



POPIA



Bidvest AFCOM

KEEPING IT ALL TOGETHER



ALERTER



WE HAVE A NEW LAW

POPIA



So why is there a need for another law?





One of the overriding reasons:

Data ..

OUR PERSONAL DATA



Data has become an asset for nearly every organization, no matter if they are profit, non-profit, large, or small.

Spearheaded by

- improved and increased technological resources for data collection; and
- the rise of inexpensive and potentially limitless cloud storage,
- organizations store massive amounts of data on private individuals.

AND

In many cases use this data is a source of revenue.

BUT

From the standpoint of the individuals whose personal information is being bought and sold, **THIS IS A PROBLEM.**



Countries around the world, in order to address these concerns have introduced General Data Protection Rules.

These Rules protect a person's data and their privacy.

Global Laws



Privacy laws around the world.

- Information Privacy Act 2014 (Australian Capital Territory)
- Information Act 2002 (Northern Territory)
- Privacy and Personal Information Protection Act 1998 (New South Wales)
- Information Privacy Act 2009 (Queensland)
- Personal Information Protection Act 2004 (Tasmania), and
- Privacy and Data Protection Act 2014 (Victoria)
- General Data Protection Regulation (GDPR) – EU and UK
- Californian Data Protection Act (CDPA)

What are these laws about ?

These data protection laws are aimed at strengthening the privacy rights of persons in today's data-driven landscape.

These laws all embrace or share much the same guiding principles, including **accountability, transparency, security, data minimization, purpose limitation and the rights of data subjects.**

Our law is known as the Protection of Personal Information Act, or POPIA



SO WHAT IS POPIA ALL ABOUT ?



POPIA

POPIA protects a person's right to privacy.

POPIA gives persons the right **NOT** to have their personal information **misused, abused or shared without their knowledge.**

About POPIA



POPIA came into operation in July 2020.

It sets out rules on how individuals and legal entities (including private, public bodies), who are known as **Responsible Parties** - may use an individual or legal entity's (including private, public bodies), who are known as **Data Subjects'** - **personal data or information.**

Application



POPIA applies to companies based in South Africa or those that use and process personal data within South African borders.

POPIA Definitions



POPIA houses numerous important definitions and phrases, **which need to be understood.**

What is “Personal Information”?

Personal Information includes:

- Name, address and ID number;
- A person’s educational and/or employment history;
- Financial details such as income or earnings;
- Views or opinions of another;







PERSONAL INFORMATION

1. What's your first name? _____
2. What's your surname? _____
3. What are your parents' names? _____
4. Do you have any pets? _____
5. How old are you? _____
6. What is your favorite food? _____
7. What is your favorite color? _____
8. What is your favorite animal? _____
9. Where do you go to school? _____
10. What grade are you in? _____
11. What is your teacher's name? _____
12. Who is your best friend? _____
13. Do you play sports? Which ones? _____
14. What is your favorite TV show? _____
15. What is your favorite book? _____

About POPIA



Personal Information

 <ul style="list-style-type: none">·name·address·date of birth	 <p>Fingerprint data</p>	 <p>Facial-recognition data</p>	 <p>Passport number</p>	 <p>Driver's license number</p>	 <p>MY NUMBER (Individual numbers)</p>
---	---	---	--	--	---

= newly defined* =

What is “Special Personal Information”?

- **Special Personal Information**, such as person’s information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, birth of a person, and biometric information such as one’s blood type and fingerprints;

“Processing” includes sharing

Importantly, **Processing** will include **sharing**,



i.e., where Afcom uses or shares a Data Subject’s Personal Information with another party, i.e., with a credit bureaux or a marketing agency.

In doing so, such sharing must be done in accordance with the provisions of POPIA.

Responsible Party

The Responsible Party is the person or legal entity who is using and processing a Data Subject's Personal Information.



**Bidvest Afcom is a
Responsible Party in
terms of POPIA**

“Operator (s)”



POPIA also applies to persons who process Personal Information on behalf of another, known as an Operator.

This is a person who Processes Personal Information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of the Responsible Party.

“Operator (s)”



An Operator will include any contractor or third party who has been asked by Afcom to Process a Data Subject’s Personal Information on its behalf.

Afcom notwithstanding the activities of the Operator will remain legally responsible for the Processing activities carried out by the Operator.

POPIA however **does require Afcom to conclude a processing agreement with such Operator**, which will bind the Operator contractually in relation to data security and confidentiality.



Application of POPIA

POPIA therefore applies to Data Subjects and Responsible Parties, including;

- individuals,
- legal entities, such as a public and/or private body, and
- to all personal information belonging to individuals and to private and public bodies and / or individuals.



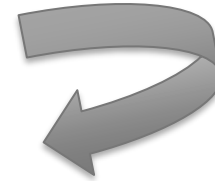
Does not apply to

POPIA does not apply to:

- **National security and safety activities**, including policing, road and traffic controls, investigating, prosecution, courts, and judicial functions;
- **Journalists** and reporting;
- **Purely household** activities;
- **Exempted entities**, especially those performing a public duty.



Impact on Bidvest Afcom



Following this,

POPIA will apply to Bidvest Afcom as a **Responsible Party**, when it or its employees and / or service providers or representatives **Processes Personal Information** which belongs to **Data Subjects**.

Including personal information belonging to its employees, service providers, tenants, patrons and visitors, vendors, clients, customers, and other third parties.

Examples of Data Subjects

- Suppliers of raw materials – regardless of where located...
- Individuals who purchase Afcom's products – i.e. Customers
- Service providers and other vendors who Afcom trades with or vend with
- Visitors to the Afcom Facilities
- Users of the Afcom website
- Persons who Afcom direct markets to or recipients of advertisements or PR material
- Afcom employees and managers, as well as directors

Examples of HR. Data Subjects

- Employees
- Recruitment agencies
- Job applicants
- Bursary applicants or candidates
- Learners
- Service providers such as trainers

Finance

Data Subjects

- Employees
- Service providers
- Customers
- Debtors
- Creditors
- Banks



Examples of Marketing Data Subjects

- Persons who the marketing department markets to
- Retailers
- Persons on marketing database
- Persons who receive newsletters and updates



Examples of Procurement Data Subjects



Examples of Personal Information

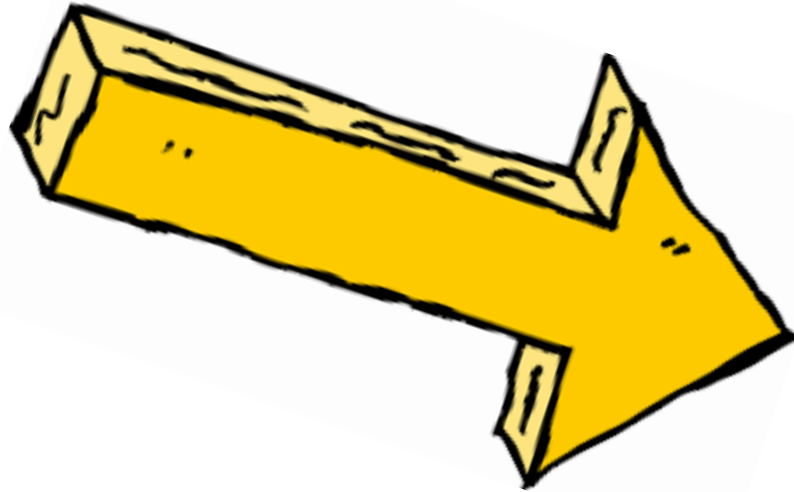
- Identity details, such as ID or registration numbers
- Contact details
- Financial details
- Earnings - employees
- Medical history and records- employees
- Banking details
- Performance history
- Opinions
- Dietary preferences
- SARS and TAX details
- Race and gender
- Opinions and preferences
- Images and photos



Examples of Operators

- Credit Bureaus
- Training or skills development Service Providers
- Recruitment agencies-employees
- ICAS- wellness programs

Examples of how Bidvest Afcom uses a Data Subject's Personal Information



Employee

- Applicant responds to a Job advertisement
- HR receives person's details and CV
- HR and Manager interview applicant
- Applicant is offered a job
- Applicant signs an employment contract
- Employee completes a number of internal documents
- Employee has to fly somewhere for business and the secretary books the employee a flight and accommodation
- Employee is registered for COIDA and UIF and SD
- Employee is paid, less PAYE which payroll or finance deducts and pays over to SARS
- Employee is disciplined

Customer

- Person contacts Afcom with a sales enquiry
- Afcom in response sends list of goods and services and price list
- Person states he wants to purchase goods
- Purchaser sent a Credit Application which he completes and is vetted and approved after undergoing reference checks
- Afcom loads person as a customer
- Customer orders goods
- Afcom customer corresponds with sales and operations
- Afcom invoices customer for purchase and delivery
- Customer is invited to functions
- Customer is sent emails

Supplier

- Afcom contacts supplier with an enquiry on certain requirements
- Supplier in response sends list of goods and services and price list
- Afcom states they want to purchase goods
- Vendor process is completed
- Afcom loads person as a supplier
- Afcom corresponds with supplier sales and operations
- Afcom orders, receives and is invoiced for purchase and delivery

Marketing

- Marketing contacts customer via mailchimp
- Marketing sends bulk mailer to customer

**So how do you process all this
Personal Information?**



UNDERSTAND

The 8 universal personal data protection principles or conditions



THE PRINCIPLES OF DATA PROTECTION

- LAWFULNESS, FAIRNESS AND TRANSPARENCY**
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- PURPOSE LIMITATION**
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- DATA MINIMISATION**
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- ACCURACY**
Personal data shall be accurate and, where necessary, kept up to date.
- STORAGE LIMITATION**
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- INTEGRITY AND CONFIDENTIALITY**
Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- ACCOUNTABILITY**
The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles.

Helping small businesses work towards Data Protection Compliance and success on their Web Application path.

www.ServellIT.com

Rights under POPIA

POPIA embraces and sets out 8 universal personal data processing principles (known as conditions under POPIA) that have to be met by **Responsible Parties** when they **Process Personal Information**.

It is important that you all understand these rights and give effect to them when you process a Data Subject's Personal Information.



Step 1 - Accountability



Afcom is the Responsible Party and therefore is accountable for compliance with POPIA.

In other words –YOU as Afcom employees must ensure that the POPIA Law is followed and that all uses of a person's personal information is done in accordance with POPIA.

When you process Personal Information on behalf of Afcom it must be done lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject and it must be done in accordance with POPIA.

If not- Unlawful Processing – fines, criminal and civil penalties

Step 2 - Purpose Specific

There must be a reason for the collection of the Data.

Personal Information

- must be collected for a **specific, explicitly defined and lawful purpose related** to a function or activity of Afcom;
- may only be processed with the knowledge of the Data Subject,
- must be processed in order to comply with a legal obligation, a contractual obligation or to protect Afcom or the Data Subject.... Or in the absence of these scenarios, with the Data Subject's consent.

If not- Unlawful Processing

Step 3 - Adequate and not Excessive



- Personal information may only be processed if, given the purpose for which it is processed, it is **adequate, relevant and not excessive**.
- Person's information, therefore, may not be “overprocessed” – i.e. where information is taken and used which is not needed for the purpose which has given rise to the processing.
- Furthermore, Personal Information **must not be retained any longer than is necessary** for achieving the purpose for which the information was collected or subsequently processed.

If not- Unlawful Processing

Step 4 - Openness



Afcom employees has an obligation, which should be performed at the time when the collection takes place, to make the Data Subject aware of

- the purpose or reason (s) why the Personal Information is being Processed;
- what will be done with such Personal Information;
- who the Personal Information will be shared with;
- how the Personal Information will be handled, stored and safeguarded; and
- the rights which the Data Subject has in respect of the information.

If not- Unlawful Processing

Step 4 - Openness



In order to comply with the above, the Data Subject must at the time of the processing be directed to **an Afcom Processing Notice** describing the processing activities, who the information is to be shared with, how it will be used, for what purpose and how it will be safeguarded, transferred, and destroyed once its no longer needed, etc.

These are housed on the Afcom Website.

Step 5 - Personal Information Quality

Afcom employees must ensure that all Personal Information held by it, is accurate, complete, not misleading, and is always kept up to date.



Step 6 - Security Safeguards



Afcom has a duty to safeguard the Personal Information against any unauthorised or unlawful access or Processing.

This should be done by way of the implementation of technical and organisational measures, such as safe filing, fire walls, IT policy compliance, sound email etiquette, physical and electronic security controls, ensuring that personal data is not left lying around, or shared with people who don't need it... etc.

Step 7 - Individual Participation

Data Subjects have a number of rights in relation to their Personal Information, including the right to ask Afcom:

- to describe what Personal Information it holds and to describe what it is doing with the Personal Information;
- to update Personal Information;

Trans-border Information Flows



In terms of POPIA, Afcom may NOT transfer Personal Information outside the borders of South Africa or abroad unless:

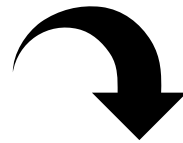
- the recipient country is subject to a law, binding corporate rule, binding agreement or memorandum of understanding which provides similar levels of protection to those set out under POPIA;
- where no laws or agreements mentioned above are in place, then the transfer may only take place if the Data Subject has consented to the transfer; or the transfer is necessary for the performance of a contract; or the transfer is for the benefit of the Data Subject and it was not reasonably practicable to get the Data Subject's consent.



So- to recap- what do you, an Afcom employee have to do when you use and processes Personal Information on behalf of Bidvest Afcom?



In other words what do you have to do when performing the following:



EXAMPLES OF PROCESSESSING

HR Processing

- Collecting information from a candidate when he or she applies for a job
- Putting a person through a psychometric test
- Employing an employee and managing that person
- Paying an employee
- Disciplining an employee
- Using a service provider to provide HR. Manuals or do training.

Procurement Processing

- Collecting information from a potential service provider who is desirous of doing business with you
- Running the various credit checks
- Concluding a service agreement with a service provider
- Paying a service provider
- Communicating generally with service provider
- Using a service provider to provide Manuals or do training

Sales Processing

- Collecting information from a potential customer who is desirous of doing business with Afcom
- Concluding a transaction with a customer
- Invoicing and receiving payment from a customer
- Communicating generally with a customer

Marketing Processing

- Obtaining permission from a customer to send it direct marketing
- Inviting a customer to an event
- Communicating generally with a customer in relation to your goods or services and promotions
- Building a data base of customers/clients

Rules



Follow the rules.....

Understand the Afcom Rules, as per POPIA, on how Afcom must process personal information.

Got it?

POPIA Policy

These rules are clearly set out under the Bidvest Afcom POPIA Policy which will tell you what you must do when processing Personal Information.



Processing Notice

Afcom has developed certain Processing Notices which are housed on its website which describe to the Data Subject how Afcom is going to use the Data Subject's data.

Please ensure that before you process any Data Subject's Personal Information that you tell the Data Subject to consider and read this Processing Notice – which sets out how information is used, shared, stored etc.

All the Bidvest Afcom documents and forms must house a reference to its processing notices and house a hyperlink which allows the Data Subject to access the said notice.

Take note that all the POPIA related documents including its Processing Notices are housed on the on the Bidvest Afcom website.



Website

PROMOTION OF ACCESS TO INFORMATION ACT (PAIA)	THE PROTECTION OF PERSONAL INFORMATION ACT
ACT AND REGULATIONS	ACT AND REGULATIONS
SUMMARY OF PAIA & GUIDE LINES	SUMMARY OF POPIA & GUIDE LINES
PAIA MANUAL	POPIA POLICY
INFORMATION OFFICER AND DEPUTY INFORMATION OFFICER DETAILS	
HOW TO APPLY FOR INFORMATION	<p>WEBSITE TERMS AND CONDITIONS</p> <p>PROCESSING NOTICES</p> <p>Website processing notice Cookies Notice- H.R processing notice Procurement and Supply Chain processing notice Customer processing notice Security processing notice</p> <p>Operator agreement Data transfer agreement</p> <p>DATA SUBJECT FORMS</p> <p>Withdrawal of consent notice Objection notice Update to details notice</p>



**Consequences of
non-compliance**

with POPIA

NON-COMPLIANCE



Any breach or non-compliance with POPIA can be referred to the **Information Regulator**.

On receipt of this information, the Information Regulator will then:

- Conduct a pre-investigation,
- Act as conciliator,
- Either Dismiss the complaint, or Conduct full investigation,
- Refer the matter to an enforcement process,
- Serve the Responsible Party with a Compliance notice and levy a fine in the case of noncompliance, of up to R10 000 000.00



(10 million rands).

Criminal

Certain criminal offences have been created under POPIA, which will be brought where a person:

- refuses to comply with an order,
- refuses to give effect to a valid search warrant,
- gives incorrect information,
- refuses to give information, and/or
- breaches one's duty of confidence.



Criminal



If a person is charged with a criminal offence and found guilty in a court of law such person could be imprisoned for a period not exceeding



10 years or fined or given both a jail sentence and a fine.

Civil Remedies

- In addition to a criminal sanction or an administrative penalty, any person who has had their rights offended or abused under POPIA may bring a civil action against the perpetrator or wrongdoer.
- In this regard, the aggrieved and/or offended Data Subject or the Regulator, upon request of the Data Subject, has the right to institute a civil claim for damages where non-compliance with POPIA can be shown, regardless of intention or negligence on the part of the person who has not complied with the Act.

Civil Remedies



If the court finds that the Data Subject's rights have been abused and the Act contravened, then the court has the right to order payment of pecuniary damages, nonpecuniary damages and legal costs.

CAUTION

If you don't comply you maybe subject to possible disciplinary action and dismissal
!!!!

