

# ARMATA POPIA ADVISORY SERVICE

WITH POTENTIAL FINES OR JAIL TIME FOR  
POPIA BREACHES, CAN YOU AFFORD  
NOT TO KNOW YOUR STATUS?

- Learn how PoPIA impacts your organisation.
- Ensure the adequate measures needed to comply with PoPIA's eight conditions for lawful processing of personal information are in place.
- Accountability for personal information fosters trust with all business stakeholders
- Consult with your legal and IT experts to determine the best approach to resolving these issues.
- Minimise the risk of an information breach, penalties and/or civil action for damages.
- Identify any glaringly obvious compliance gaps.

## PRODUCT OVERVIEW\_

The purpose of the Protection of Personal Information Act (PoPIA) is to enforce everyone's constitutional right to privacy and the safeguarding of their personal information against theft, fraud and other abuses.

PoPIA is compulsory for all, and sets out conditions around how personal information should be lawfully processed and stored by third parties to ensure its security and protection. All businesses have personal information about their employees, suppliers and clients. In fact, policies like FICA (Financial Intelligence Centre Act) actually demand personal and financial client Data be gathered and stored.

Businesses need to be familiar with PoPIA provisions or face the risk of substantial fines, imprisonment or both. For these reasons, it's important to understand whether you have the right processes and controls in place to protect your company and its Data.

But what happens if Data is misused, stolen or lost? Data breaches can come from a variety of sources and not every Data breach is caused by sophisticated hacking attempts. Many can stem from human error or mundane oversights, which doesn't make them any less damaging.

**Armata offers a PoPIA Advisory Service service with the following options:**

1. Conduct an Information Audit to determine:
  - The categories of personal information your organisation processes.
  - Why is it processed [what's the purpose?]
  - Where and how you store the personal information.
  - Who you share personal information with.
2. Appoint or work with an Information Officer.
3. Conduct an Organisational Impact assessment.
4. Create an awareness guideline for the organisation and staff.
5. Run a Posture Assessment.
6. Run security assessments to see how easily Data can be compromised by third parties or internally.
7. Recommend improvements.
8. Offer on-going monitoring and reporting of your Data compliance.

## POPIA GOVERNANCE\_

### COLLECT

What data do we collect?  
Do we have permission to collect the data?

### STORE

Where do we store the data?  
How old is the data?

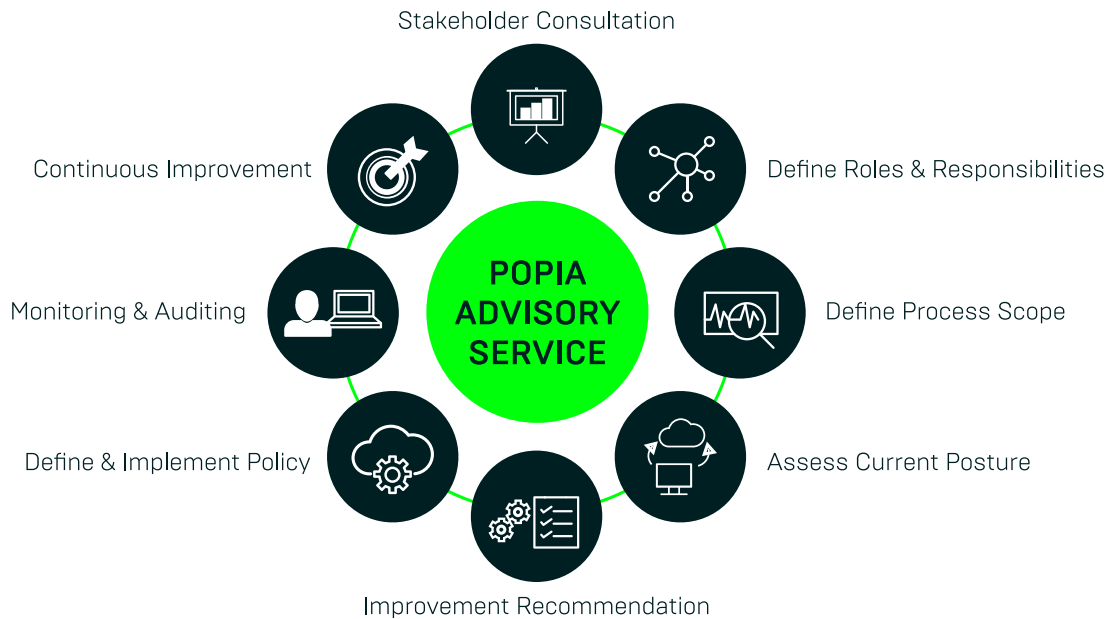
### USE

How can we use the data?  
Who in our supply also processes the data?

### DESTROY

When do we need to delete or destroy the data?

## HOW IT WORKS\_



## FEATURES & BENEFITS\_

### **Understand your current PoPIA status**

A baseline of the current PoPIA status will be created allowing a company to establish their current risk.

### **Gain insight on where to improve**

Recommendations on what to improve and a plan to become PoPIA compliant.

### **Get recommendations on solutions and policies to protect digital Data**

Solutions like Data discovery, classification and protection allow for stronger control of Data and policies, while awareness helps eliminate the human factor.

### **Utilise services to continually monitor and audit your PoPIA compliance**

On-going monitoring and auditing will ensure an organisation remains PoPIA compliant.

# \_ARE YOU READY FOR POPIA?