

# PrivIQ POPIA Product Overview

---

*Intelligent Compliance, Simply*



**Data Privacy is one of the most important topics of the decade as we move to a digital economy.**

## Gartner

“By 2023, 65% of the world’s population will have its personal information covered under modern privacy regulations, up from 10% today.”

“By 2023, companies that earn and maintain digital trust with customers will see 30% more digital commerce profits than their competitors.”

“By 2024, more than 80% of organisations worldwide will face modern privacy and data protection requirements.”



# A comprehensive Data Privacy program will increase your profits and valuation.

Achieving positive returns on privacy investments.

“Most organisations are seeing positive returns on their privacy investments, and more than 40% are seeing benefits at least twice that of their privacy spend.”

\* Cisco Data Privacy Benchmark Study 2020

### Business impact of privacy

Percentage of companies getting significant benefits in each area, N=2549



Reducing sales delays



Mitigating losses from data breaches



Enabling agility and innovation



Achieving operational efficiency from data controls



Making company more attractive to investors



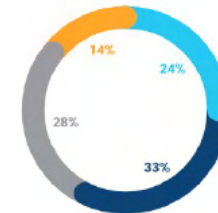
Building loyalty and trust with customers

Source: Cisco 2020 Data Privacy Benchmark Study

### Annual privacy spending overall and by company size

N=2549

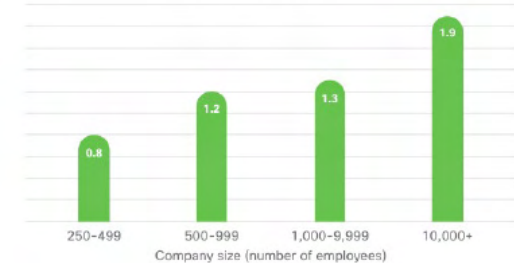
Spending (all companies)  
Average = \$1.2 M



0 to \$500k    \$1M to \$2M  
\$500k to \$1M    Over \$2M

Source: Cisco 2020 Data Privacy Benchmark Study

### Average spending (\$M)





## Our Purpose

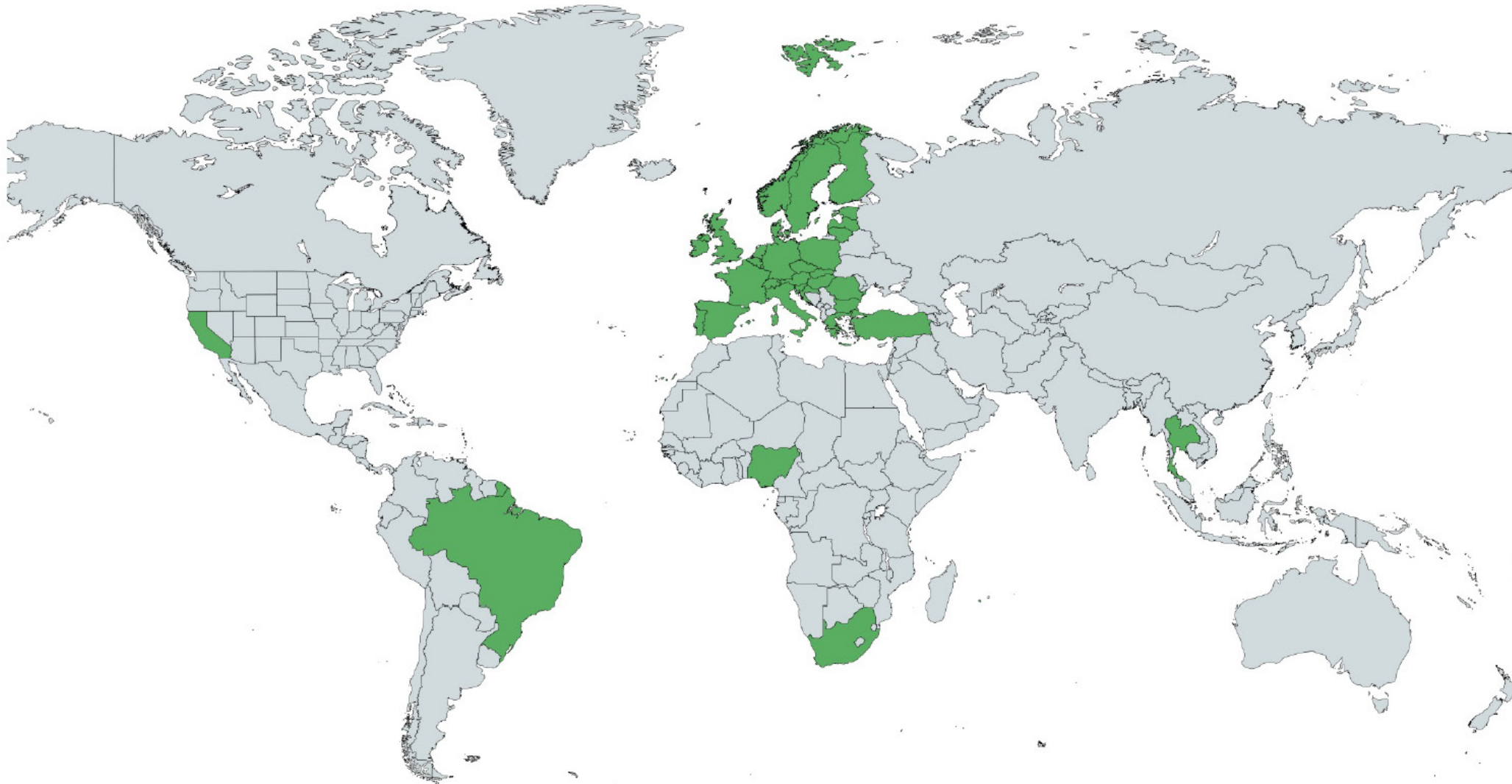
To provide privacy compliance management SAAS solutions as a cloud-based offering to a broad base of organisations covering various legal regulations worldwide.

---

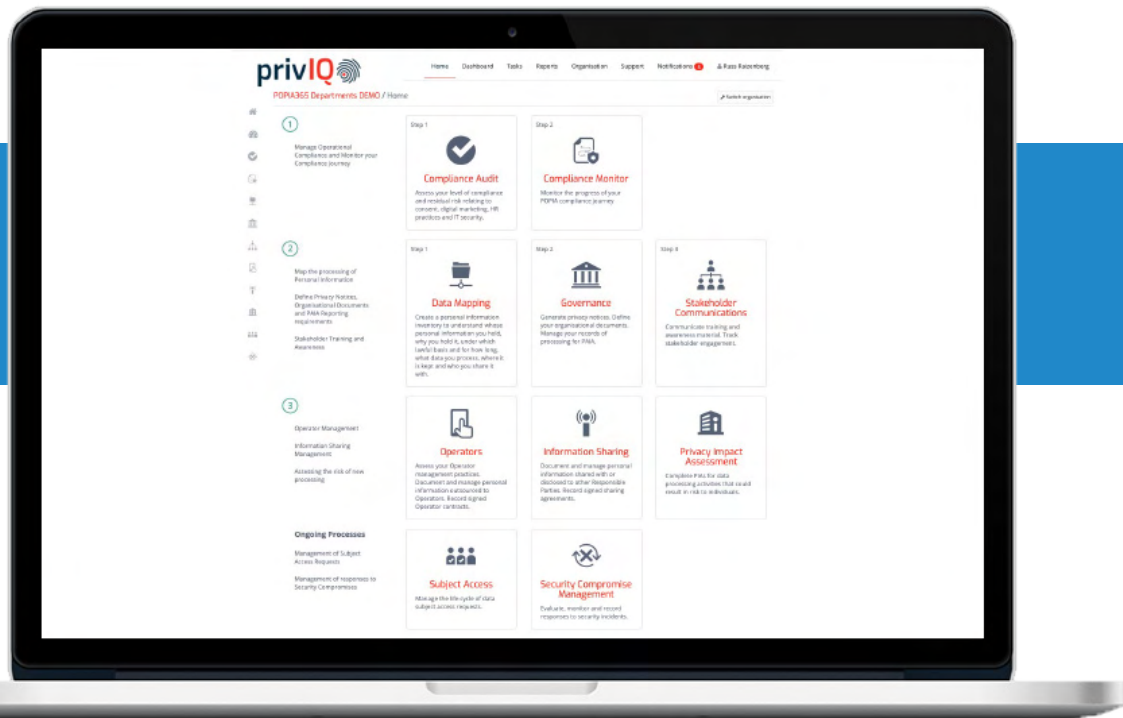
*Intelligent Compliance, Simply*



**Our reach - 8 Regulations worldwide,  
23% of global economy.**



# PrivIQ - Intelligent Compliance, Simply



## Global privacy law compliance service.

### Designed

- Multi-lingual
- Multiple-regulation
- Collaborative

### For

- Mid-Tier
- Enterprise

### Current Regulations

EU / UK / Turkey / South Africa / Nigeria / Brazil / Thailand / California \*

- In development

The following slides are using the GDPR version.

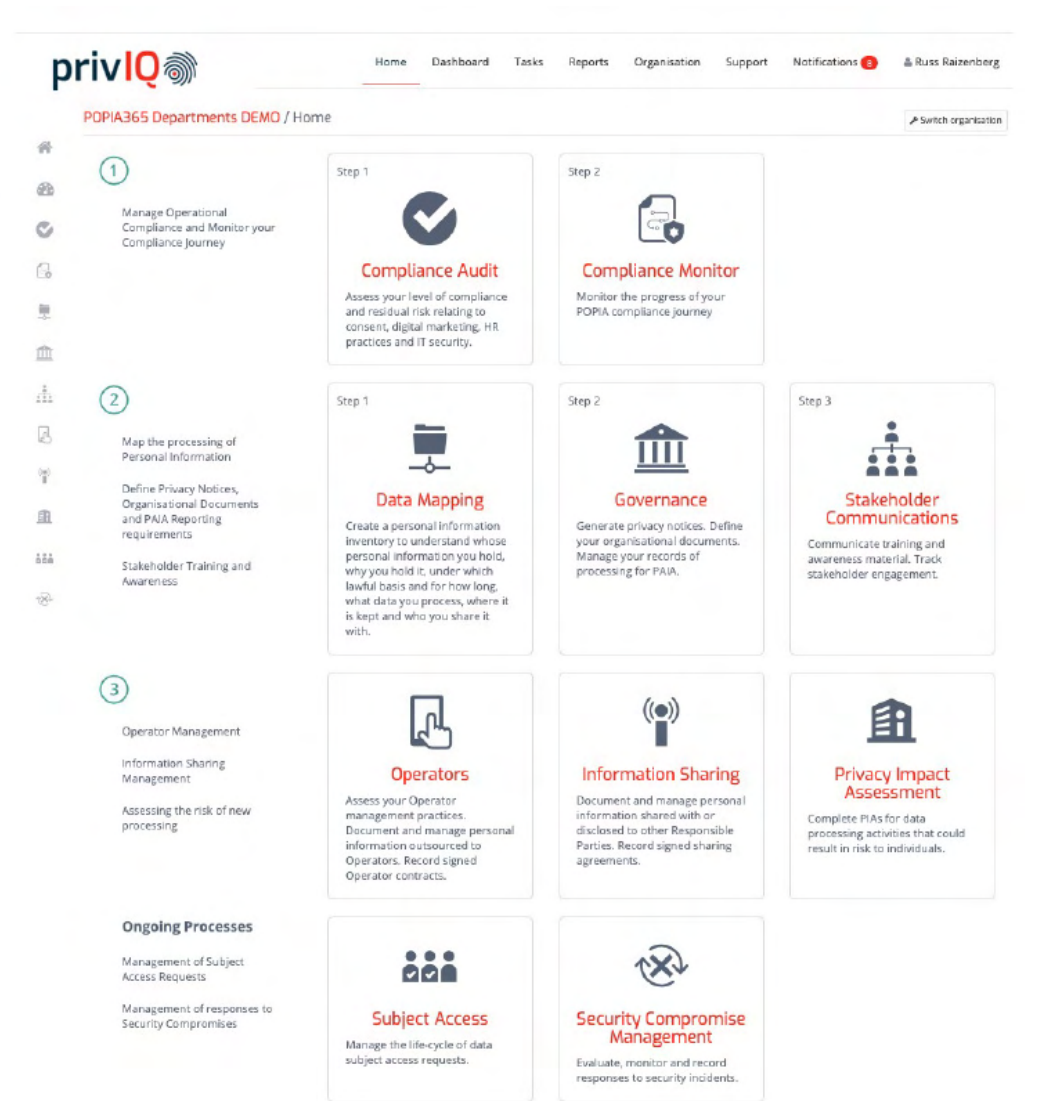
# Software Features

- ✓ Easy to use
- ✓ Collaboration and notification
- ✓ Dashboards
- ✓ Reporting Tools



# Home Screen Layout

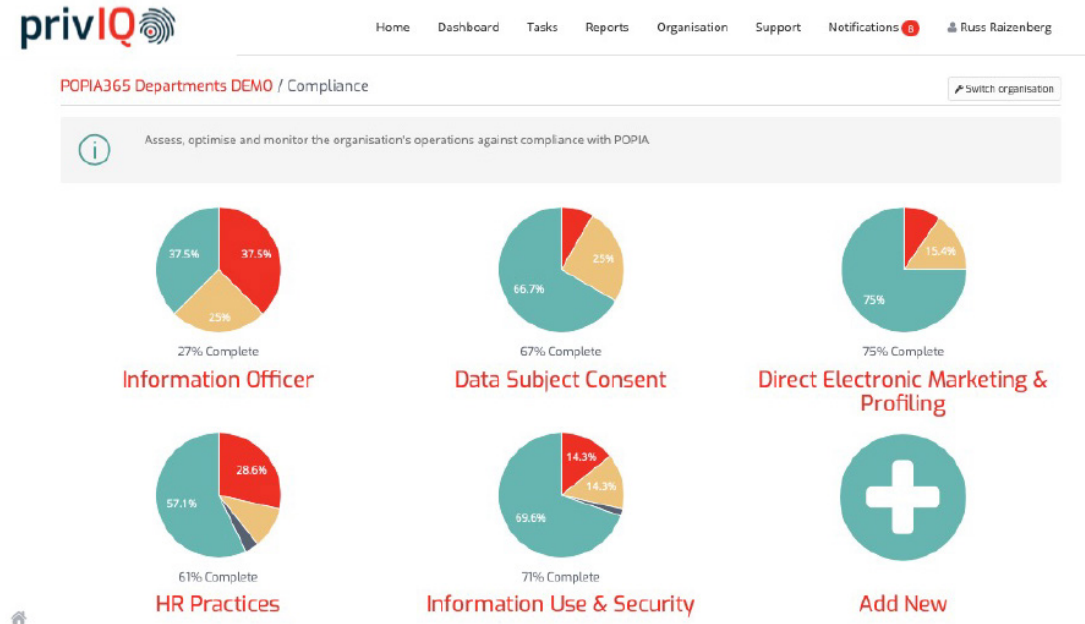
- **Home screen** with all functionality available.
- All text specific to regulation of company.
- **Section 1**
  - Information officer
  - Ongoing compliance reviews.
  - Readiness Assessment of compliance areas.
- **Section 2**
  - Data Mapping of data subjects, processing purposes and legitimate basis.
  - Governance - Privacy Notices, Governance documents, Document library.
  - Employee training and notification.
- **Section 3**
  - Operators and data sharing agreements.
- **Ongoing processes**
  - Data Protection Impact Assessments, Subject access requests and security compromise recording.





# Compliance Section

- Predefined or add your own.
- Main Areas - Data subject consent, Marketing, HR, IT & Security.
- Add your own compliance areas for specific regulation for example, Anti-Money Laundering, PCI, Own Practices.



# Compliance Items

- Predefined or add your own.
- Assign to task owner, specify review periods, due dates.
- Set Task status - Not started, in progress, N/A, Completed.
- Set risk level.
- Add notes and files to each item as required.

The screenshot displays the privIQ interface for managing compliance items. The top navigation bar includes 'Home', 'Dashboard', 'Tasks', 'Reports', 'Organisation', 'Support', 'Notifications', and the user 'Russ Raizenberg'. The main content area is titled 'POPIA365 Departments DEMO / Compliance / HR Practices / Monitoring at work'.

An information box at the top explains that monitoring is a recognized component of the employment relationship, used to safeguard employees and protect their interests. It notes that monitoring must be done lawfully and fairly.

The task is assigned to 'Francis Cronje'. The interface shows a 'Checklist' view with tabs for 'Background' and 'Risk Rankings'. Action buttons include 'Show all notes', 'CSV template', 'Import items', and 'Add new item'.

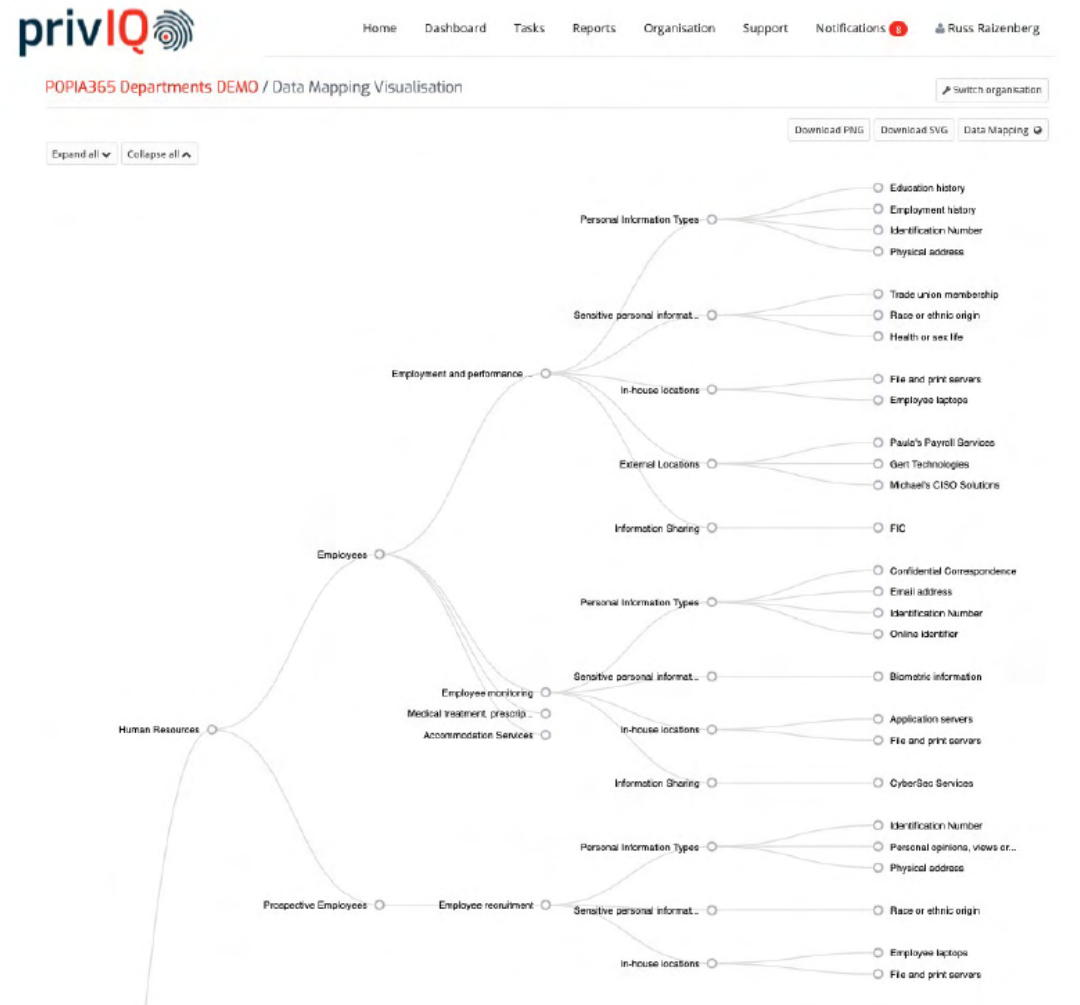
The task is categorized as 'Medium Risk'. The main table lists four compliance items:

Description	Assignment	Status
1. Where there might be an organisational requirement to monitor employees, we perform a privacy impact assessment to justify such monitoring and we fully inform our employees as to the reasons for monitoring. <input type="radio"/> Low Risk <input checked="" type="radio"/> Medium Risk <input type="radio"/> High Risk	Assigned to: Tai Chesselet Due: 08 Mar 2021 Review every: 2 Months Buttons: Set for all, Remove	Not started (Red, Yellow, Green circles)
2. Where there is the need to use the biometric information of employees, we do so in accordance with the rules established in compliance with labour legislation. <input type="radio"/> Low Risk <input checked="" type="radio"/> Medium Risk <input type="radio"/> High Risk	Assigned to: [User]	In progress (Red, Yellow, Green circles)
3. We restrict access to and the processing of information collected through monitoring. <input type="radio"/> Low Risk <input checked="" type="radio"/> Medium Risk <input type="radio"/> High Risk	Assigned to: [User]	Completed (Red, Yellow, Green circles)
4. Our employees understand that monitoring of our computer systems may be required to ensure proper usage of our systems or perhaps to support an enquiry into a security incident. <input type="radio"/> Low Risk <input checked="" type="radio"/> Medium Risk <input type="radio"/> High Risk	Assigned to: [User]	Completed (Red, Yellow, Green circles)

Below the table, there are sections for 'Notes' (with a table of created notes) and 'Files' (with a table for file uploads).

# Data Mapping

- Personal and sensitive personal information inventory.
- Understand whose information you hold, for what purpose, under which lawful basis and for what duration.
- Assists in generating privacy notices, Records of Processing, defines 3<sup>rd</sup> parties to whom data is sent or shared with.
- Enable LIA's (Legitimate Interest Assessments), store all artifacts of data mapping.





# Governance

- Manage Privacy Notices.
- Tailor pre-loaded governance policies to your organisation.
- Upload your own documents and further policies to the document library.
- Communicate policies to all stakeholders and obtain “Read and Accepted” confirmations.

The screenshot displays the privIQ Governance interface. At the top, the privIQ logo is on the left, and navigation links (Home, Dashboard, Tasks, Reports, Organisation, Support, Notifications, Russ Raizenberg) are on the right. Below the navigation, the page title is "POPIA365 Departments DEMO / Governance". A sidebar on the left contains a vertical list of icons representing different governance areas. The main content area features a header with tabs: "Records of Processing (Details)", "Automated Decision Making", "Privacy notices", "Internal", "Optional", and "Document Library". A central information box contains a message about the importance of staff understanding organizational policies. Below this, a grid of nine policy cards is shown, each with an icon, title, and status:

Policy Title	Status
Protection of Personal Information - Program Announcement	Complete
Personal Information Protection Policy	Complete
CCTV Policy	Complete
Data Protection Training & Awareness	Complete
Best practices for protecting personal data	Complete
Transborder Information Flows	Not started
POLICY: Work from home	Complete
POLICY: Personal Information Security Compromise	In progress
POLICY: Data Subject Access Requests	In progress

# 3<sup>rd</sup> Party Contracts and Data Sharing

- Manage 3<sup>rd</sup> part and data sharing contracts.
- Ensure 3<sup>rd</sup> parties confirm their compliance.
- Store signed contracts.

The screenshot shows the 'privIQ' web application interface. At the top, there is a navigation bar with links for Home, Dashboard, Tasks, Reports, Organisation, Support, Notifications (with a red badge), and a user profile for Russ Raizenberg. The main content area is titled 'POPIA365 Departments DEMO / Operators / Operator contracts'. Below the title is an information box with a warning icon and text: 'You should only use operators that provide sufficient guarantees, in terms of expert knowledge, reliability and resources, to implement security measures which will meet POPIA's requirements. The processing done by an Operator must be governed by a written contract. If the Operator is located in SA, you can use this app's Operator contract template or your own contract. If the Operator is located outside SA, you will need to indicate the lawful basis you are using for transferring the data outside SA. Establish your Operator relationships through the data mapping process and return to this section to maintain those contracts.'

Below the information box is a search bar and a table of operator contracts. The table has columns for Operator, Operator type, Country, Renewal date, Lawful basis, Contract Status, and Contract. The table contains five rows of data:

Operator	Operator type	Country	Renewal date	Lawful basis	Contract Status	Contract
Amazon Web Services	SaaS Provider	Ireland		To conclude or perform a contract with a third party in the interest of the data subject	Not signed In progress ✓ Signed	Template contract Own contract Upload Signed contract Upload Edit Delete
Annamie & Arst PTY	Broker Services	Azerbaijan			Not signed ✓ In progress Signed	Template contract Own contract Upload Signed contract Upload Edit Delete
Arat Cloud Solutions	Cloud Service Provider	Antarctica			Not signed ✓ In progress Signed	Template contract Own contract Upload Signed contract Upload Edit Delete
Claude's Cleaning & Catering	Cleaning & Catering	South Africa			Not signed ✓ In progress Signed	Template contract Own contract Upload Signed contract Upload Edit Delete
Gert Technologies	Cloud Service Provider	Anörcia			Not signed ✓ In progress Signed	Template contract Own contract Upload Signed contract Upload Edit Delete

At the bottom of the page, there is a pagination control showing '1' and '2'.

# Data Protection Impact Assessments

Organisations need to assess any personal data processing that might result in high risk to individuals. Pre-defined screening and purpose questionnaires.

- Wizard for justifying processing and documenting individual's rights are protected.
- Workflows to get feedback from stakeholders and manage the approval process.
- Analyse risks and record mitigation records using automation rules.
- Easily run reports for stakeholders and regulators.

The screenshot shows the 'privIQ' Data Protection Impact Assessment console. The interface includes a navigation menu with 'Dashboard', 'Reports', 'Organisation', 'Support', 'Notifications', 'English', and 'Jane Van Hoorn'. The main content area is titled 'GDPR / Amsterdam Accounting Services / Data Protection Impact Assessments' and contains a 'Legacy Data Protection Impact Assessment console' section. A dark header bar displays 'test' and 'AMSTERDAM000000161, Created 09 Sep 20, Draft'. Below this, there are buttons for 'Message for reviewer', 'Select reviewer', 'Submit for review', 'Select approver', and 'Submit for approval'. A central instruction box states: 'Visit each tab. Respond to items by toggling sliders if an item is relevant or answering the question. Submit for review to get feedback from colleagues or approval when you've completed all tabs. After the initial approval, a risks tab will appear where you can detail each risk and how it's being mitigated. Before a DPIA can be approved all risks must be individually approved. Editors, reviewers and approvers can add comments or upload files against any item by clicking on the Notes icon.' The main assessment area has tabs for 'Overview', 'Screening questions', 'Purpose', 'Processing justification', and 'Individual's rights'. An information icon indicates: 'Complete the following checklist to determine if a DPIA is necessary. If you toggle any of the items, a DPIA isn't necessary. You may upload comments or documents to justify your reasoning by clicking on the Notes icon.' The checklist includes seven items, each with a toggle switch and a 'Notes' icon:
 

- 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.
- I am a lawyer and the processing of my clients' personal data is not to be considered large-scale.
- Our processing operations appear on an exemption list provided by our supervisory authority for which NO data protection impact assessment is required. Please provide details.
- The lawfulness of processing applies to clauses 6.1(c) or 6.1(e), has a legal basis in EU or our Member State law, AND a data protection impact assessment has already been carried out in the context of the adoption of that legal basis. Please provide details.
- We comply with an approved code of conduct that has assessed the impact of the relevant processing operations. Please provide details.
- A prior data protection impact assessment has addressed a set of similar processing operations that present similar risks. Please provide details.
- The processing is NOT likely to result in high risk to the rights and freedoms of data subjects. Please provide details on how you came to this conclusion.

 Below the checklist are buttons for 'Add new justification', 'Review', and 'Approval'. The 'Review' and 'Approval' sections show 'No review history. Submit for review to get comments.' and 'No approval history. Submit for approval to get feedback.' respectively. At the bottom right, there are 'Previous', 'Next', and 'Cancel' navigation buttons.



# Subject Access Requests

A **subject access request** is a request made by a data subject for the information that your organisation holds about them.

- A pre-built brandable form you can link to from any website or application.
- Real-time alerts and reminders.
- A case management system that records and stores your SAR responses in one location.
- The option to add written and verbal requests manually.
- Guidance to ensure you respond correctly.
- Multilingual forms.
- Workflow to ensure you validate and respond before deadlines.

privIQ

Home Dashboard Tasks Reports Organisation Support Notifications Russ Raizenberg

POPIA365 Departments DEMO / Subject access request [Switch organisation](#)

Requests Settings Request response guide

Person responsible Russ Raizenberg

We provide you with a page where **data subjects** can submit their queries from your website.

**Domains**  
Add all the domains from which you will be calling the widget. Any requests not originating from one of the domains in this list will be rejected. For example: https://test.popia365.co.za, http://demo.popia365.co.za, etc.  
[Add new](#)

**Code to include on your site**  
Add a link to this page on your website by using the code given here.

```
<script>(function [w,d,s,o,f,j,s] { w["365Compliance"]=o.w[o]=w[o] || function () { (w[o].q = w[o].q || []).push(arguments) }; s = d.createElement(s); fs = d.getElementsByTagName(s)[0]; s.id = o; js.src = f; js.async = 1; fs.parentNode.insertBefore(s, fs); })(window, document, 'script', 'mw', 'https://app.popia365.co.za/js/365Compliance.min.js');mw("init",{container:'your-element-id',key:'866b7e3-abe5-4059-a08e-df5a530f814f'});mw("dsar");</script>
```

Copy the code above into your web page html and replace 'your-element-id' with the id of the html element within which you want the content displayed. If you don't specify a container element id or if the specified element does not exist, the content will be inserted at the bottom of your html page.

Once the code is inserted in your web page, the following form will be injected into the page:

Use this form to make enquiries or requests around your personal information that we might be collecting and using.

Affidavits, unique identifiers, proof of identity (where required) or other documentary evidence in support of your request or, if the space provided proves inadequate, additional information as a signed Annexure, may be attached by clicking the **UPLOAD** button below.

What is the nature of your request?  
[Access \(Form 1\)](#) [Objection \(Form 1\)](#) [Correction \(Form 2\)](#) [Deletion \(Form 2\)](#)

Particulars of the person making the request

First name  Last name  Email address

Postal address  Telephone number  Fax number

Person's relationship with our organisation

Are you applying on behalf of another person?  No  Yes

How would you prefer our response and any information to be presented to you?

# Breach Management

The high incidence of data breaches means that avoiding a personal data breach is no longer good enough for small to medium-sized organisations.

We enable you to prepare for data breaches by having a system in place to manage your response to them, from assessing and documenting to reporting them within the stipulated time of becoming aware.

- Manage your responses to personal data breaches.
- Report personal data breaches to the authorities.
- Protect your business from the risk of a bad reputation.

The screenshot shows the 'privIQ' Risk Assessment interface. The breadcrumb trail is 'POPIA365 Departments DEMO / Security Compromise / Contained Incident'. The form title is 'Risk Assessment' with 'Cancel', 'Previous', and 'Next' buttons. An information icon and text state: 'Not all breaches will lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be equipment failure where files were backed up and can be recovered, albeit at some cost to the organisation. While these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of a customer database, which may be used to commit identity fraud. Most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.'

The form fields are as follows:

- What type of data is involved? Employees
- Approximate number of records involved? 1234
- Which types of data subjects are impacted? Employees
- How many data subjects are impacted? 1234
- What are the likely causes of this incident?
  - Improper disposal of equipment or documents
  - Lost or stolen equipment or documents
  - Ineffective access controls (digital and physical)
  - Inefficient data governance
  - Inappropriate defence against cyber threats
  - Unprotected transmissions (email, video conferences etc.)
  - Insufficient, or lack of policies, procedures, controls
  - Equipment failure
  - Poorly trained, unaware, negligent employees
  - Other
- The incident has been contained and it is unlikely to impact data subjects
- The incident happened Internally
- The location has been secured from tampering
- Are you able to prevent further loss / continuation of the incident?

A progress bar at the bottom shows 9 steps, with step 5 highlighted in orange.





**Thank  
You**

---