privIQ

South Africa
Onboarding Guide

Contents

Implementation Guide 2

Organisation Setup 3

Key Terms 3

Information Officer 3

Home Page 4

Data Mapping 5

- A word on granularity 5
- Data mapping is done in phases: 6

Governance 8

- Privacy Notices 8
- Integration 8
- Training & Awareness 9
- Record of Processing 9
- Automated Decision Making 9

Stakeholder Communications 10

Compliance Audit 11

Compliance Monitor 12

Information Sharing 14

Subject Access 15

- Settings 15
- Online subject access request form 15
- Requests 16
- Received 16
- In progress 17

Security Compromise 18

Privacy Impact Assessment 20

- Screening Questions 21
- Purpose 21
- Processing justification 22
- Individual's rights 22
- Risks and Mitigations 23
- Final Approval 23

Dashboard 24

- User Maintenance 24

Glossary 25

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, in which applications do they process 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).

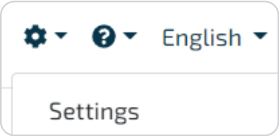
9. Following point 2. above, Information Owners to review and understand ALL processing of personal information in their respective departments. Be aware of and record all informal processing too. For example, populating spreadsheets to manage processes outside of the formal, networked and security protected systems and apps.

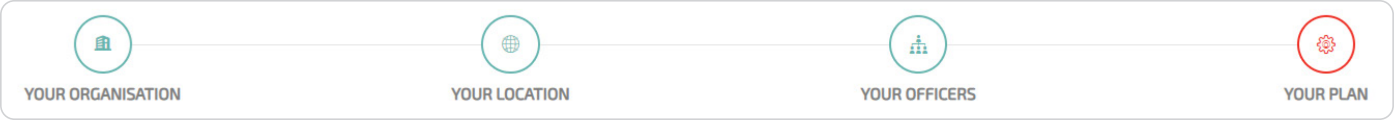
10. Begin the data mapping exercise, using the prep work done by the Information Owners and record any work to be done beyond this session. The head of IT could provide valuable insight or guidance especially around any processing of personal information that may be outsourced to **Operators** as well 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.

Follow the steps as indicated by the various sections below – remember, **compliance is on-going.**

Organisation Setup

To get to Settings, click the wheel 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. Ensure that you register the Information Officer with the Regulator.

Under 'Your Plan' you will find the settings and features that determine your package size. Be aware of switching between data mapping by department. **Any data mapping done prior to your switching will be lost.**

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

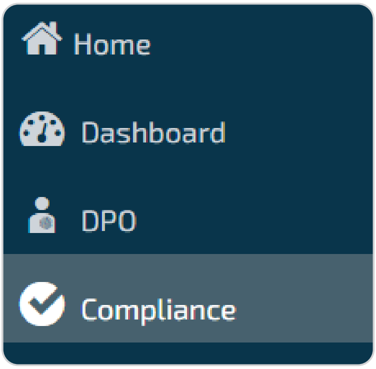
The Information Officer of a private body means the head of that body and **is accountable** for developing, implementing, monitoring, and maintaining the organisation's compliance framework.

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

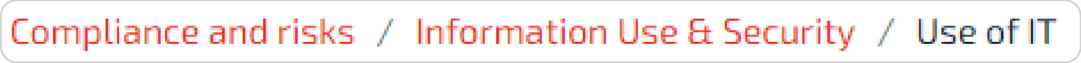
Find the checklist in the Compliance Audit section.

Home Page

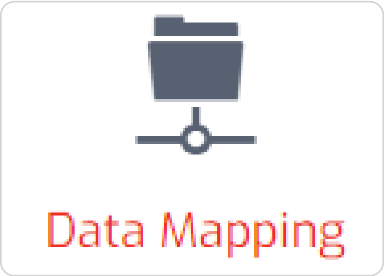
The features you see on the home page will be those that were selected under Your Plan in the Organisation Settings. When switching between different sections you are encouraged to use the sidebar.



At other times it might be convenient to click on the breadcrumb, as in the below picture where you're simply moving 1 level back to 'Information Use & Security'.


Compliance and risks / Information Use & Security / Use of IT

Data Mapping



Remember that saying regarding risk – “you can’t manage it if you can’t see it”? If people make enquiries about their personal information, or there’s an incident, 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.

Information owners must direct the data mapping and be involved throughout the process. Identify any informal processing and record it in the data mapping. These are typically the areas of vulnerability, and any risks or issues should be documented and managed in the relevant compliance section.

A word on granularity

Granularity is important when describing your processing purposes. Don’t crowd many types of processing into a singular description, especially where there are different types of personal information, and different **Operators**. 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”?

Granularity is also 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 when searching for personal information to be used in response to a subject access request.

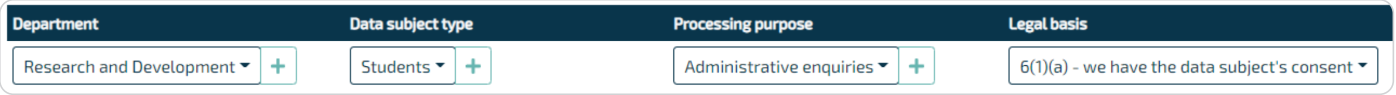
If there are commercial sensitivities around having the names of **Operators or Responsible Parties** on your privacy notices then, add them as category names here and then add them individually in the Operators or Information Sharing sections, respectively. For example, you might not want to use ‘Paula’s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

Data mapping is done in phases:

In our example, we're doing data mapping by department.

Record the 'who' and 'why'

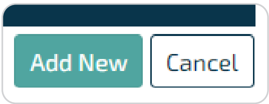
To begin, select the relevant data elements from the drop-down lists (or add new elements by clicking the green cross).



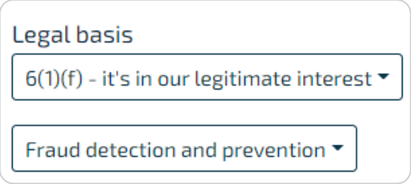
Department	Data subject type	Processing purpose	Legal basis
Research and Development ▾ +	Students ▾ +	Administrative enquiries ▾ +	6(1)(a) - we have the data subject's consent ▾

Select the department, data subject type (WHO), processing purpose (WHY) and lawful basis.

Then, clicking 'Add New' will take you to the next step where you describe the 'what' and 'where'.



NOTE: If you select the lawful basis – ***'it's in our organisation's legitimate interest'***, in the next section you must indicate the type of legitimate interest and, you should use the template to complete a legitimate interest impact assessment. This is done to ensure that your organisation's interests don't outweigh those of the data subject.

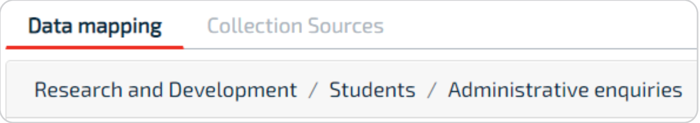


Legal basis

6(1)(f) - it's in our legitimate interest ▾

Fraud detection and prevention ▾

Describe the 'what' and 'where'

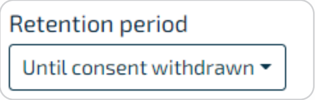


Research and Development / Students / Administrative enquiries

Clicking 'Add New' earlier will open the above box where you will need to:

For this purpose, ...Administrative enquiries...

Enter the **Retention Period** (you may add your own by selecting 'Other'



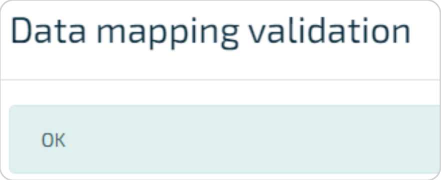
Retention period

Until consent withdrawn ▾

Enter the **Personal Information** types.
Enter the **Special Personal Information** types, including that second lawful basis.
Enter the **Processing locations**, In-house (within the organisation) and, externally by any **Operators.**
Under **Information Sharing**, add any **Responsible Parties** to whom you disclose personal information.
Add relevant **Notes and Files.**

Once you're happy with your input, click 'Validate'.

If you see OK, then you're done with this piece of data mapping. If not, you will be informed as to where to complete your data mapping.



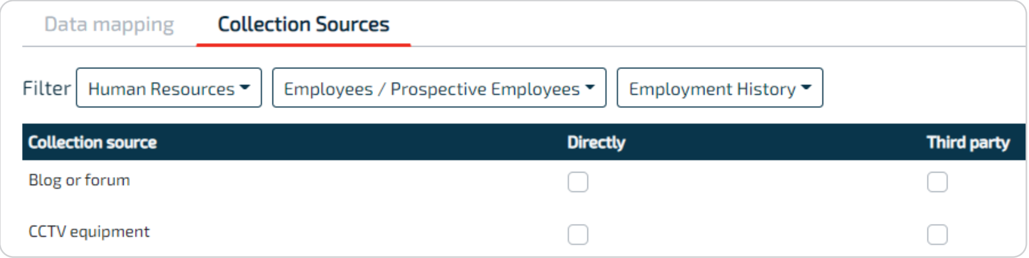
Data mapping validation

OK

Continue data mapping for the next set of data subject types, purposes etc...

OR, go to Collection Sources.

Identify the collection source



Filter: Human Resources ▾ | Employees / Prospective Employees ▾ | Employment History ▾

Collection source	Directly	Third party
Blog or forum	□	□
CCTV equipment	□	□

After successfully validating each section under Data Mapping, indicate the Collection Source/s for each of the personal data or special category types you selected in the data mapping.

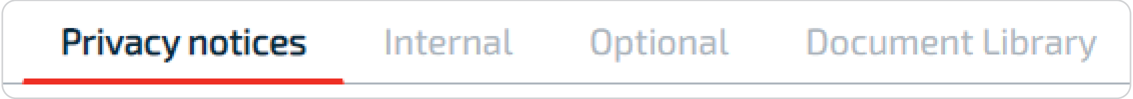
Use the Filter to select the department, data subject type and personal data type. Select the collection source/s and if it's from a Third Party, enter the category of the third party e.g., Credit Bureau.

Click Validate. If there are issues, the validation will inform you as to where the issues are. If you see 'OK', move on to the next set of collection sources.

Data mapping will integrate with the **Records of Processing Report which you will find under Governance.**

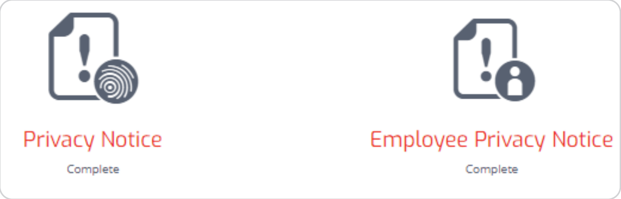
HINT: In Data Mapping and Collection Sources, click 'Visualise' to get an overview of your progress.

Governance

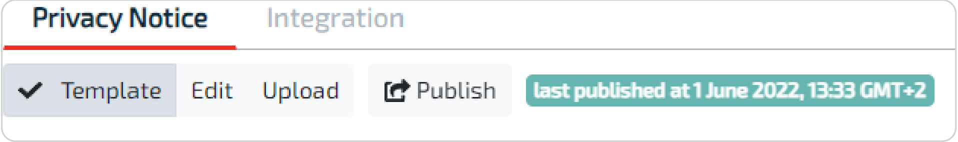


Maintenance of your organisation settings and your data mapping, provides essential information to your privacy notices templates. The Record of Processing must be maintained and there are documents that you need to share with stakeholders.

Privacy Notices



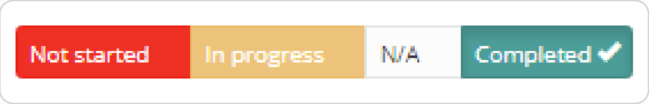
Section 18 of POPIA has specific requirements for notifying individuals when collecting their personal information. The keyword being – *collecting*. Your notice must be displayed at or near the point of collection. Notice the external Privacy Notice as well as one for Employees. Click 'Privacy Notice'.



last published at 1 June 2022, 13:33 GMT+2

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.

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

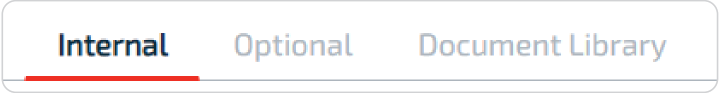


Remember to publish the employee privacy notice too.

Integration

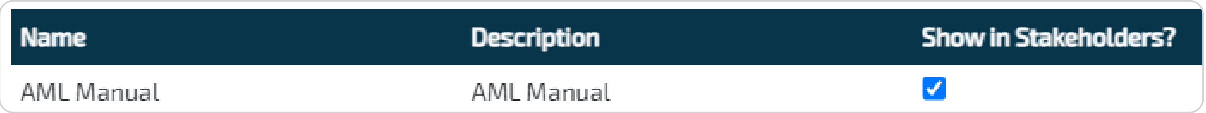
The integration tab is next to the privacy notice tab. Here you will find the **code that you can embed in your websites** so that when people click on your privacy notice link, they will see whatever you have published here. There is also the option to download your published version in case you share the privacy notice other than via your websites. It is unlikely that you will present your employee privacy notice on your websites, but you must publish it before you share with your employees.

Training & Awareness



One of the ways to demonstrate compliance is to show how you have promoted the relevant training & awareness within your organisation. In these tabs you can find documents to share with various stakeholders. Some of them have the 'template', 'own version', 'upload' options. If you are going to share a document with employees and other stakeholders, **you MUST set the document status to 'Complete'**. If you don't want to share them, mark them as N/A.

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



Name	Description	Show in Stakeholders?
AML Manual	AML Manual	☑

Security Measures

The Promotion of Access to Information Act (PAIA) Section 51 provides for a general description of information security measures that ensure confidentiality, integrity, and availability of personal information. In the 'Use template' section, you will find suggested content based on completion of the Information Use and Security compliance checklists. We recommend that you update the 'Use my own content' tab instead of the 'Use template'. Whichever option you choose will automatically update the Record of Processing Report which is found in the next tab on this page.

Record of Processing

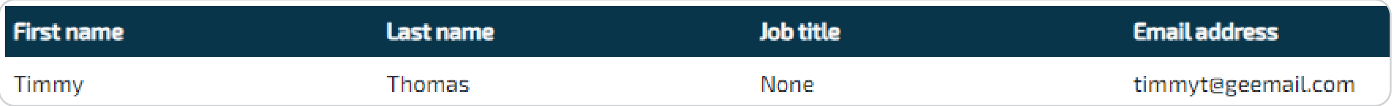
IMPORTANT! – Section 51 of the PAIA (Manual of Private Body) has been amended to include certain information required by POPIA. This report provides that additional information. Ensure that your data mapping is accurate and current. It's a good idea to print and file this report from time to time. Use the content to populate the Regulator's PAIA Manual Template.

Automated Decision Making

Profiling' involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Automated processing implies the exclusion of any human intervention in any decisions which may be taken about such profiling. This is where you inform data subjects of their associated rights as well as the suitable safeguards. Content captured here will update the Template Privacy Notice.

Stakeholder Communications

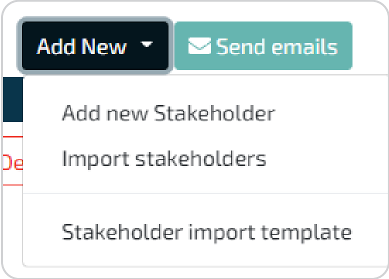
Stakeholders are directly involved in the organisation – managers, employees, directors, trustees etc. One of the ways in which to demonstrate compliance with POPIA is by keeping all stakeholders informed of their roles and responsibilities towards privacy protection. In the Governance section you would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



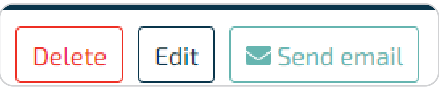
First name	Last name	Job title	Email address
Timmy	Thomas	None	timmyt@geemail.com

NOTE: You will only be able to select documents that have been set as 'Complete' in the Governance section.

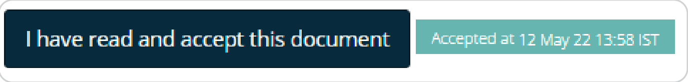
You may add a stakeholder individually or use the template to upload. You may send emails globally, i.e., to everyone.



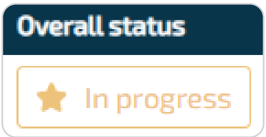
Or you can email individually by clicking the envelope. You can also customise your message to the individuals.



They will need to open that document by clicking the link in the email, reading the document, and then clicking 'I have read and accept this document'.

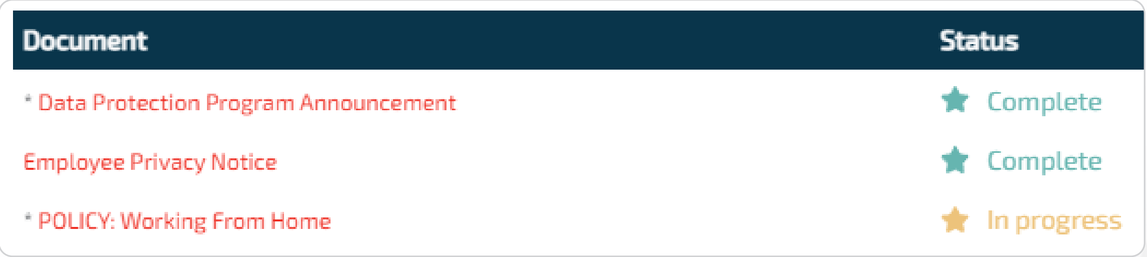

I have read and accept this document
Accepted at 12 May 22 13:58 IST

The overall status appears next to each name.



Overall status
★ In progress

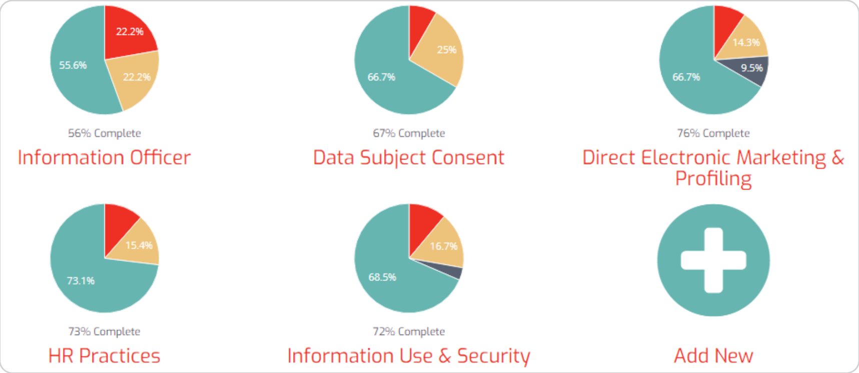
If you click on a name, you will see the status of each document. A red star means the document has not been sent. A yellow star means it has been sent but there is no response. A green star means the employee has accepted the document. Hover over the stars to see the meta-data.



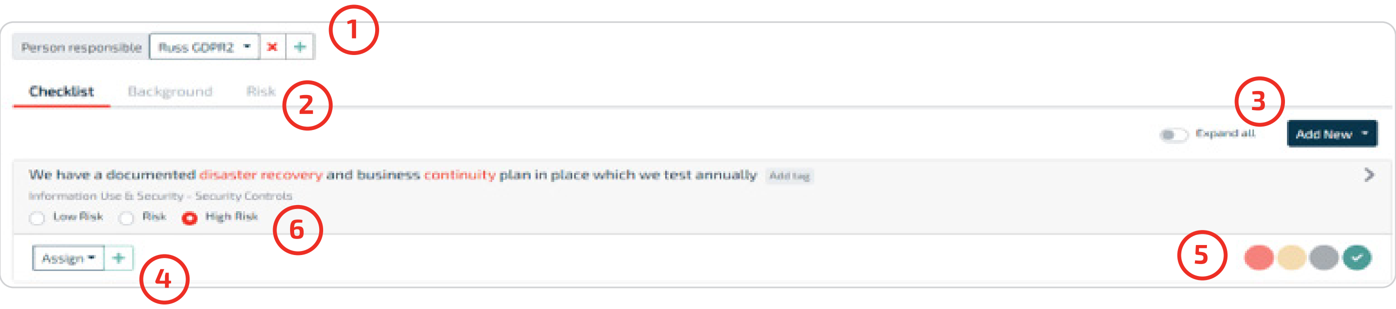
Document	Status
* Data Protection Program Announcement	★ Complete
Employee Privacy Notice	★ Complete
* POLICY: Working From Home	★ In progress

Compliance Audit

Operations involving the processing of personal information require regular review, assessment, and maintenance. 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. When you do your data mapping you will almost certainly uncover operational risks and issues that need to be managed. If these are not covered by the default sections and tasks, you may add your own sections and tasks.



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



Person responsible: Russ GDPR2

Checklist | Background | Risk

Expand all | Add New

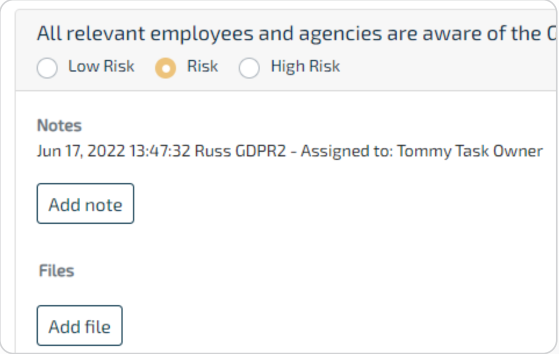
We have a documented disaster recovery and business continuity plan in place which we test annually

Information Use & Security - Security Controls

○ Low Risk ○ Risk ● High Risk

Assign

1. You MUST assign all compliance sections to Compliance Users. If not in the drop-down list, add users by clicking the green cross. A compliance user only sees sections assigned.
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 Task Owners and, **most importantly, 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. Reset the residual risk level after you set your Status (in **5.**).



All relevant employees and agencies are aware of the C

○ Low Risk ● Risk ○ High Risk

Notes

Jun 17, 2022 13:47:32 Russ GDPR2 - Assigned to: Tommy Task Owner

Add note

Files

Add file

NOTE: By clicking the drop-down arrow on the right, the task owner can add audit notes and upload documents in support of the review.

Setting items to Complete in the Information Use & Security will also update the Records of Processing Information Report which you will find under Governance.

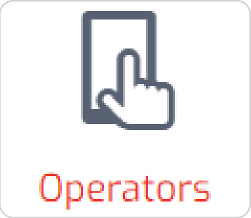
BIG TIP: By clicking the white cross in the green circle, you may add your own sections and checklist items in each section. This feature is especially useful where you need to manage risks and issues you identify during the onboarding procedure or during normal operations.

Compliance Monitor

Compliance Monitor

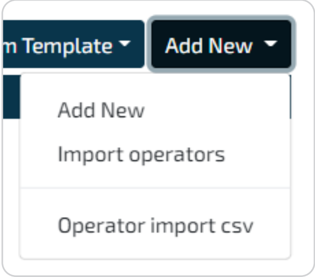
Run this report to keep track of and report on your compliance journey. Use the filter to target specific sections. Download the report in PDF or Excel format. It's a good idea to regularly run and print the full report.

Operators

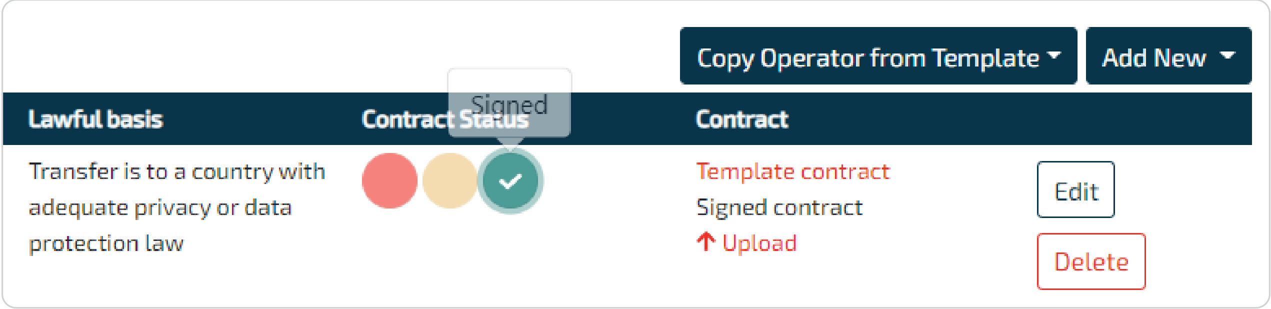


An Operator is a person/organisation that processes personal information on your behalf, under contract. They cannot use the personal information for their own purposes. An example would be a company that does payroll processing on behalf of your company.

Note that there is a Checklist. Go to Operator contracts. If you added any Operators in data mapping, they would 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.



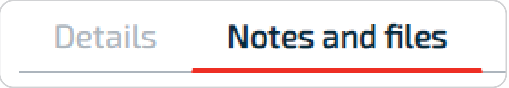
POPIA doesn't say who must draw up the contract, only that the Responsible Party (your organisation) must ensure that the written contract stipulates the appropriate security measures that the Operator must establish and maintain. You might well find that some Operators already have the relevant contract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



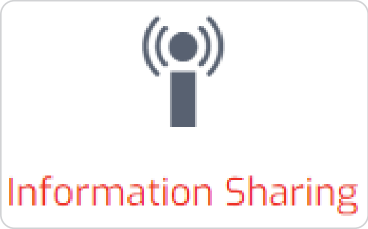
Lawful basis	Contract Status	Contract	
Transfer is to a country with adequate privacy or data protection law	● ● ✓	Template contract Signed contract ↑ Upload	Edit Delete

Edit the form to insert relevant information about the Operator. If the Operator country is outside South Africa, indicate the lawful basis that applies to the export of the personal information. Upload the signed contract and set the status to 'Signed'. **For exports of personal information outside South Africa, it's important for you to understand Chapter 9 of POPIA.**

New feature – when you Edit an Operator you may now add Notes and Files to every Operator.



Information Sharing



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 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 the other Conditions (principles) come into play. It's important the data subject knows who to approach.

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

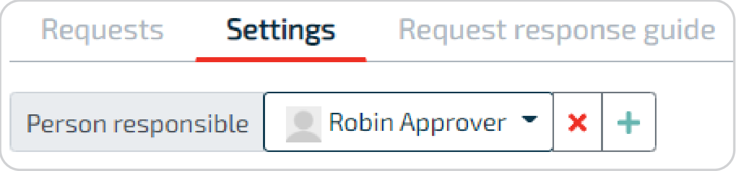
New feature – when you Edit a Responsible Party under Information Sharing you may now add Notes and Files to every Responsible Party.

Subject Access

There are several reasons why individuals might want to gain access to their personal information and several ways in which they can make these requests for access. Equally, there are several 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.

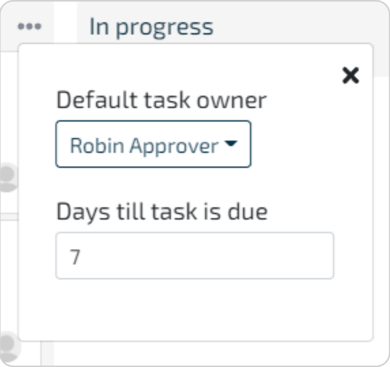
Settings



Person responsible: Robin Approver

Click Settings and set the 'Person responsible' for receiving online requests. If not in the drop-down, click the green cross to add new persons. The 'Person responsible' **must set the Notification Preference to be notified** when an online subject access request is received. To do this, click the drop-down under the username in the top right corner.

The 'Received' and 'In progress' sections have 3 dots. Set the default task owner and the number of days within which the default task owner must respond.



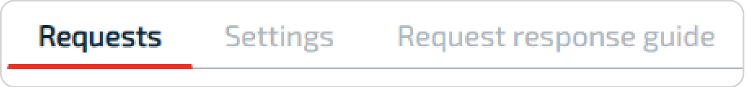
Default task owner: Robin Approver

Days till task is due: 7

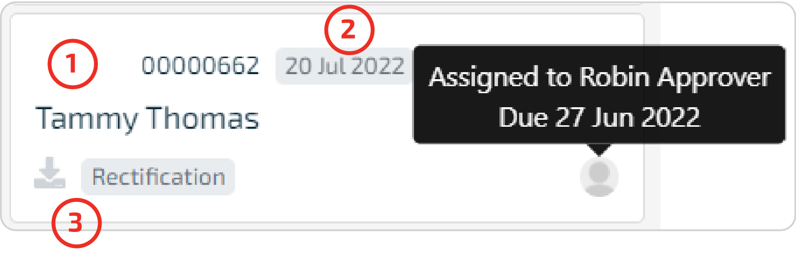
Online subject access request form

Still under Settings – ask your web developer to embed the code behind a link on your website – name it something relevant like 'Subject Access Requests'. Add the domains from where you will be calling this link. Click 'Preview' to see how it will present to the requester.

Requests



Online requests are auto-received here. You may add requests manually by clicking Add New

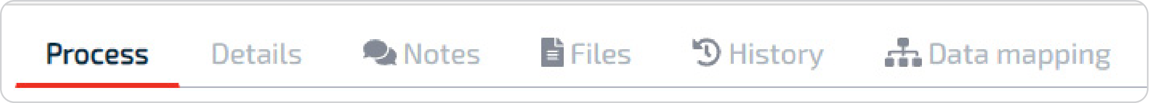


00000662 20 Jul 2022

Tammy Thomas

Assigned to Robin Approver
Due 27 Jun 2022

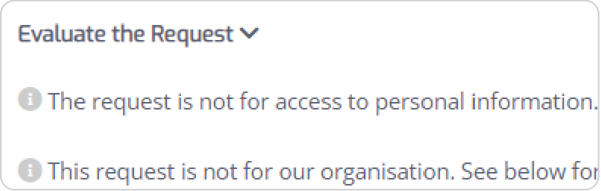
Looking at the panel above, we can see the automatically assigned reference number **(1)**, the due date **(2)** and the download button, **(3)**



Click a panel to enter. In 'Process' you will notice the 3 stages – **Received, In Progress, and Complete.**

Received

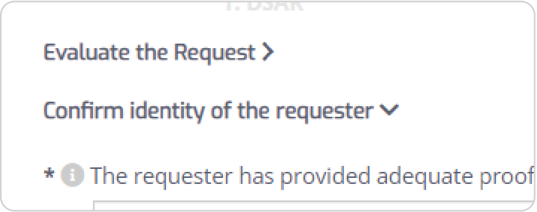
Evaluate the request as there may be reasons why you wish to reject it.



The request is not for access to personal information.

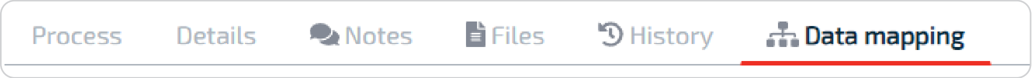
This request is not for our organisation. See below for

If it's a legitimate request, indicate how you have proven the identity of the requester. As soon as you tab out of that field, the Move to In Progress button is revealed.



* The requester has provided adequate proof

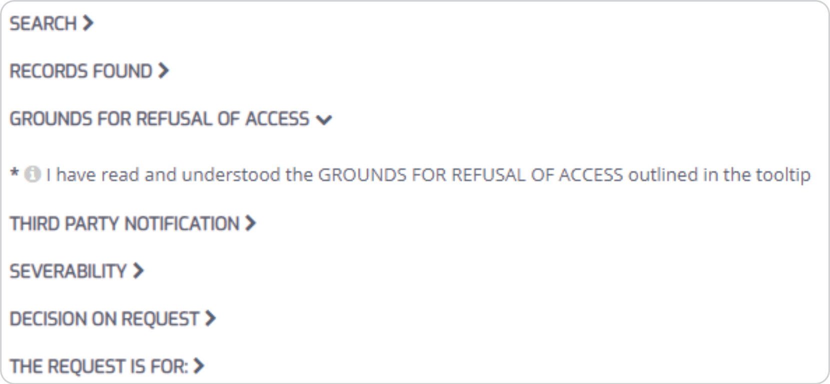
In progress



If your data mapping is accurate and current, it should give you clear indication of where to search. If you think any of the data mapping appears vague, inform your privacy manager. For example, if a processing location suggested 'Application Server', it might be useful to name the application instead.

Once you have all the data to support your decision, step through the rules. Any rule with a star * is mandatory. **The blue text indicates the request is successful and the red text means it has failed.**

The tooltips (i) give you important information on POPIA's dependence on PAIA. **You must understand PAIA's conditions before you acknowledge the steps in this section.**



SEARCH >

RECORDS FOUND >

GROUNDS FOR REFUSAL OF ACCESS ⌄

* ⓘ I have read and understood the GROUNDS FOR REFUSAL OF ACCESS outlined in the tooltip

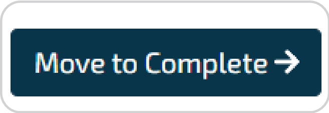
THIRD PARTY NOTIFICATION >

SEVERABILITY >

DECISION ON REQUEST >

THE REQUEST IS FOR: >

If you have followed the steps correctly, you'll be able to move the request to the Complete column.

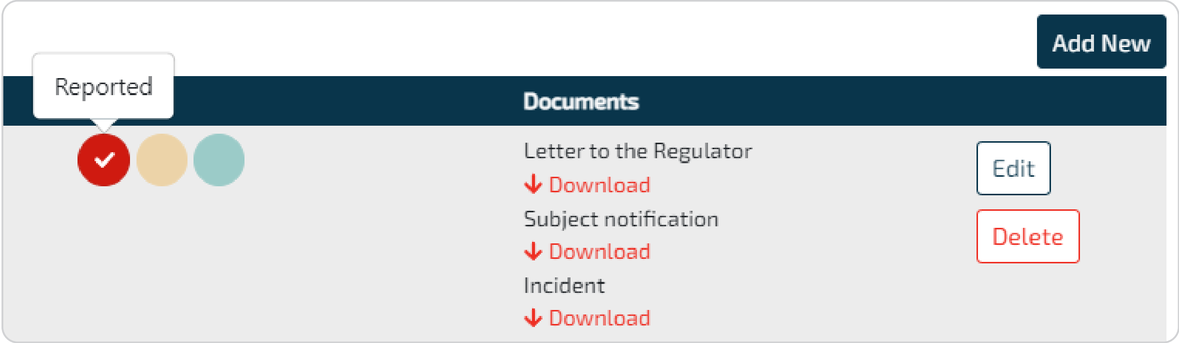


Security Compromise

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.

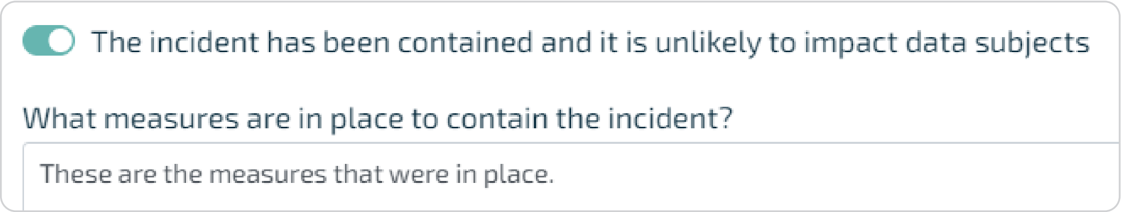
Use this section to capture and manage your responses to any incidents as well as communications with the Regulator and data subjects. Ensure that your Operators have a similar process in place. Doing table-top exercises fosters good practice that keeps the relevant staff aware of the processes involved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



Click Add New

Read the Introduction, followed by some background into Containment & Recovery. Fill in the details required for the Incident title, followed by the Incident details.

Next, we're at the Risk Assessment step.



The incident has been contained and it is unlikely to impact data subjects

What measures are in place to contain the incident?

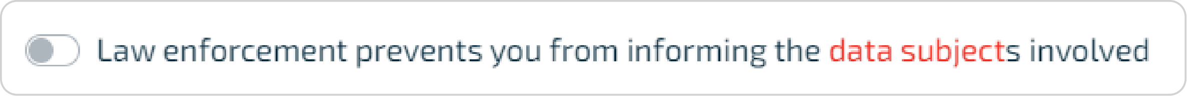
These are the measures that were in place.

Move to the final step which is the Incident evaluation and response. Clicking 'Finish' takes you back to the register and you will notice that it is only the Incident Report that is produced.

However, if the incident hasn't been contained you will move through the steps until you get Notification to the Regulator. Here you will find all the content which is based on your prior input. Use this information in your engagement with the Regulator.

The next page is the content based on your prior input and should inform your communications with those data subjects who may be affected by the incident.

NOTE: Law enforcement – If you had selected this item under the Risk Assessment, the content you would normally use to communicate with data subjects will not be displayed.



Law enforcement prevents you from informing the data subjects involved

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 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.

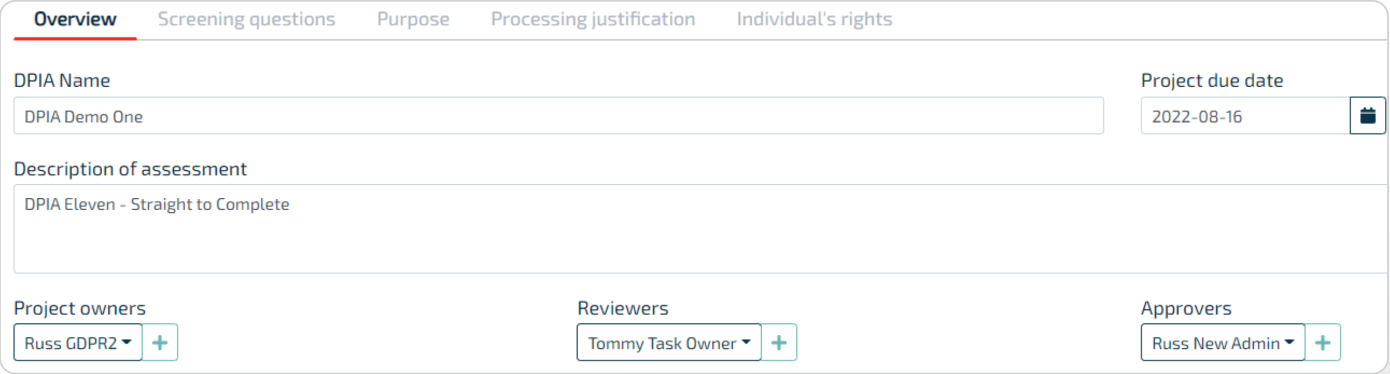
We have followed a global model so, most suggestions in the section on 'Screening questions' might not be relevant at this stage, but likely to be so in the future.

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:

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



DPIA Name: DPIA Demo One

Project due date: 2022-08-16

Description of assessment: DPIA Eleven - Straight to Complete

Project owners: Russ GDPR2

Reviewers: Tommy Task Owner

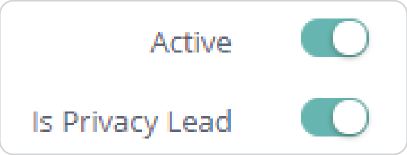
Approvers: Russ New Admin

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 green cross). Reviewers can only be Compliance Users or Task Owners.

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

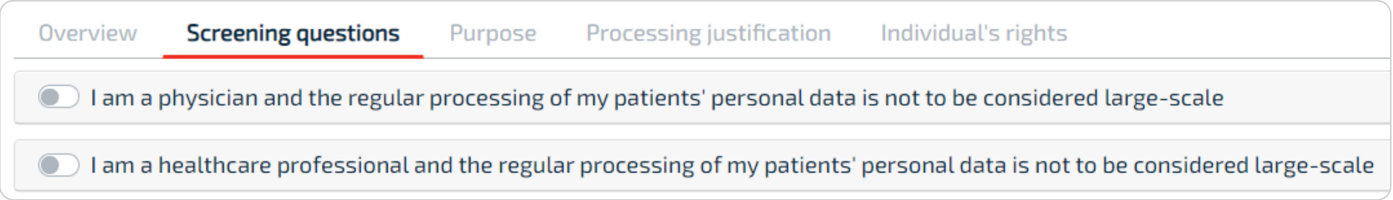
The Privacy Lead's comments in the PIA will be recorded as such. Indicate which user is the privacy lead under Organisation /Users.



Active ☑

Is Privacy Lead ☑

Screening Questions



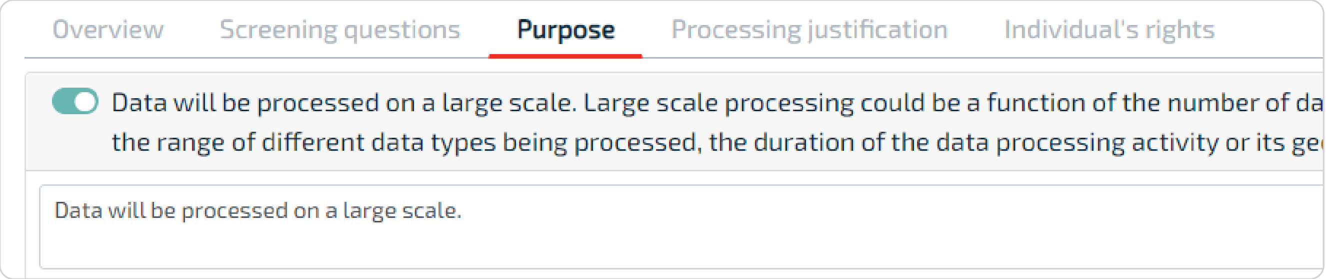
☐ I am a physician and the regular processing of my patients' personal data is not to be considered large-scale

☐ I am a healthcare professional and the regular processing of my patients' personal data is not to be considered large-scale

CAUTION: Most scenarios here probably don't apply in POPIA.

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.

Purpose

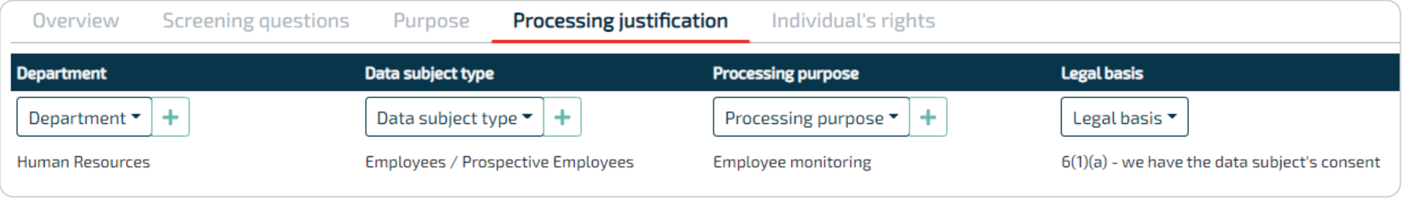


☑ Data will be processed on a large scale. Large scale processing could be a function of the number of da the range of different data types being processed, the duration of the data processing activity or its ge

Data will be processed on a large scale.

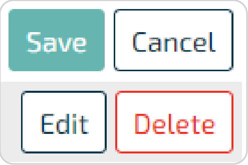
In this section, you indicate why the PIA is relevant to this project or planned processing of personal data. Add comments or upload documents by clicking 'Notes and Files'. You may add your own reason for conducting a PIA.

Processing justification

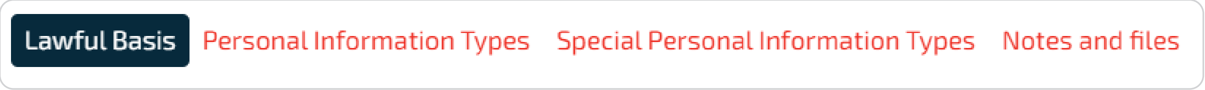


Department	Data subject type	Processing purpose	Legal basis
Department ▾ +	Data subject type ▾ +	Processing purpose ▾ +	Legal basis ▾
Human Resources	Employees / Prospective Employees	Employee monitoring	6(1)(a) - we have the data subject's consent

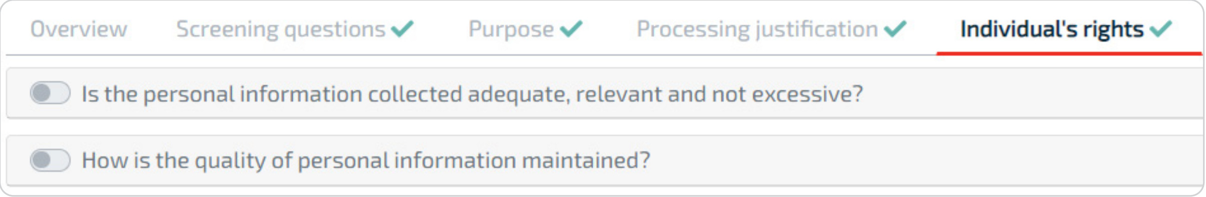
Select the relevant department / data subject type / processing purpose and legal basis. Then click **Save**.



In the next panel, complete the mandatory fields, enter the relevant personal information types, add any notes and files, and then click Close.


Lawful Basis
Personal Information Types
Special Personal Information Types
Notes and files

Individual's rights

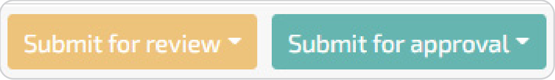


○ Is the personal information collected adequate, relevant and not excessive?

○ How is the quality of personal information maintained?

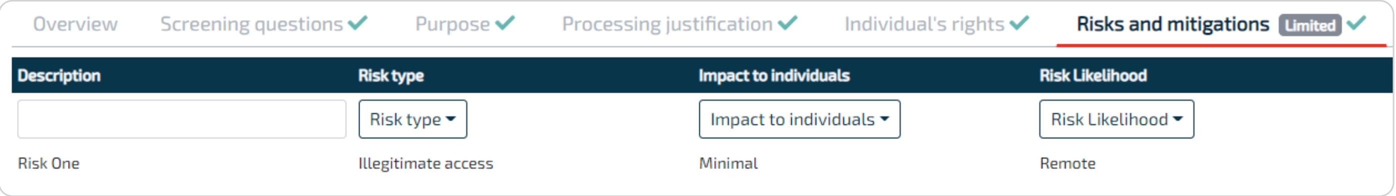
Section 5 of POPIA states that a data subject has the right to have personal information processed in accordance with the conditions for the lawful processing of personal information.

This section concerns data subjects' rights and **how those rights will be protected**. Once you have completed this section, you're now ready to submit the PIA for Review (first) and for Approval (last). The reviewer and approver will receive notifications informing them of the task. After inserting their comments, the reviewer may return the PIA for improvement, or the Approver can approve the sections.



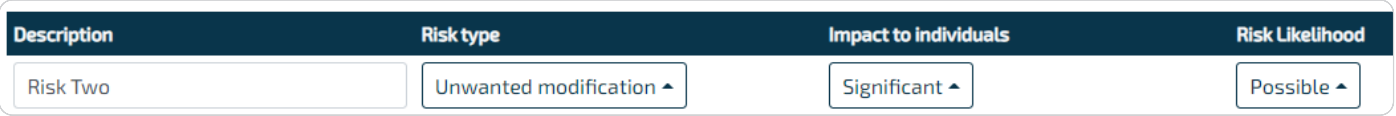
Risks and Mitigations

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



Description	Risk type	Impact to individuals	Risk Likelihood
	Risk type ▾	Impact to individuals ▾	Risk Likelihood ▾
Risk One	Illegitimate access	Minimal	Remote

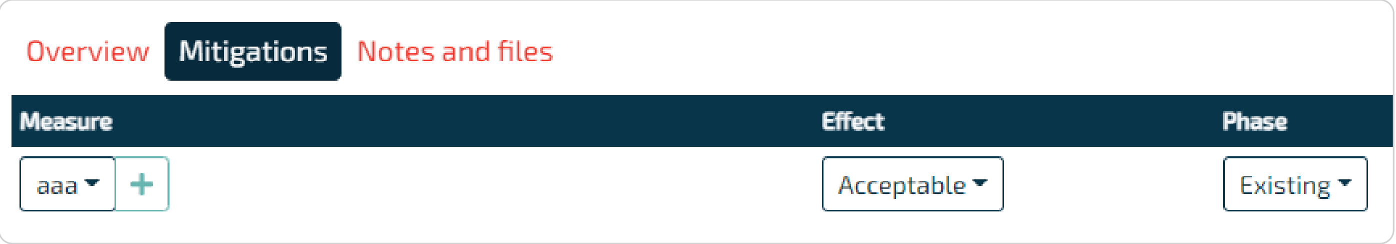
The PIA owner will then add a relevant risk and click Save.



Description	Risk type	Impact to individuals	Risk Likelihood
Risk Two	Unwanted modification ▴	Significant ▴	Possible ▴

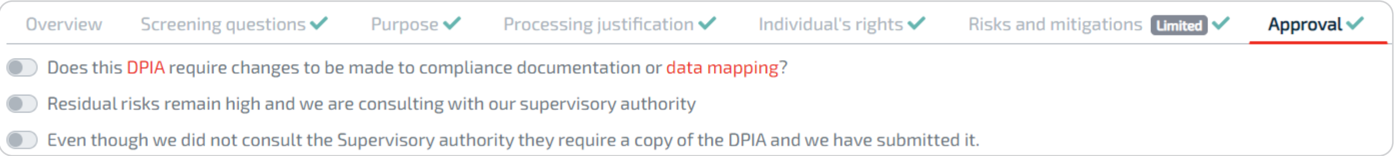
Then add an associated mitigation.

NOTE: If a mitigation has been added, it cannot be edited – it must be deleted and then replaced by the correct mitigation.



Measure	Effect	Phase
aaa ▾ +	Acceptable ▾	Existing ▾

When all risks and mitigations are captured, submit the DPIA for approval.



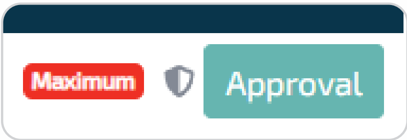
○ Does this DPIA require changes to be made to compliance documentation or data mapping?

○ Residual risks remain high and we are consulting with our supervisory authority

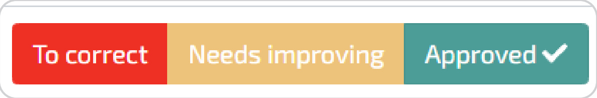
○ Even though we did not consult the Supervisory authority they require a copy of the DPIA and we have submitted it.

Final Approval

Approve each risk individually by clicking 'Approval' to the right. Click Close and return to the main approval page.



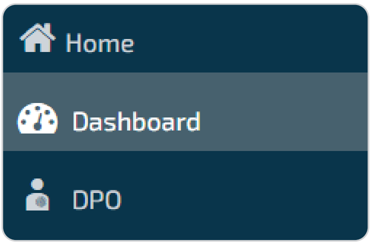
Then approve the risks overall by adding comments and the approval at the bottom of the page and submit to the owner.



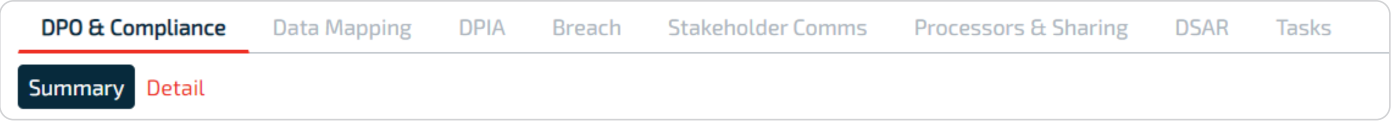
There are 2 possible outcomes after final approval. The owner could move the PIA to Complete where those identified risks must be incorporated into your projects risk management framework or move it to the Submitted column where engagement with the Regulator.

Dashboard

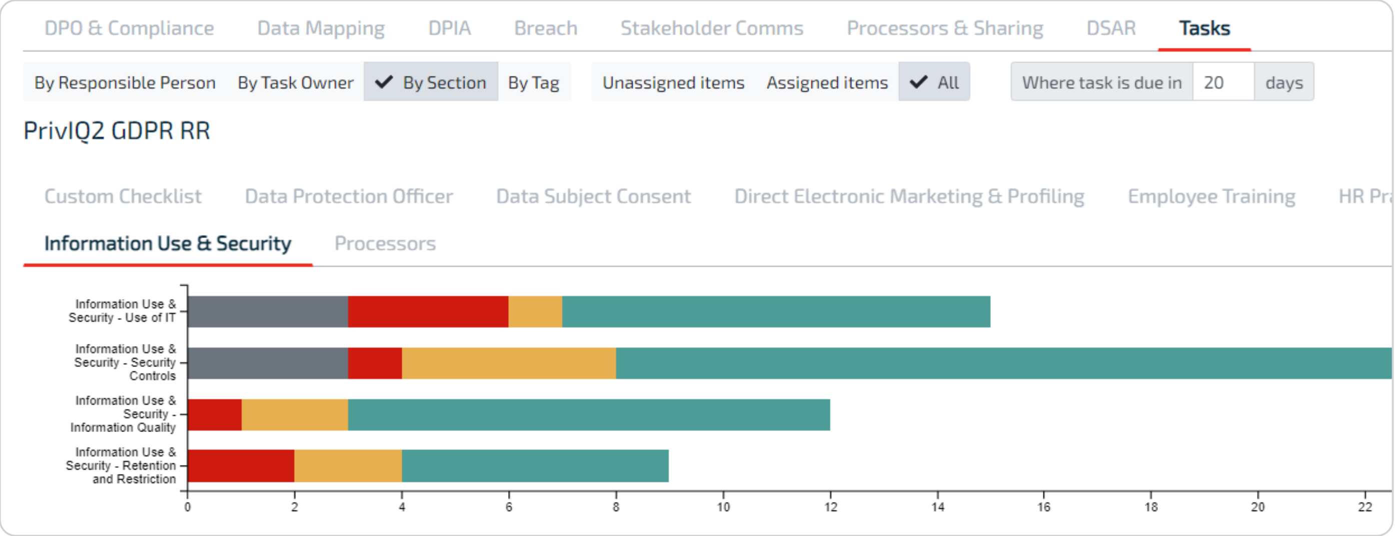
Find the dashboard icon in the sidebar.



You may view across the various sections.



When you view tasks by task owner, click on the task owner to see which tasks have been assigned to the task owner.



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.