



South Africa

Onboarding Guide

Contents

Implementation Guide	2
Organisation Setup	3
Key Terms.....	3
Information Officer	3
Data Mapping.....	4
Compliance Audit.....	5
Governance	7
Privacy Notices.....	7
Security Measures.....	7
Training & Awareness	8
Compliance Monitor	8
Stakeholder Communications.....	9
Operators	10
Information Sharing	11
Subject Access.....	12
Requests.....	12
Received.....	13
In progress	13
Security Compromise	14
Privacy Impact Assessment.....	15
Screening Questions	16
Purpose	16
Processing justification	16
Individual's rights	17
Risks and Mitigations	17
User Maintenance.....	18
Glossary.....	18

Implementation Guide

Your organisation is the [Responsible Party](#). We suggest you adopt the following approach to rolling out your privacy compliance program.

1. Understand the organisation's activity by asking:
 - what are the core activities?
 - how many employees?
 - do you outsource the processing of personal information?
 - do you disclose personal information to other organisations?
 - do you transfer personal information outside of South Africa?
 - who heads up departments, e.g., HR, Sales and others that deal with personal information?
 - who is leading the privacy program?
2. Heads of departments ([Information Owners](#)) to formulate a list of ALL processing activities that involve personal information; including any informal activities. If possible, record the sources of the personal information, where the information is stored in their departments, and to whom the information is disclosed. Include physical media as well.
3. Heads of IT / Procurement to compile a list of all Vendors involved with processing of personal information, the country in which they are located, the expiry date of those contracts.
4. Inform the CEO / MD / head of organisation of the responsibilities of the [Information Officer](#), who must also complete and maintain the Information Officer checklist found in Compliance Audit. Check the Regulator's [website](#).
5. Information Officer to appoint Deputies as appropriate.
6. Register with the Information [Regulator](#)
7. Ensure your Organisation Settings are complete. (see next section).
8. Add the relevant heads of departments and the program lead as users with the system role of Administrator. (Compliance User and Task Owner must be added via the Compliance sections)
9. Following point 2. above, Information Owners to review and understand ALL processing of personal information in their respective departments. Be aware of and record all *informal* processing too. For example, populating spreadsheets to manage processes outside of the formal, networked and security protected systems and apps.
10. Begin the data mapping exercise, using the prep work done by the Information Owners and record any work to be done beyond this session. The head of IT could provide valuable insight or guidance especially around any processing of personal information that may be outsourced to [Operators](#) as well as the processing done by IT. Set a date for a follow-up data mapping session. Use the follow-up session to complete the data mapping exercise.
11. Follow the steps as indicated by the various sections below – remember, compliance is on-going.

Organisation Setup



You should have received a welcome email inviting you to set a password. If not taken directly to this page you will find it under Organisation / Settings in the upper navigation bar.

Under **'Your Organisation'** enter your contact details and upload your logo.

Under **'Your Location'** enter your physical and postal addresses.

Under **'Your Officers'** enter the organisation lead's (e.g. the CEO) name and email address as well as the Information Officer's details. In most cases, this will be the same as the Organisation lead but you must still complete both sections.

Under **'Your Needs'** select the organisation size and any features you may need to add to the solution.

Under **'Your Plan'** you have the option of subscribing or going to a 14-day trial. To go to trial, select **'Skip, I'll do this later'** or click on the company name or Home icon. You can always activate/subscribe from within the app. If you don't see 'Your Plan' this means that it has already been subscribed; or taken to trial.

Key Terms

These key terms are essential to the proper interpretation of POPIA and to maintain PrivIQ.

Responsible Party – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information e.g., your organisation.

Information Officer – of a private body means the head of a private body, e.g., the CEO.

Operator – means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, e.g., the external payroll company that does your monthly payroll run.

Personal Information – means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, e.g., name, contact details, location, and **special personal information** such as health status, political persuasion etc.

Data Subject – means the person to whom personal information relates.

Information Owner – an individual that has approved management responsibility for controlling the maintenance, use and security of the personal information

Information Officer

The Information Officer of a private body means the head of that body and **is accountable** for developing, implementing, monitoring and maintaining the organisation's compliance framework.

COMPULSORY STEP – Your organisation's Information Officer must first complete and maintain the checklist called 'Information Officer'

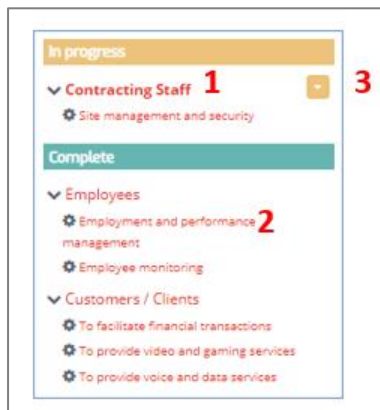
Find the checklist in the Compliance Audit section.

Data Mapping



Remember that saying regarding risk – “you can’t manage it if you can’t see it”? If an individual makes an enquiry about his or her personal information, or there’s a breach in security, you need a detailed map to help you respond. But data mapping is much more than producing an inventory.

This represents the first step towards building a proper foundation upon which to manage your compliance program. The who, why, when, where and what of processing. Throughout the process you may add your own data items, should the default items not be sufficient. It starts with selecting your data subject types and goes all the way through to indicating where you collect the personal information.



1. Who are your organisation’s data subjects? Employees, clients? Select the data subject types and go **Next**.

2. Why do you collect and use their personal information? In other words, the purpose. Click on a data subject type (1) and select the relevant purposes together with the appropriate lawful basis and retention period.

Employment and performance management <input checked="" type="checkbox"/>	S11 - To conclude or perform a contract with t... ▼	Until contract completed ▼
---	---	----------------------------

Click on a purpose (2) then, for each purpose:

Employees / Employment and performance management			
Personal Information Types	Special Personal Information Types	Processing Locations	Data Sharing

- what personal information are you processing
- what sensitive personal information are you processing and what is the lawful basis?
- where are you processing the information within your organisation?
- which Operators are processing the personal information?
- are you sharing the personal information with other Responsible Parties?

A word on granularity


Granularity is important when it comes to In-house processing locations. You don't want to use 'Application Server' when that will be meaningless to someone who manages subject access requests. Add a location that is more descriptive, that enables the person to search the relevant systems or apps. At the same time, you don't want to be overly granular when entering personal information types. Rather than recording every data element in a passport, would it not be better to say, "Passport details"?


If there are commercial sensitivities around having the names of Operators or Responsible Parties on your privacy notices then, add them as category names here and then add them individually in the Operators or Information Sharing sections, respectively. For example, you might not want to use 'Paula's Payroll Services', but rather use 'Payroll Processing Company' instead.

Once you're done with a data subject type, set it to Complete by clicking the orange drop-down (3). When all data subject types are set to Complete, click Next to advance to **Collection Sources**.

Under Collection Sources, click on each personal data type and indicate the collection source and whether it is collected directly from the data subject or indirectly. If indirectly, you must enter the indirect source category e.g. General Practitioner, Credit Bureau etc. The final step is to click 'Finish'. You can use the visualisation tool to confirm the accuracy of your data mapping.

Name	Collected Directly	Collected Indirectly	Indirect source name
Another Responsible Party	<input type="checkbox"/>	<input type="checkbox"/>	
Application form	<input type="checkbox"/>	<input type="checkbox"/>	
Attendance form	<input type="checkbox"/>	<input type="checkbox"/>	

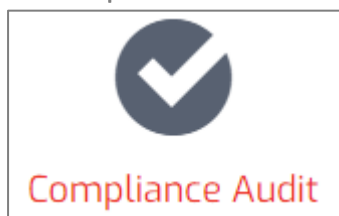
Visualise 

 Previous

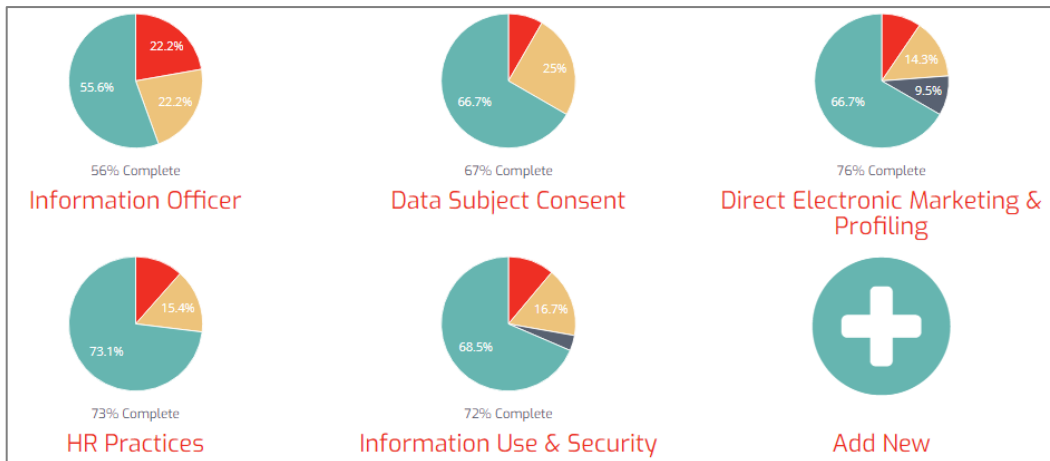
→ Finish

Data mapping will integrate with the **Records of Processing Report** which you will find under Reports in the upper navigation bar.

Compliance Audit



Once data mapping is complete, commence with your compliance audit. There will almost certainly, be risks and issues from data mapping that will be addressed here. Depending on your organisation's structure, you may need to get others involved – the Information Owners, e.g., your HR Manager, IT Manager, Sales Manager etc. Besides the default sections, you may also add your own sections by clicking 'Add New'. Functionality is the same across all checklists.



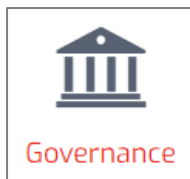
By way of example, let's take a look at 'Security Controls' which you will find under 'Information Use & Security'.

The screenshot shows the 'Security Controls' checklist interface. It includes a 'Person responsible' dropdown (1), tabs for 'Checklist', 'Background', and 'Risk Rankings' (2), and buttons for 'Show all notes', 'CSV template', 'Import items', and 'Add new item' (3). The 'Risk' section has a 'Description' field (6), an 'Assignment' field (4) with a dropdown for 'Abel Adam' and a 'Due' date of '25 Mar 2020', and a 'Status' field (5) with three radio buttons: 'Low Risk', 'Risk', and 'High Risk' (7). The 'Status' field also has a 'Review every' dropdown set to '3 Months' and a 'Set for all' button.

1. You may assign compliance sections to what we call Compliance Users. If not in the drop-down list, add users by clicking the white cross in the green circle.
2. Find useful information in the Background and Risk Rankings tabs.
3. Add your own relevant checklist items individually, or upload using the csv template.
4. Assign checklist items to what we call Task Owners and set a review cycle which triggers notifications to the task owners.
5. Assess your organisation's progress against each checklist item. (Not started; In progress; N/A; Complete)
6. Add notes and upload documents against a checklist item. We also keep track of any changes in Status here.
7. Reset the risk level after you set your Status (in 5.)

Setting items to Complete in the Information Use & Security will also update the **Records of Processing Information Report** which you will find under Reports in the upper navigation bar. You will have the option to edit this content in the Governance section.

Governance

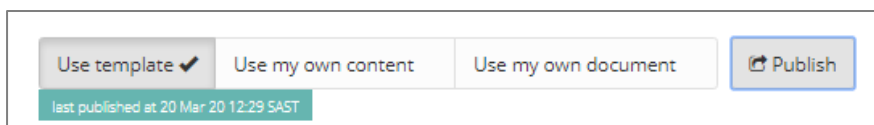


Maintenance of your organisation settings and your data mapping, provides essential information to your privacy notices. And there are documents that you need to share with stakeholders involved with privacy protection.

Privacy Notices



Notice the external privacy notice as well as one for employees.

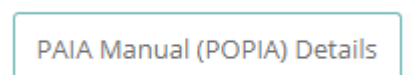


There are 3 options. the template which is updated from organisation settings and data mapping; the editable version where you create your own content; or the option to upload your own PDF. Regardless of the option, you must remember to regularly publish the privacy notice. You will also find the **code that you can embed in your websites** so that when people click on your privacy notice link, they will see whatever you have published here. There is also the option to download your published version in case you share the privacy notice other than via your websites.

Once published, set the status to Completed – this will update your dashboard.



Security Measures



The current PAIA manual (section 51) calls for a general description of information security measures that ensure confidentiality, integrity, and availability. In this section, you will find suggested content based on completion of the Information Use and Security compliance checklists. Instead of the Template, you may also Use your own content. This content will update the Record of Processing Report which is found under Reports in the top navigation bar.

Training & Awareness

Internal

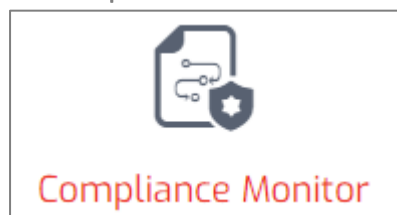
Optional

In these two tabs you can find documents to share with various stakeholders. Some of them have the 'template', 'own version', 'upload' options. If you don't want to share them, mark them as N/A. If you don't see the Optional tab this means you are using an entry level version of the app.

In the Document Library you can edit or upload your own documents. If you want to share them you must tick 'Share with Stakeholders?'

▼ Share with Stakeholders?	▼ Last published	▼ Preference
<input checked="" type="checkbox"/>	12 Feb 20 11:26 SAST	<div>Use my own content ✓ Use my own document</div> <div>Content ✓Delete</div>

Compliance Monitor

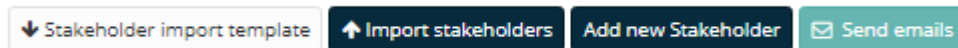


Run this report to keep track of your compliance journey. Use the filter to target specific sections. Download the report in PDF or Excel format. It's a good idea to regularly run and print the full report.




Stakeholder Communications



One of the ways in which to demonstrate compliance with POPIA is by keeping all stakeholders informed of their roles and responsibilities towards privacy protection. In the Governance section you would have selected the relevant documents that you would need to share with your employees, contractors, suppliers and the like. Go to the Compliance section.



You may add a stakeholder individually or use the template to upload. You may send emails globally, i.e. to everyone.

▼ First name	▼ Last name	▼ Job title	
Jacky	Kontacky	Privacy Manager	  

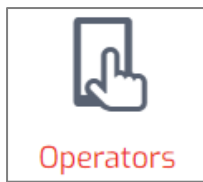
Or you can email individually by clicking the envelope. You can also customise your message to the individuals. They will need to open that document by clicking the link in the email, reading the document and then clicking 'I have read and understand the document'.

(If you are limited by your package size, speak to your PrivIQ vendor)

Employee Privacy Notice	* Personal Information Protection Policy	Acceptable Use Policy
		
		

The red star indicates 'Not started', the orange star means it has been sent but has not been actioned and the green star indicates that the person has clicked 'I have read and understand the document'. Hover over the orange and green stars to see extra info. All activity here will update the Compliance Monitor.

Operators



An Operator is a person/organisation that processes personal information on your behalf, under contract. They cannot use the personal information for their own purposes. An example would be a company that does payroll processing on behalf of your company.

Note that there is a Checklist. Go to Operator contracts. If you added any Operators in data mapping, they will appear here. This is where you maintain the Operator contracts. You could have uploaded your Operators here and they would have been available when you did your data mapping. You can add individually or by using the import template.



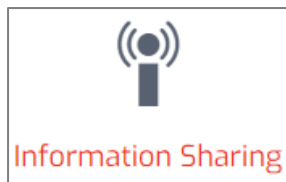
POPIA doesn't say *who* must draw up the contract, only that the Responsible Party (your organisation) must ensure that the written contract stipulates the appropriate security measures that the Operator must establish and maintain. You might well find that some Operators already have the relevant contract *template*.

Lawful basis	Contract Status	Contract	
	Not signed	↓ Template contract	1 Edit
	In progress ✓ 2	Own contract	Delete
	Signed	↑ Upload	
		Signed contract	3 ↑ Upload
Binding corporate rules 4	Not signed ✓	Binding corporate rules	5 Edit
	In progress		Delete
	Signed		

Edit the form (**1**) by completing the contact details, the contract start and end dates, and select the relevant personal information that the Operator will be processing. Set the status (**2**) and Save the form. Once you have the signed contract, upload it here (**3**) – (ignore 'Own contract')

You would have noticed that there is nothing under Lawful basis for our first Operator. That's because, in this example, they are based in South Africa. However, the lawful basis in the second example (**4**) is 'Binding corporate rules – BCRs'. The link (**5**) will display a suggested template for BCRs. What is this about? – **it's important for you to understand Chapter 9 of POPIA.**

Information Sharing



Unlike the 'sharing' of personal information between Responsible Party and Operator (which is under written contract), here we speak of the sharing (or, disclosure) of personal information *between Responsible Parties*. An example might be the organisation providing medical insurance to your employees. In most cases there should already be some sort of agreement acknowledged between the two organisations. Simply upload a copy and set the status to Signed.

The functionality within the app is identical to the Operators section, except that the template we offer is slightly different to the one in the Operators section.

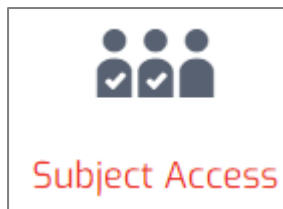
It might help to look at a simple example.

Let's say that a travel agent makes bookings on behalf of its clients with an airline and hotel chain. It's unlikely that the hotel chain and airline would be considered Operators. They are Responsible Parties in their own right. But what if the three companies got together to develop a system or app that would be of value to ALL of their clients? Now we're talking of *further* processing that brings about a **JOINT** sharing relationship – and will almost definitely require data subjects' consent. In fact, all of the other Conditions (principles) come into play. It's important the data subject knows who to approach.

So, you can see the need to have an agreement in place. The template we offer may help you manage a one-way sharing relationship where you share your data subject's personal information with another Responsible Party – but you may need a different template where there are **joint responsibilities** between and among Responsible Parties.

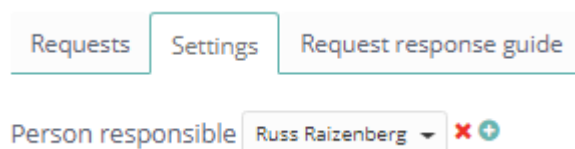
A more sophisticated and potentially, more-risky scenario of personal information sharing will be that of the world of data brokers.

Subject Access

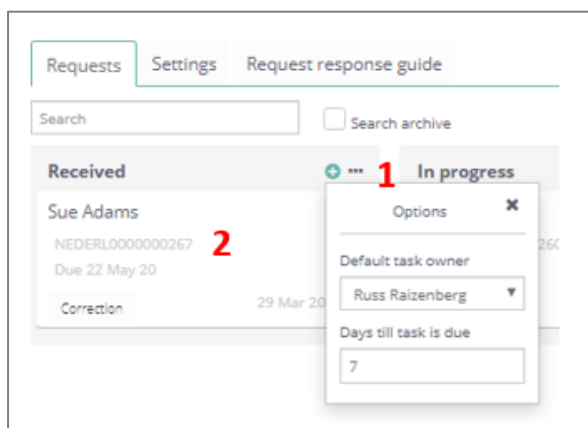


There are a number of reasons why individuals might want to gain access to their personal information and a number of ways in which they can make these requests for access. Equally, there are a number of different responses that could come from your organisation. Much has to do with the interplay between POPIA and PAIA (the Promotion of Access to Information Act).

PrivIQ provides requesters with an online link and allows you to receive or capture the requests, delegate them as appropriate, navigate and understand the rules and gain oversight of progress via a dashboard.



Click Settings and set the 'Person responsible' for receiving online requests. If not in the drop-down, click the white cross in green circle to add new persons.

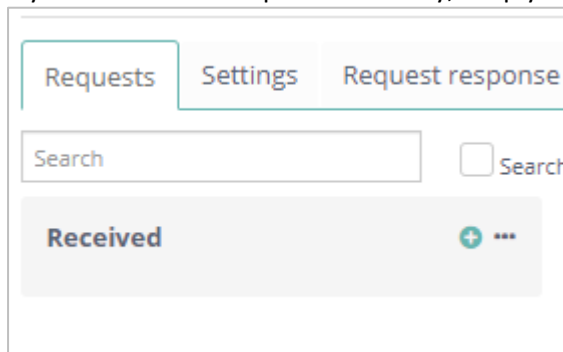


Requests

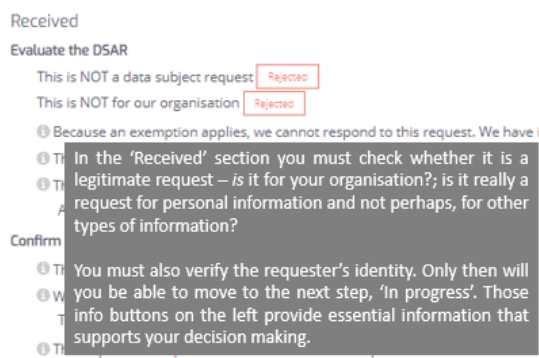
Note the 4 sections i.e. 'Received', 'In progress', 'Complete' and 'Rejected'. In the 'Received' and 'In progress' sections, click on the 3 dots (1) to set the 'Default task owner' and 'Days till task is due'.

Looking at the panel (2) we see that Sue Adams is the requester. Below that is the automatically assigned reference number to be used in communications with the requester. Then there is the due date – which is the date by which you must respond. Of course, this date could change depending on what happens further down the line. 'Correction' is the request type. Finally, there is 29 March 2020 which is the 7 'Days till task is due' date. To capture any manually received requests, click on the white cross in the green circle. Now, click on a panel to start the process.

If you need to add requests manually, simply click the white cross in the green circle.



Received



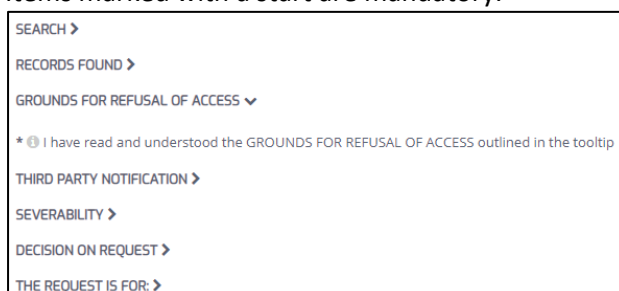
In progress

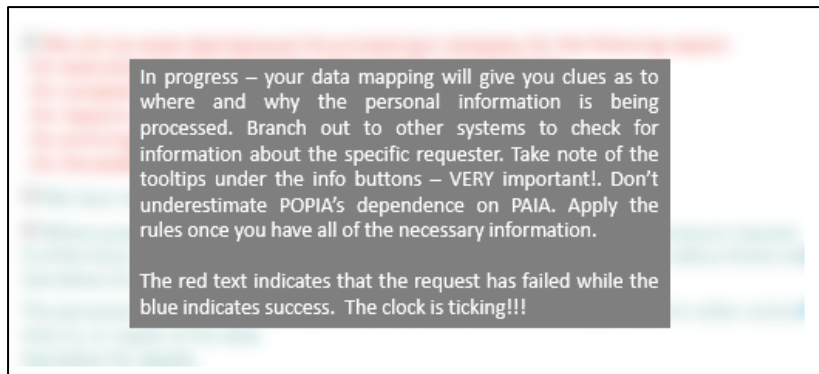


In the top-right corner:

- 1 – add notes to the request
- 2 – upload documents to the request
- 3 – check the history of requests from the requester
- 4 – check your data mapping against this type of requester
- 5 – download the request form

Items marked with a star are mandatory.





Security Compromise



A personal information security compromise could lead to the accidental or unlawful use, destruction, loss, alteration or disclosure of that information – in other words, a breach. A breach, not appropriately responded to, could result in physical, material or non-material stress to data subjects and could well have a financial and/or reputational impact on your organisation.

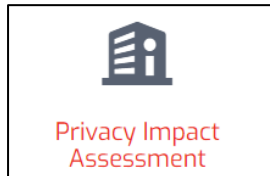
A Responsible Party must inform the Regulator as soon as reasonably possible after becoming aware of a security compromise. The Responsible Party also needs to communicate with data subjects, especially where the exposure presents a high-risk to them. They should also consider the possibility that law enforcement authorities may need to be involved e.g., where there are safety concerns or perhaps, where early disclosure to data subjects could hamper investigations.

Use this section to capture and manage your responses to any incidents as well as communications with the Regulator and data subjects. Ensure that your Operators have a similar process in place. Doing table-top exercises fosters good practice that keeps the relevant staff aware of the processes involved in breach response management. Print those documents as evidence of training and then remove the incidents so that they don't obscure your dashboard.

▼ Status		Documents	
Reported	Incident	Download	Edit Delete
In progress			
Complete ✓			
Reported ✓	Letter to the Regulator	Download	Edit Delete
In progress	Subject notification	Download	
Complete	Incident	Download	

In the above example we have two types – the first where the incident was contained, there was no need to report it and we only needed the incident report. The second is where it had to be reported to both the Regulator and the data subjects impacted – in some cases you may be prevented from informing the data subjects.

Privacy Impact Assessment



In the 2018 Regulations, the Regulator calls for Information Officers to ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.

This is generally interpreted as an assessment on *existing* operations. However, in this section we perform an assessment on processing of personal information that is being *planned* i.e., still in project mode. A Privacy Impact Assessment, PIA – is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to individuals’ resulting from the processing of personal information, by assessing them and determining the measures to address them. PIAs are important tools for Accountability, as they help a Responsible Party to demonstrate that appropriate measures will be or have been taken to ensure compliance with POPIA.

We have followed a global model so, most suggestions in the section on ‘Screening questions’ might not be relevant at this stage, but likely to be so in the future.

Some examples of where a PIA may be required:

A hospital processing its patients' genetic and health data

The use of a camera system to monitor driving behaviour on highways. The data controller envisages to use an intelligent video analysis system to single out cars and automatically recognise license plates

A company monitoring its employees' activities, including the monitoring of the employees' workstation, internet activity, etc

The gathering of public social media profiles data to be used by private companies generating profiles for contact directories

In some instances where the processing might require prior consultation with the Regulator

Click:

Add New

Enter the PIA Name, Description and Project due date. Click **Save**

Overview

PIA Name

Health & Wellness Services

Project due date

25 May 2021

Project status

Draft

Description of assessment

Description

Project owners

Russ DEPT

Reviewers

James Reviewer

Approver

Jane Approver

Save

Cancel

The Project owner is *usually* the person compiling and editing the PIA.

Select the **Reviewer(s)** or add any not in the drop-down list (click the white square in the green circle).

Reviewers can only be Compliance Users or Task Owners.

Select the **Approver(s)**. Approvers must be Administrator type users.

The Privacy Lead's comments in the PIA will be recorded as such. Indicate which user is the privacy lead under Organisation /Users.

Active ☒

Is Privacy Lead ☒

Screening Questions

By selecting an option under screening questions, you're suggesting that a PIA is not relevant or required. The rest of the PIA falls away. However, you still need to send it for approval.

Overview

Screening questions

Purpose

Overview

Screening questions

Purpose

Processing justification

Individual's rights

In this section, you indicate why the PIA is relevant to this project or planned processing of personal information. Note that you may add comments or upload documents.

☐



Notes

Processing justification

Overview

Screening questions

Purpose

Processing justification

Individual's rights

Personal information must be adequate, relevant, and limited to what is necessary in relation to the purposes for which the personal information is processed.

Click:

Add new process

...and add the relevant processes.

Individual's rights

Overview	Screening questions	Purpose	Processing justification	Individual's rights
----------	---------------------	---------	--------------------------	---------------------

Section 5 of POPIA states that a data subject has the right to have personal information processed in accordance with the conditions for the lawful processing of personal information. How is the processing respecting those rights?

Then submit those sections either for Review (first) or for Approval (last).

James Reviewer ▼	Submit for review	Jane Approver ▼	Submit for approval
------------------	-------------------	-----------------	---------------------

After inserting their comments, they have the options to return the PIA for improvement or the Approver can approve the sections.

Risks and Mitigations

This then reveals the Risks and mitigations tab to the PIA owner.

Overview	Screening questions ✓	Purpose ✓	Processing justification ✓	Individual's rights ✓	Risks and mitigations
----------	-----------------------	-----------	----------------------------	-----------------------	-----------------------

The PIA owner will then add all risks and associated mitigations to arrive at an overall residual risk. This will be sent for final approval.

Overview	Screening questions ✓	Purpose ✓	Processing justification ✓	Individual's rights ✓	Risks and mitigations	Negligible ✓	Approval ✓
----------	-----------------------	-----------	----------------------------	-----------------------	-----------------------	--------------	------------

The final approver will then complete the Approval tab before returning it to the owner, who may then move the PIA to Complete or move it to the Submitted column where engagement with the Regulator is necessary. Note that a PIA may be opened for editing where it will then be placed into the procedure as outlined above.

Upon final approval, identified risks must be incorporated into your risk management framework.

User Maintenance

Add and manage users under Organisation / Users. Preferably, add Compliance Users and Task Owners in the relevant Compliance sections.

To provide an extra layer of security, we've added multi-factor authentication (MFA).

New users will receive a welcome email, inviting them to login with a temporary password and then changing their password. You can choose to either receive a verification code via SMS which you will enter along with password. Or, preferably, you can use an authenticator, such as Authy, Google Authenticator (iOS/Android) or Microsoft Authenticator, that will read a QR code and generate the verification code to enter with your password.

Glossary

Data Subject – means the person to whom personal information relates.

Information Owner – an individual that has approved management responsibility for controlling the maintenance, use and security of the personal information

Information Officer – of a private body means the head of a private body, e.g., the CEO, and of a public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of PAIA (don't confuse this with the Chief Information Officer – an IT role)

Information Owner - an individual that has approved management responsibility for controlling the maintenance, use and security of the personal information

Operator – means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party, e.g., the external payroll company that does your monthly payroll run.

MFA – Multi Factor Authentication

Personal Information – means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, e.g., name, contact details, location, and special personal information such as health status, political persuasion etc.

PIA – Privacy Impact Assessment

POPIA – Protection of Personal Information Act

PAIA – Promotion of Access to Information Act

Responsible Party – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information e.g., your organisation.