LegalSkills+

Data Protection + POPIA

Website
lawcoach.co.za

LegalSkills+

Data Protection + POPIA

- **Introductory Concepts**
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- Special Cases
- Key Roleplayers
- Enforcement
- POPIA + Technology
- Implementation

LegalSkills+

Introductory Concepts

- POPIA 101
- Key Concepts
- Roleplayers
- Scope
- Application
- Exclusions

LegalSkills+

POPIA 101

Establish a solid foundation of key concepts

Get comfortable with the terminology and ideas we'll be exploring throughout the series

What is Data Protection?

Laws and safeguards put in place to protect personal information. It matters because of how the world has evolved and what can happen if your data falls into the wrong hands.

- Focus: privacy

POPIA

The Protection of Personal Information Act is the cornerstone of data protection law in South Africa.

- Enacted July 2013
- Effective July 2020

POPIA's Aims

- Upholding privacy rights
- Facilitating flow of information

POPIA + PAIA

- Promotion of Access to Information Act
- Focus: transparency

LegalSkills+

Key Concepts

Crucial concepts and definitions

Critical for context

IMPORTANT

POPIA won't apply to the processing of information other than personal information.

Personal Information

- Any information or data which can be used to identify an individual or which relates to an identifiable individual
- Names, identity numbers, contact details, biometric information like fingerprints, medical history, and more

Processing

- Processing is anything you do with Personal Information
- Collection, storage, use, sharing, and destruction of the personal information, and it can happen both manually and automatically
- Handwritten or digital

LegalSkills+

Roleplayers

↘

The Cast + Crew

- **Data Subject**
- **Responsible Party**
- **Infomation Officer**
- **Operator**
- **Information Regulator**

LegalSkills+

When does *POPIA* come into play?

LegalSkills+

Scope + Application

↘

Scope: POPIA applies to the processing of personal information that is entered into a record by or for a responsible party.
Application: POPIA applies to organisations in South Africa and some organisations based outside of South Africa

Automated Processing

- Any processing done by a computer or other automated system.

Manual Processing

- Processing done by hand.
- Part of, or intended to be part of, a filing system

South Africa

All organisations based in South Africa

Rest of the World

- Organisations based outside South Africa, if it processes personal information within South Africa
- Exception: passing through

LegalSkills+

Exclusions

↘

POPIA outlines specific situations where it doesn't apply, allowing for a balance between data protection and other important interests.

Personal / Household Activities

Deidentified Information

National Security

Law Enforcement

Cabinet + Judicial Functions

Journalism, Literature, Art

LegalSkills+

Introductory Concepts

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- **Foundations for Lawful Processing**
- Conditions for Lawful Processing
- Special Cases
- Key Roleplayers
- Enforcement
- POPIA + Technology
- Implementation

LegalSkills+

Foundations for Lawful Processing

- Grounds for Lawful Processing
- Legitimate Interests
- Consent
- Collection Requirements

LegalSkills+

Grounds for Lawful Processing

These are the specific reasons why you're allowed to process personal information.

Beware if you don't have one of these.

- **Consent**
- **Contracts**
- **Laws**
- **Public Duty**
- **Legitimate Interests:** Data Subject
- **Legitimate Interests:** Responsible or third party

LegalSkills+

Compliance Question

- Do I have a valid reason under POPIA to process this personal information?

LegalSkills+

Legitimate Interests

↘

POPIA recognises the legitimate interests of three key players: the **data subject**, the r**esponsible party**, and **any relevant third parties**.

Data Subject

- Protecting their own interest
- Examples: privacy, financial well-being

Responsible Party + Third Party

- Pursuing an interest
- Examples: business decisions, debt recovery

What is a legitimate interest?

- Specific and real
- Lawful
- Necessary
- Balanced

LegalSkills+

Consent

↘

Definition: *"**consent**" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information*

Voluntary

- Consent must be freely given, without any coercion or pressure.

Specific

- Consent must relate to a particular purpose or set of purposes.

Informed

- The person giving consent must understand what they're agreeing to.

Compliance Questions

- Is the consent I have valid? Does it meet the requirements of being voluntary, specific, and informed?
- If asked, can I prove that I obtained the necessary consent? Do I have records to back it up?

LegalSkills+

Requirements for Collection

↘

General Rule: personal information must be collected directly from the data subject.

EXCEPTIONS to the general rule, which allows for collection from another source, is found under section 12 of POPIA.

Data Protection + POPIA

Public Record or Publicly Available

- The information is already in the public domain, like details in court documents or company site.

Consent

- The data subject has given permission for you to collect their information from another source.

Necessary for Legal or Public Interest Reasons

- This could include law enforcement, national security, or protecting someone's life or health.

LegalSkills+

Compliance Questions

- Did I collect the information directly from the data subject?
- If not, can I justify it under one of the exceptions allowed by POPIA?

LegalSkills+

Foundations for Lawful Processing

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- **Conditions for Lawful Processing**
- Special Cases
- Key Roleplayers
- Enforcement
- POPIA + Technology
- Implementation

LegalSkills+

Conditions for Lawful Processing

- Accountability
- Processing Limitation
- Processing Specification
- Further Processing Limitation
- Information Quality
- Openness
- Security Safeguards
- Data Subject Participation

LegalSkills+

1 Accountability

The responsible party is ultimately responsible for ensuring that all the conditions for lawful processing are met, both when deciding how to process personal information and throughout the entire processing lifecycle.

General Principles

- Emphasis on accountability for compliance with ALL requirements.
- Demonstrate full compliance with every aspect of POPIA, from collection data to deletion or destruction.
- Extends beyond responsible party's own actions, and includes any parties engaged (e.g. operators).
- Responsible party bears the burden of proof.

LegalSkills+

2 Processing Limitation

↘

This condition sets boundaries on **how** the responsible party can process personal information, even if it has a valid reason to do so.
Two components: **Lawfulness and Reasonableness**, and **Minimality**

Lawfulness + Reasonableness

- Lawful: compliant with ALL South African laws, not just POPIA
- Reasonable: done in a way that respects the privacy of the data subject and isn't overly intrusive or harmful

Minimality

- Only collect and process personal information that's absolutely necessary for the specified purpose.
- “Just enough”

LegalSkills+

Compliance Questions

- Is there any law preventing me from processing this information in the way I plan?
- Do I really need this specific piece of information to achieve my purpose?

LegalSkills+

3 Purpose Specification

↘

Two components:

1. Collecting personal information
2. **Data management**: how long personal information can be retained and restrictions around processing

General Rule

- Personal information should not be kept for longer than necessary to achieve the purpose for which it was collected.
- When you no longer have a valid reason to keep the data, POPIA mandates that you must destroy or delete it so thoroughly that it can't be reconstructed.

Exceptions (when to retain information)

- Required by law
- Legitimate purposes
- Contractual stipulation
- Consent
- Information is anonymised and used for specific, allowed purpose

LegalSkills+

3 Purpose Specification

↘

Two components:

1. **Collecting personal information**
2. Data management

General Rule

- Responsible party must have a clear, specific, and lawful reason for collecting personal information.
- This reason must be directly related to the responsible party's functions or activities.

Exceptions

- Discussed in Part 2 of the series.

LegalSkills+

Compliance Questions

- Do I have a lawful reason for retaining this personal information?
- If I no longer need the information for its original purpose, should I destroy, delete, or de-identify it?
- Why am I collecting this information, and is it for a specific, lawful purpose related to my organisation's activities?

LegalSkills+

4 Further Processing Limitation

↘

Guides the use of personal information beyond the initial collection stage.

Guidelines for assessing compatibility

- Relationship between the original purpose and the new purpose. *Are they closely related or completely different?*
- Type of personal information. *Is it sensitive data that requires extra care?*
- Assess the potential impact on the data subject. *Will this further processing surprise or harm them in any way?*
- Consider how the information was originally collected. *Was it with a specific promise or expectation about how it would be used?*
- Take into account any contractual obligations regarding the use of the personal information.

LegalSkills+

4 Further Processing Limitation

↘

The further processing of personal information must always be justifiable in light of the original purpose for collection. POPIA recognises that sometimes further processing might be necessary or justifiable, even if it's not directly related to the original purpose.

Situations where further processing is allowable

- **Consent**
- **Public Information** or available in a public record
- **Legal Necessity**, such as court process or statutory compliance
- **Public Interest**, such as preventing crime, protecting public health, or ensuring national security
- **Threat Mitigation**, in the case of a serious or imminent threat to public health and safety, or the life or health of the data subject or another person
- **Research or Statistical Purposes**, if the data anonymised and used only for research
- **Exemption Granted** under section 37 of POPIA

LegalSkills+

Compliance Questions

- Does my current use of this information directly align with the reason I originally collected it?
- If not, is there another lawful basis under POPIA that allows me to use it for this new purpose?

LegalSkills+

5 Information Quality

↘

a responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary

Key Principles

- POPIA does not define “reasonably practicable”.
- Focus on what is sensible and practical ***in your circumstances***.
- Experts suggest a formal system.
- "Reasonably practicable" will vary depending on the nature of your business, the type of data you hold, and the resources available to you.
- **Strive for accuracy.**

Compliance Questions

- Is it feasible for me to implement a formal system for checking all my data?
- If not, what other steps can I take to ensure accuracy within my means?

LegalSkills+

6 Openness

↘

Two components

- Documentation: This requirement is found under section 17 of POPIA, which in turns directs us to sections 10 and 51 of PAIA.
- **Notification**: The responsible party must take reasonably practicable steps to ensure that the data subject is aware of certain factors when their information is being collected.

Reasonably Practicable Steps

- Meet requirements of **section 18** of POPIA.
- Best approach: well-crafted privacy policy can serve as notification.

Information to be included in notification

- Section 18 of POPIA provides extensive checklist.
- Who: Your organisation's name and contact details.
- What: Types of personal information you collect and how you collect it.
- When and Where: Whether data is collected directly from the individual or from other sources
- Why: The purposes for which you're collecting and using the information.
- How: What you do with the data, whether it's transferred overseas, and the security measures you have in place
- Additional Rights

LegalSkills+

6 Openness: *Notification*

↘

As a general rule, you need to inform data subjects about your data practices at the time you collect their information. If you're getting information from someone else, you must notify the data subject as soon as reasonably possible afterwards. But there are exceptions.

Exceptions

- Consent
- Not notifying them wouldn't harm their interests.
- Necessary for legal reasons, like preventing crime or complying with a court order.
- Notification would interfere with a legitimate purpose, such as crime prevention.
- Not reasonably practicable to notify them, given the circumstances.
- If the information is used in a way that doesn't identify the individual, like anonymised research data.

LegalSkills+

Compliance Question

- Have I provided adequate notice to all the data subjects whose information I am processing?

LegalSkills+

7 Security Safeguards

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent unauthorised access, and accidental loss or damage.

Data Protection + POPIA

Key Terminology

- **Technical Measures**, such as firewalls, encryption, access controls, regular software updates
- **Organisational Materials**, such as policies, procedures, training programs

Identifying and Mitigating Risks

- Conduct regular audits of your systems and processes.
- Identify potential vulnerabilities, like weak passwords or outdated software.
- Implement targeted safeguards.
- Continuously monitor and update security measures as new threats emerge.

LegalSkills+

7 Security Safeguards

↘

The Responsible Party still retains all its obligations even if an Operator processes personal information on its behalf.

Monitoring Operators

- Have a written contract with the operator that clearly outlines their data protection obligations.
- Require the operator to implement security measures that are in line with POPIA's standards.
- Make sure the operator provides immediate notice if they suspect a security compromise.

LegalSkills+

7 Security Safeguards

↘

Section 22 of POPIA contains notification requirements in the event of data breaches, leaks and hacks.

More on this later...

- Notify Information Regulator and, usually, data subjects.
- Specific requirements for the content and timing of the notification.

Compliance Questions

- Have I conducted a thorough risk assessment of my data processing activities?
- Do I have appropriate technical and organisational measures in place to address those risks?

Compliance Questions

- Are my security measures regularly reviewed and updated to keep pace with evolving threats?
- If I use operators, do my contracts with them adequately address data protection and security?

Compliance Questions

- Do I have a clear plan for responding to and notifying stakeholders in the event of a security compromise?

LegalSkills+

8 Data Subject Participation

↘

Data Subject participation involves the rights of Data Subjects in relation to their personal information.

More on this later...

- Sections 23 to 25 of POPIA.
- Rights to access, rectification, and the specific manner in which access to information must be granted.

LegalSkills+

Conditions for Lawful Processing

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- **Special Cases**
- Key Roleplayers
- Enforcement
- POPIA + Technology
- Implementation

LegalSkills+

Special Cases

- Special Personal Information
- Employment Relationships
- Children's Information
- Direct Marketing
- Prior Authorisation
- Transborder Information Flows

LegalSkills+

Special Personal Information

↘

Special personal information includes information that, if mishandled, could lead to significant harm or discrimination. Sensitivity is the common thread.

What is it?

- *the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or*
- *the criminal behaviour of a data subject to the extent that such information relates to—*
  - *the alleged commission by a data subject of any offence; or*
  - *any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.*

LegalSkills+

Special Personal Information

↘

General rule: You cannot process special personal information without explicit consent from the data subject. There are additional requirements to process special personal information, and unique provisions for each category of special personal information, outlining when and how it can be processed.

Exceptions to the General Rule

- Medical treatment or healthcare administration
- Compliance with employment or social security laws
- Legal proceedings
- Protect someone's life
- For specific purposes like historical research or statistical analysis, with appropriate safeguards.

Requirements for Processing

- Stricter Consent Requirements: Consent must be explicit and unambiguous.
- Purpose Limitation: The information can only be used for the specific purpose for which it was collected.
- Heightened Security: Stringent measures required.

LegalSkills+

The Employment Relationship

↘

In the employment context, consent may not always be required. Processing personal information may be lawful if it's necessary for the performance of an employment contract or for complying with legal obligations, like tax reporting.

Measures for Compliance

- Clear Contracts
- Privacy Policies
- Regular Training
- Data Security Measures
- Incident Response Plan

Special Personal Information

- Obtain the employee's explicit consent or establish a legal basis for processing this type of information.

Vicarious Liability

- If an employee mishandles personal information, the employer could be liable for any resulting harm

LegalSkills+

Children's Information

↘

General Rule: you cannot process a child's personal information without the prior consent of a competent person (someone who is legally able to consent on behalf of the child, such as a parent or legal guardian). *See sections 34 and 35 of POPIA*.

Exceptions to the General Rule

- Legal Necessity
- Public Interest
- Publicly Available Information
- Specific Authorisation

Additional Safeguards

- Allowing the competent person to review and refuse further processing of the child's information.
- Providing clear notice about how the information is being collected and used.
- Avoiding actions that pressure a child to disclose more information than necessary.
- Maintaining strict confidentiality and security measures to protect the child's data.

LegalSkills+

Direct Marketing

↘

Definition: approaching a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of promoting or offering to supply, in the ordinary course of business, any goods or services, or requesting a donation.

General Rule

The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication is prohibited unless the data subject has **consented** or is a **customer**.

Electronic Communication

- Electronic: automatic calling machines, facsimile machines, SMSs, e-mail
- Not electronic: phone calls from a human, flyers - **different considerations apply**

Existing Customer

- Purchased product or service from responsible party
- Goods and services being marketed are similar

LegalSkills+

Prior Authorisation

The responsible party must obtain prior authorisation from the Regulator, in terms of section 58, prior to any processing in certain cases. This means that it will not be sufficient to comply with the eight conditions for lawful processing , and prior authorisation to process is required.

When is Prior Authorisation required?

- Use unique identifiers for a different purpose
- Process information about criminal behavior on behalf of others
- Engage in credit reporting
- Transfer special personal information or children's data to another country

Prior Authorisation Process

- Notify the Information Regulator about intended processing and provide requisite details.
- Regulator assesses application and decides whether to grant authorisation.
- Only one application is needed.
- Where Prior Authorisation is required, it is a crime to process information without such authorisation.

LegalSkills+

Transborder Information Flows

↘

Transborder information flows entail transferring personal information to countries outside of South Africa. The requirements related to transborder information flows are contained under section 72 of POPIA.

Duty of Care

- A responsible party must ensure that the recipient country has adequate data protection laws in place.
- If the recipient country doesn't have adequate laws, the transfer is generally prohibited unless certain conditions are met, such as consent or contractual necessity.

Key Considerations

- Assess the Recipient Country
- Implement Safeguards
- Obtain Consent (or establish an alternate ground)
- Document the Transfer

LegalSkills+

Special Cases

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- Special Cases
- **Key Roleplayers**
- Enforcement
- POPIA + Technology
- Implementation

LegalSkills+

Key Roleplayers

- Data Subject
- Responsible Party
- Information Officer
- Operator

LegalSkills+

Data Subject

↘

Definition: *the person to whom personal information relates*

Data Subject Rights

The right to:

- Be Informed
- Access
- Rectification
- Deletion
- Object to Processing
- Restrict Processing
- Data Portability
- Object to Automated Decision-Making

Remedies

- Internal resolution
- Lodge complaint with Information Regulator
- Civil action

LegalSkills+

Responsible Party

↘

Definition: *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*

Key Takeaways

- The responsible party bears the obligation to comply with all conditions for lawful processing under POPIA and the onus to prove compliance.
- Non-compliance could result in hefty fines and even imprisonment.
- No definitive test to identify the responsible party. Consider asking "*Who decides the purpose and methods of processing personal information?*"
- **Joint responsible parties**, proposed guideline:
  - The processing operation would be impossible without the participation of both parties.
  - Their involvement in determining the purposes and means of processing is inseparable.

LegalSkills+

Information Officer

An Information Officer ensures an organisation's compliance with data protection laws and manages personal information processing.

Requirements

- Public body: statutorily determined.
- Private body: head of organisation - but the responsibility may be delegated.
  - Must hold executive level position.
- For multinational entities outside South Africa, the Information Regulator requires a locally-based representative to act as the Information Officer.
- Deputy information officers may be appointed.
- Information officers and deputies must register with the Regulator

Responsibilities

- Responding to Inquiries
- Internal Compliance Champion
- Training and Awareness Advocate
- Cooperation and Reporting

LegalSkills+

Operator

↘

Definition: *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*

Elements

- Processes information on the instructions of a responsible party
- Does not come under the direct authority of the responsible party
- Acts in accordance with a contract or mandate

Considerations for Responsible Parties

- Only work with reputable third parties
- Conduct due diligence before appointing operators
- Ensure contracts are clear and easily enforceable
    - If you're handing over large volumes of data, account numbers, or special personal information, seek legal assistance to ensure your contracts are in order

LegalSkills+

Key Roleplayers

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- Special Cases
- Key Roleplayers
- **Enforcement**
- POPIA + Technology
- Implementation

LegalSkills+

Enforcement

- Information Regulator
- Enforcement
- Offences + Penalties

LegalSkills+

Information Regulator

The Information Regulator is an independent body established under POPIA to monitor and enforce compliance with data protection laws, ensuring the protection of personal information and promoting access to information.

Structure

- **Chairperson**: Leads the Regulator and oversees its functions
- **Four Ordinary Members**: Support the Chairperson in executing the Regulator's mandate
- **Chief Executive Officer**: Manages day-to-day activities
- **Divisions**: Responsible for specific operational areas
- **Enforcement Committee**: Assists in investigating and resolving complaints

Roles

- Educator
- Investigator
- Advisor

LegalSkills+

Information Regulator

↘

Sections 39 to 54 offer substantial on the Information Regulator, including its structure, powers, and duties

Powers

- **Monitoring compliance**
  - It actively tracks POPIA compliance throughout South Africa.
- **Investigating complaints**
  - It has the authority to dig deep into complaints and conduct its own investigations
- **Issuing Codes of Conduct**
- **Enforcing the provisions of POPIA**
  - If it finds a violation, it can issue warnings, impose fines, or even refer cases for criminal prosecution.

LegalSkills+

Enforcement

↘

Enforcement involves the Information Regulator monitoring compliance, investigating breaches, issuing enforcement notices, and imposing penalties, including fines up to ZAR 10 million or imprisonment, to ensure adherence to data protection laws

Enforcement Process

- **Lodging a Complaint**
  - Data subject submits a written complaint to the Information Regulator
- **Initial Assessment**
  - Regulator acknowledges and assesses the complaint's validity
- **Investigation**
  - Regulator investigates, gathering information from involved parties
- **Enforcement Actions**
  - Options include resolution (settlement), referral to Enforcement Committee
- **Appeals**
  - Either party can appeal through an internal review or court
- Regulator may elect not to proceed further at any stage

LegalSkills+

Enforcement *Pro Tips*

↘

What do you do when you’re a complainant or respondent in an enforcement process?

Consider the Regulator's Rules of Procedure available on its website for detailed guidance on these processes.

Complainant

- Be clear about your concerns
- Provide evidence you have
- Cooperate with the Regulator's investigation.
- For damages, seek professional legal assistance or do your best to substantiate, in as much detail and with documentary evidence, your damages claim

Respondent

- Respond promptly and thoroughly to the Regulator's requests
- Be cooperative and transparent
- If you think the complaint has any merit, immediately seek legal advice

LegalSkills+

Enforcement *Notices*

↘

Information Notice: A directive from the Information Regulator requesting specific information from a responsible party.
Enforcement Notice: An order issued by the Information Regulator mandating corrective actions for non-compliance.

Information Notice

- Request for information, usually indicative of an investigation by the Regulator
- Respond promptly, thoroughly, honestly
- Ignoring the notice is an offence

Enforcement Notice

- Legal order that requires you to take specific steps to fix a POPIA violation
- Contains compliance deadline

General

- Decision to issue notice may be appealed
- Seek legal advice if any notice is received

LegalSkills+

Enforcement
Direct Access

POPIA allows you to directly approach the court and sue the responsible party for damages. You may also petition the Regulator to sue a responsible party on your behalf.

LegalSkills+

Offences + Penalties

POPIA's penalties cover a wide spectrum, from administrative fines to criminal charges, reflecting the gravity of data protection in South Africa.

Offences + Penalties

Serious Offences

↘

For the most egregious violations, POPIA outlines serious offences that can result in a hefty fine, imprisonment for up to 10 years, or both.

Examples of Serious Offences

- Obstructing or hindering the Information Regulator's work.
- Giving false evidence under oath during an investigation.
- Failing to comply with an enforcement notice issued by the Regulator.
- Illegally obtaining, disclosing, or selling sensitive financial information like account numbers.

Offences + Penalties
Less Serious Offences

↘

Less serious offences can result in fines, imprisonment for up to 12 months, or both

Examples of Less Serious Offences

- Not getting prior authorisation when required (we covered this in Part 4).
- Breaching confidentiality obligations.
- Obstructing the execution of a warrant, and
- Providing false information to the Regulator.

LegalSkills+

Offences + Penalties

↘

On top of criminal penalties, the Information Regulator can issue administrative fines. Responsible parties can also face civil liability.

Administrative Fines

- Fines of up to ZAR 10 million
- Direct penalties, separate from any criminal charges
- The amount of the fine depends on factors like the severity of the violation, how long it lasted, and how many people were affected

Civil Liability or Civil Damages

- Data subjects who have suffered harm or damages may sue a responsible party for POPIA breaches

Additional Considerations

- Contractual Liability
- Reputational Harm

LegalSkills+

Enforcement

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- Special Cases
- Key Roleplayers
- Enforcement
- **POPIA + Technology**
- Implementation

LegalSkills+

Technology + POPIA

- Cookies
- Big Data
- Automated Decision Making
- AI
- Social Media
- Search Engines
- Websites

LegalSkills+

Cookies

Cookies are small data files stored on your device by websites to remember your preferences, login details, and browsing activity. They can collect personal information, such as IP addresses and login details.

Purpose

Enables personalised content and enhances user experience through Functionality and Tracking

Types

- Session Cookies: Temporary
- Persistent Cookies: Longer period
- First-Party Cookies: Set by website you visit
- Third-Party Cookies: Set by other companies, whose content is embedded on the website you're visiting

Practical Impact

- Consent is required for non-essential cookies
- Websites should have clear cookie notices and policies

LegalSkills+

Big Data

↘

Big Data refers to extremely large and complex datasets that traditional data processing applications cannot handle efficiently, characterised by high volume, velocity, and variety.

Purpose

Mainly used to analyse different sets of data to identify patterns

Practical Impact

- Volume and variety of data being collected can make it difficult to protect individual privacy.
- POPIA principles of **purpose limitation** and **data minimisation**, are especially relevant.
- Organisations who process Big Data should:
  - Be transparent about collection and use
  - Ensure they have a lawful basis for processing
  - Implement strong security measures
  - Anonymise or deidentify data where possible

LegalSkills+

Profiling

Profiling refers to the process of analysing data to understand its structure, content, and quality. This involves examining datasets to identify patterns, anomalies, and relationships, ensuring data integrity and suitability for various applications.

Purpose

Profiling is commonly used for predictive analytics, underscoring activities such as targeted ads, credit scoring, and insurance risk assessment.

Risks

Can lead to unfair discrimination, unfair treatment, and a loss of control over your personal information.

POPIA's Protections

- Organisations must be transparent about their profiling activities.
- Individuals have the right to object to processing based on profiling.
- Automated decision making based on profiling alone is prohibited.

LegalSkills+

Automated Decision Making

↘

Automated decision-making refers to decisions made solely through automated processing of personal information, without human intervention.

Purpose

Automated decision making is used to analyse large and complex volumes of data and arrive at quick conclusions, enhancing efficiency.

Risks

Can lead to issues around fairness, transparency, and the potential for discrimination.

POPIA's Protections

- Prohibition on a data subject being subject to a decision with legal consequences for that data subject or which affects them to a substantial degree if that decision is based solely on automated processing.

LegalSkills+

Artificial Intelligence (AI)

↘

AI is the simulation of human intelligence processes by machines, especially computer systems, enabling them to perform tasks like learning, reasoning, and problem-solving.

Purpose

AI can be a valuable tool for enhancing data protection, such as by detecting and preventing fraud. However, it can also be used to create highly detailed profiles of individuals, potentially leading to discriminatory or harmful outcomes.

Practical Impact

- **Sharing information with AI is still processing under POPIA.**
- Organisations must be upfront about how they use AI, ensure human oversight of AI systems, and take steps to mitigate bias and discrimination.
- No person should share personal information with AI models unless there is a lawful basis to do so.

LegalSkills+

Social Media

↘

Social media refers to digital platforms and applications that enable users to create, share, and interact with content and each other online.

User Impact

Users can be both data subjects and responsible parties, depending on the context.

Liability

- Users and social media platforms can face liability.
- Platforms can be fined or prosecuted for failing to protect user data.
- Users can face consequences for misusing others' personal information.

Practical Impact

- Adjust privacy settings.
- Don’t share personal information about any third party.
- Report privacy concerns to the Regulator.

LegalSkills+

Search Engines

Search engines, like Google, play a crucial role in how we access information online. They also collect and process vast amounts of personal data to deliver their services and personalise our experiences.

How do search engines gather data?

- Search Queries
- Clickstream Data
- Location Data
- Device Information

Privacy Implications

- Search engines can build detailed profiles of users, which can be used for targeted advertising or other purposes.
- Personalisation can be convenient, but raises concerns about privacy and the potential for misuse of personal information.
- *Google Spain SL v AEPD and Maria Costeja Gonzalez*: Established that search engine operators are considered "controllers" (or responsible parties in POPIA speak) under data protection law.

LegalSkills+

POPIA for your Website

↘

If your website collects personal information, you need to ensure it complies with POPIA

Must-Have

- Privacy Policy
- Cookie Notice and Policy
- PAIA Manual

Must-Do

- Implement appropriate security measures to protect personal information from unauthorised access, loss, or damage.
- Have a plan in place to respond to any security breaches promptly and effectively, and
- Educate your staff on POPIA's requirements and the importance of data protection.

LegalSkills+

POPIA + Technology

Conclusion

LegalSkills+

Data Protection + POPIA

- Introductory Concepts
- Foundations for Lawful Processing
- Conditions for Lawful Processing
- Special Cases
- Key Roleplayers
- Enforcement
- POPIA + Technology
- **Implementation**

LegalSkills+

Implementation

- Privacy Policy
- PAIA Manual
- Impact Assessments
- General Tips
- Handling Complaints
- Security Compromises

LegalSkills+

Drafting your Privacy Policy

↘

While POPIA doesn't explicitly require a privacy policy, it's essential for fulfilling your transparency obligations under the law. Remember, data subjects have the right to know what you're doing with their personal information. A well-crafted privacy policy is the best way to meet this requirement.

What information should be included?

- Types of Personal Information Collected
- Collection Methods
- Use and Protection of Data
- Data Subject Rights
- Choice and Consent
- Cookie Use
- Your Contact Information
- Effective Date

Drafting Tips

- Avoid legal jargon
- Be concise, skip unnecessary details
- Consider a layered approach
- Make it easy to read
- Make it easy to find
- Get legal advice

LegalSkills+

Drafting your PAIA Manual

↘

Required under the Promotion of Access to Information Act (PAIA), your PAIA Manual explains how someone can request information, what kind of information they can access, and the procedures involved.

Contents

- Note: template PAIA Manuals are available on the Regulator's website
- **Sections 10 and 51 of PAIA specify the information that should be contained in a PAIA Manual**
- In summary:
  - Contact Information for your information
  - Categories of records available without a formal request
  - Sufficient detail to help someone understand what kind of information you hold and how it's categorised
  - POPIA-specific information
- Your organisation may need a more comprehensive PAIA Manual, especially if your processing activities are potentially high-risk.

LegalSkills+

Impact Assessments

↘

An impact assessment is a process that helps you identify and understand the potential risks your organisation's activities pose to the privacy and protection of personal information.

How often should you conduct these?

- Periodically (every 6 to 12 months)
- Launching new projects or initiatives that involve personal information.
- Implementing new technologies or systems.
- Making significant changes to your existing data processing activities.

Questions to answer

- What kind of personal information are we processing?
- How are we collecting it?
- Why are we processing it?
- Who has access to the data?
- How are we protecting it?
- What could go wrong (what are the risks)?
- What can we do to reduce those risks?

LegalSkills+

General Tips

↘

These general tips will help you strengthen your compliance framework.

Tips

- **Tip 1**: **Make consent forms clear and easy to understand.**
  - Explain purpose and intended use clearly.
  - Be specific and get separate consent where you can.
  - Use plain language.
  - Make it voluntary.
  - Have a clear withdrawal mechanism.
- **Tip 2: Improve your contracts.**
  - Include clauses that address confidentiality, data security measures to be maintained by the other party, data breach notification requirements, indemnifications for their non-compliance
- **Tip 3**: **Keep excellent records.**
  - Track consents obtained and withdrawn, all processing activities, data breaches

LegalSkills+

Dealing with Complaints

↘

Scenario: **the data subject has complained directly to you**

Tips

- **Acknowledge the Complaint**
  - Respond promptly, even if it's just to say you're looking into the matter.
- **Investigate Thoroughly**
  - Gather all relevant information, including any supporting documentation provided by the complainant.
- **Communicate Transparently**
  - Be open and honest about your findings.
- **Take Corrective Action**
  - If the complaint is valid, take appropriate steps to rectify the situation.
- **Outline and Follow Clear Processes**
  - Identify the person responsible for handling the complaint and ensure the process is easy for the complainant.

LegalSkills+

Dealing with Complaints

↘

In the best case scenario, a complainant will approach you directly. The complainant is not obliged to do so and may approach the Regulator directly. If they approached you first, they may still approach the Regulator if they find the outcome unsatisfactory.

What to do when you receive a complaint directly

- **Acknowledge the Complaint**
  - Respond promptly, even if it's just to say you're looking into the matter.
- **Investigate Thoroughly**
  - Gather all relevant information, including any supporting documentation provided by the complainant.
- **Communicate Transparently**
  - Be open and honest about your findings.
- **Take Corrective Action**
  - If the complaint is valid, take appropriate steps to rectify the situation.
- **Outline and Follow Clear Processes**
  - Identify the person responsible for handling the complaint and ensure the process is easy for the complainant.

LegalSkills+

Handling Security Compromises

↘

When a security compromise occurs, swift action is essential. Ideally, a security compromise policy should be in place. If not, POPIA clearly outlines the required steps that must be taken.

Steps to Take (POPIA)

- **Notification**
  - **The Information Regulator**
    - Include details about the nature of the breach, the number of data subjects affected, and any potential consequences.
  - **The individuals whose personal information was compromised (in writing)**
    - Unless their identity cannot be established or if law enforcement believes notification would impede a criminal investigation
    - Include sufficient information for individuals to protect themselves and steps they can take to mitigate against risk or harm
- **Containment and Recovery**
- **Investigation**
- **Remediation**
- **Documentation**

LegalSkills+

Implementation

Conclusion

LegalSkills+

Data Protection Series

Thank you.

Website
lawcoach.co.za