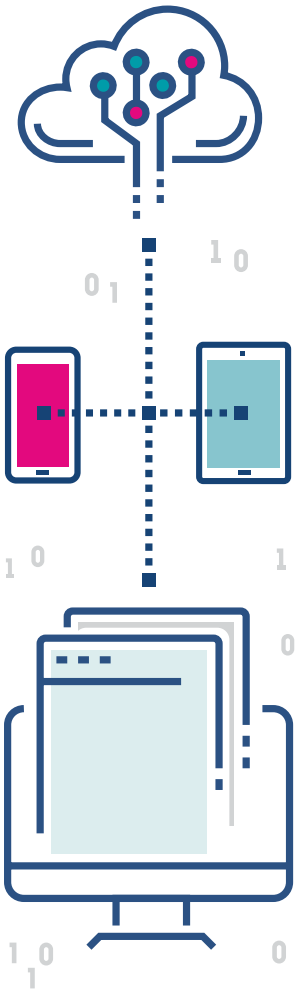
HAVE A PLAN FOR THE REST:

The POPIA regulations require that information officers must develop, implement, monitor and maintain (so many *&^% verbs) a compliance framework

07. **LEAVE IT ALONE;** THE POPIA IS NOT THEIR PROBLEM

Lesson #7

The POPIA is not an IT project.



We ♥ IT, but they shouldn't 'own' POPIA programmes.

When you make POPIA compliance IT's responsibility, the rest of the organisation tends to think:

- The POPIA is just about protecting digital information from hackers. While cybersecurity is undoubtedly critical, it is a small part of the POPIA.
- You can correct all information risk with technology.

Best practice in corporate governance is to split the governance of information from the governance of technology. Privacy falls under information governance, but is usually also one of the ethical principles that underpin the governance of technology.'

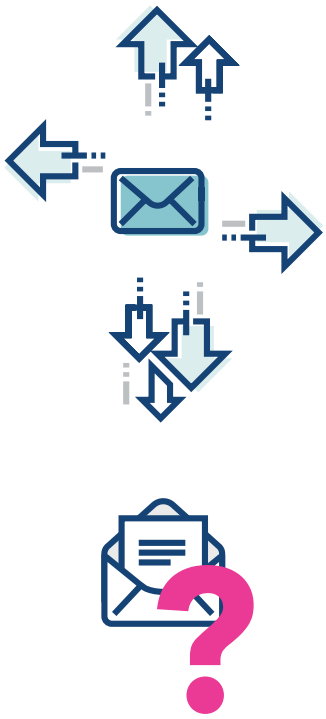
'IT IS RECOGNISED THAT INFORMATION AND TECHNOLOGY OVERLAP BUT ARE ALSO DISTINCT SOURCES OF VALUE CREATION WHICH POSE INDIVIDUAL RISKS AND OPPORTUNITIES. IT IS TO REINFORCE THIS DISTINCTION THAT [PRINCIPLE 12] IN THE KING IV CODE NOW REFERS TO TECHNOLOGY AND INFORMATION INSTEAD OF INFORMATION TECHNOLOGY.'

– King IV Report on Corporate Governance for South Africa 2016

08. EMAILING A POLICY TO EVERYBODY IS NOT THE SAME AS IMPLEMENTING IT

Lesson #8

Just because you have emailed the new data protection policy to everybody doesn't mean that you have implemented it.



Too many organisations still write policies that they never implement. The policies are there, in a folder somewhere, but no one follows them, compliance isn't measured in a meaningful way, and there are no consequences for non-compliance.

Think about the impression it creates with an Information Regulator when the Board has approved a Data Protection Policy, but no one is complying with the policy, and there are no consequences? It says 'we knew what we were supposed to do, but we couldn't be bothered'.

What does it mean to implement a policy?

Start by measuring the impact of the policy.

1. Who is the **team** responsible for implementation?
2. What is the impact on other **policies?**
3. What is the impact on **processes?**
4. What is the impact on **infrastructure?**
5. What is the impact on **people?**

It is wise to measure the impact of a policy before the policy is approved to ensure that it is realistic. If a policy is unrealistic, employees will not follow it, not because they are lazy or careless, but because they couldn't follow it and still do their jobs effectively.

Your Records Management Policy says that your organisation disposes of physical records that contain personal information by shredding them. You purchase a shredder for this purpose, but the shredder can only shred eight pages per minute and can only shred for three minutes at a time.

This means that it will take fifteen minutes to destroy one hundred pages. On the first day, employees stand in long queues to shred their documents. On the second day, they have gone back to keeping everything.

09. AT LEAST 50% OF YOUR POPIA BUDGET SHOULD BE SPENT ON TRAINING. OTHERWISE YOU ARE DOING IT WRONG.

Lesson #9

The POPIA is a people problem. This is why you need to spend 50% of your budget on training.

Compliance is about getting people to change their behaviour to a degree. The POPIA demands extensive change; it will change how most people at your organisation work in one way or another. A successful compliance project depends on deliberate change management.

'SEEK FIRST TO UNDERSTAND, THEN TO BE UNDERSTOOD.'

– **Dr Stephen Covey** (*Seven Habits of Highly Effective People*)

Understand that change is loss

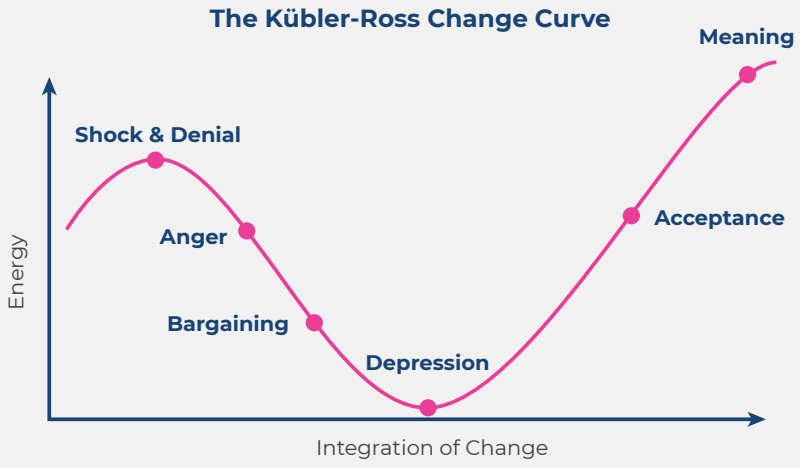
One of the keys to navigating change is understanding that all change involves loss, and that the human response to loss is grief. It sounds terribly dramatic and out of place in a business context, but the POPIA is a mean girl; she will make you grieve.

Luckily, people like David Kessler, Elisabeth Kübler-Ross, and David Kessler have been studying grief for decades. They wrote *On Grief & Grieving: Finding the Meaning of Grief Through the Five Stages of Grief*. We use the five stages of grief often when we guide organisations through significant change.

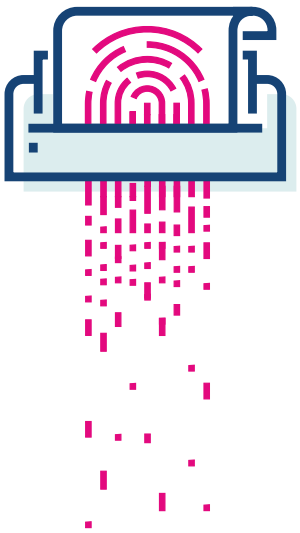
What is the meaning of this?

Kessler's new book, *Finding Meaning: The Sixth Stage of Grief*, was published just in time. For those who need a reminder, here are the five stages of grief, plus the new sixth stage:

6 STAGES OF CHANGE



09. (continued)



Seasoned compliance folk will recognise these phases:

- **Shock & denial:** Surely the POPIA won't come into effect this year. We don't have to worry about this yet.
- **Anger:** *^$&%^%%$@! We have just done a compliance project, now the POPIA. Where are we supposed to get the budget?
- **Bargaining:** We don't really do much with personal information. We are not the type of business to which the POPIA applies. We are not a bank.
- **Depression:** Just get it over with, but count me out. Decline meeting invite.
- **Acceptance:** Righto, let's do this. Accept meeting invite.
- **Meaning:** See lesson #1.

But, change doesn't have to be hard.

Here are some things that will make it easier on them (and you!):

- Involve them in the change. If they feel that they are causing the change, they may skip ahead to acceptance.
- Ask them why they do things a certain way, before you tell them how you think it should be done. People find the best way to achieve their shared goals when everybody is listening.

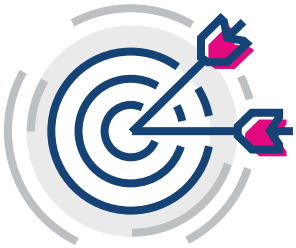
> **'THE MORE YOU LISTEN TO SOMEONE...AND THE MORE THAT PERSON LISTENS TO YOU, THE MORE LIKELY YOU TWO WILL BE OF LIKE MINDS.'**
>
> – Kate Murphy *(You're Not Listening: What You're Missing and Why It Matters)*

- Emphasise the benefit instead of the loss. Lesson #1 again.
- Get the 'influencers' on your side. No, we are not talking about a Kardashian. There are influential, charismatic people in every organisation who can make or break programmes. Find them, convince them of your cause – others will follow.

10. THERE IS NO SUCH THING AS 'GENERAL AWARENESS'

Lesson #10

One size fits all training is a waste of money. There is no such thing as 'general awareness'.



We often get asked to come and do 'POPIA general awareness training' for all employees. The answer is always no. Can you imagine something worse than sitting through the eight conditions for the lawful processing of personal information if you have nothing to do with the processing of personal information? We can't. Half the reason why people think compliance is boring is because we keep training them on things that are not relevant to them.

'AN INFORMATION OFFICER MUST…ENSURE THAT…INTERNAL AWARENESS SESSIONS ARE CONDUCTED REGARDING THE PROVISIONS OF THE ACT…'

– The POPIA Regulations

But the POPIA requires training?

Sure, the POPIA requires training, but we firmly believe that it doesn't require irrelevant training. Training should be customised for different audiences. Develop a training plan that answers these questions:

- Who do you need to train? Hint, if you don't need someone to do their job differently tomorrow, leave them alone so they can get on with their jobs!
- What do you need to train them on? Don't train them on what the POPIA says. They are not lawyers. Teach them what they need to do differently.
- How will you train them? Look at how this audience prefers to be trained, the infrastructure available to you, and how much time you can reasonably expect them to devote to learning.
- How often must they be trained? Change is a process, and training is rarely a once-off exercise.

If this all sounds foreign to you, find the people in your organisation who are experts at communicating with your employees. They usually sit in your Learning and Development team in Human Resources, your Internal Communications team or in Marketing.

'There are only two ways to influence human behaviour: you can manipulate it, or you can inspire it.

– Simon Sinek *(Start With Why)*

ABOUT NOVATION

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.
- 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.

ABOUT JUTA

Juta is South Africa's leading academic and law publisher trusted for quality academic, legal, professional and school publications that match the power of technology with authoritative local content.

Juta's new generation of resources and services, customised for the needs of non-legal professionals and corporate users requiring legal content to perform their functions, enable organisations to achieve compliance, facilitate good governance and mitigate risk.

Juta has remained relevant by embracing technological innovation and diversifying beyond publishing to offer accessible e-learning solutions as well as technology-driven information and research platforms that help businesses simplify and automate their operations.

Juta is proud publisher of a Elizabeth de Stadlers, *A Guide to the Protection of Personal Information Act* (co-authored with Paul Esselaar and Ilze Luttig Hattingh). Pre-order here.