PAIA and POPIA Manual

Prepared in terms of the Promotion of Access to Information Act (PAIA) 2 of 2000 and Protection of Personal Information Act (POPIA) 4 of 2013

Date of Compilation: July 29, 2023

Date of Revision: July 29, 2023

ADGSTUDIOS

Contents

1 Introduction

In today's information-driven world, organizations' data management practices are foundational to their operations. Transparent governance and the safeguarding of personal information are paramount. South Africa's response to this global challenge is the enactment of the Promotion of Access to Information Act (PAIA) 2 of 2000 and the Protection of Personal Information Act (POPIA) 4 of 2013.

PAIA promotes transparency and accountability across both public and private sectors. It empowers individuals to understand institutional decision-making processes that impact their rights. By granting citizens access to information, PAIA ensures institutions align with the democratic values of the South African Constitution.

Conversely, POPIA addresses data protection in our digital age. As organizations handle vast amounts of personal information, the potential for misuse grows. POPIA establishes principles for personal information processing, ensuring organizations respect privacy rights, prevent data breaches, and maintain data integrity.

This manual reflects ADGSTUDIOS' commitment to these principles, offering clarity on our processes, responsibilities, and the rights of our stakeholders. By adhering to PAIA and POPIA, we foster trust, build stronger relationships, and lay a foundation for sustainable growth in the evolving information landscape.

2 PAIA Manual

2.1 Purpose of PAIA

The Promotion of Access to Information Act (PAIA) 2 of 2000 stands as a landmark piece of legislation in South Africa's democratic journey. Its inception is rooted in the broader global movement towards transparency, openness, and accountability in governance and institutional operations. The Act is not just a legal instrument but a reflection of the nation's commitment to the principles enshrined in its Constitution, particularly the right to access information.

At its core, PAIA seeks to give effect to the constitutional right of access to any information held by the state and any information held by another person that is required for the exercise or protection of any rights. This right is not just a theoretical construct but a practical tool that empowers citizens to scrutinize, understand, and, if necessary, challenge the actions and decisions of both public and private entities.

One of the primary purposes of PAIA is to promote transparency and accountability in public administration. In a democratic society, public bodies are accountable to the citizens they serve. By granting individuals the right to access information, PAIA ensures that the public can understand the decision-making processes, policies, and actions of these bodies. This transparency ensures that corruption, inefficiencies, and any other malpractices can be identified, challenged, and rectified.

Furthermore, PAIA recognizes that the right to access information is not just crucial for public bodies but also for private entities. In an age where corporations and private institutions wield significant power and influence, the Act ensures that their operations do not infringe upon the rights of individuals or the broader public interest. Whether it's understanding the environmental practices of a company, the data handling procedures of a tech firm, or the financial dealings of a private institution, PAIA ensures that private entities operate with a degree of transparency.

Moreover, PAIA serves as a tool for the realization of other rights. Whether it's the right to a clean environment, the right to housing, or the right to health, access to information is often the first step in understanding, asserting, and realizing these rights. For instance, a community facing environmental degradation due to industrial activities can use PAIA to access information about the pollutants being released, enabling them to take informed actions to protect their environment.

In conclusion, the Promotion of Access to Information Act is not just about accessing documents or data. It's about strengthening the pillars of democracy, ensuring that power is exercised responsibly, and providing citizens with the tools they need to participate actively and meaningfully in the democratic process. It underscores the belief that information is a powerful tool, and when wielded responsibly, it can shape societies, protect rights, and foster a culture of accountability and openness.

2.2 Access to Information

The Promotion of Access to Information Act (PAIA) establishes a clear framework for individuals and entities seeking access to records held by both public and private bodies. The process is designed to be user-friendly, ensuring that the right to information is not just a theoretical construct but a practical tool that can be exercised by all citizens.

1. Request Procedure - To access information, a requester must use the prescribed form provided by the relevant body. This form typically requires the requester to provide sufficient particulars to enable the information officer of the public or private body to identify the record being requested and the requester. - The requester must also indicate the form in which they wish to access the record (e.g., viewing, copying, or receiving a digital copy). - If the request is made on behalf of another person, the requester must provide proof of the capacity in which they are making the request.

2. Fees: - There might be a request fee associated with seeking information, especially from private bodies. If the search for the record requires more than the prescribed hours (usually six hours), a deposit may be required. - Once the information is ready to be accessed, an access fee might be charged, covering the reproduction of the information, search and preparation time, and, if applicable, any time spent arranging to view the document.

3. Timeframes: - Public bodies are generally required to decide on a request within 30 days, while private bodies have 60 days. These timeframes can be extended under certain circumstances.

4. Grounds for Refusal: - PAIA does outline specific grounds on which a request can be refused, including but not limited to: protection of the privacy of a third party, protection of commercial information of a third party, or if the record would result in the disclosure of a trade secret. - If a request is denied, the body must provide reasons for the refusal, and the requester has the right to appeal the decision.

5. Appeals: - If a requester is not satisfied with the response or if no response is received within the stipulated timeframe, they can lodge an internal appeal if the information is held by a public body. For private bodies, the requester can approach the courts for relief. - The Information Regulator, established under the Protection of Personal Information Act (POPIA), also plays a role in addressing grievances related to information access.

In conclusion, while the right to access information is enshrined in PAIA, it is essential for requesters to understand the procedural aspects to exercise this right effectively. By following the prescribed steps and being aware of their rights and responsibilities, individuals can ensure that they harness the power of information to uphold democratic values, promote transparency, and protect their rights.

2.3 Fees and Charges

The Promotion of Access to Information Act (PAIA) recognizes that while the right to access information is fundamental, there are administrative costs associated with providing such access. To strike a balance between ensuring the right to information and covering the administrative expenses, PAIA has established a fee structure for requesting and accessing records. Here's a breakdown of the potential fees and charges:

1. Request Fees: - For public bodies: There is typically no request fee for personal requests, meaning if an individual is seeking information about themselves. However, for other requests, a nominal fee might be charged. - For private bodies: A request fee is usually applicable. This fee is meant to cover the initial administrative costs of locating and compiling the requested record.

2. Access Fees: - These fees are charged once the request has been approved and before the information is accessed or provided. The access fee covers the actual costs of reproduction and any time spent searching and preparing the record for disclosure. - The fee might vary based on the format in which the record is provided. For instance, fees for a digital copy might differ from a printed or photocopied document. - If the preparation time required to search, retrieve, prepare, and provide the record exceeds the prescribed hours (usually six hours), additional fees may be charged.

3. Deposit: - If the requester is informed that they need to pay an access fee and the fee exceeds a certain threshold (often double the request fee), the information officer may require the requester to pay a deposit, usually one-third of the access fee.

4. Waiver or Reduction of Fees: - In certain circumstances, the information officer may waive or reduce the request or access fees. This is typically considered if the requester is indigent or if paying the fees would cause financial hardship. Additionally, if the information being requested is in the public interest, fees might be waived.

5. Payment Methods: - Fees can usually be paid via bank draft, money order, or electronic transfer to the respective ADGSTUDIOS (PTY) LTD valid payment channel.

6. Refunds: - If a request is refused after a deposit has been paid, the deposit should be refunded to the requester.

In conclusion, while PAIA ensures the right to access information, it also establishes a fee structure to cover the administrative costs associated with this right. Requesters should be aware of these potential fees and charges and should inquire about the exact amounts and payment methods when making a request. It's also worth noting that these fees are subject to change, and it's advisable to consult the latest fee regulations or the respective body's information officer for the most up-to-date information.

3 POPIA Manual

3.1 Purpose of POPIA

The **Protection of Personal Information Act (POPIA) 4 of 2013** is a seminal piece of legislation in South Africa, addressing the pressing need for data protection in an increasingly digitalized world. As the volume of personal data being collected, processed, and stored by organizations grows exponentially, so does the potential for misuse, breaches, and violations of privacy rights. POPIA was enacted to address these challenges and to ensure that South Africa upholds the highest standards of data protection.

At its core, POPIA seeks to protect the personal information of individuals, ensuring that such information is processed in a manner that respects the rights and dignity of the data subjects. The Act achieves this by introducing a set of principles and requirements that organizations must adhere to when processing personal information.

1. **Rights of Data Subjects**: One of the primary purposes of POPIA is to give effect to the constitutional right to privacy by safeguarding personal information. The Act ensures that data subjects are informed about the collection, processing, and storage of their personal data. They have the right to access their data, correct inaccuracies, and object to processing under certain circumstances.

2. **Accountability**: Organizations that process personal information are held accountable for complying with the Act's provisions. They must ensure that adequate measures are in place to protect the data and that any breaches are promptly addressed and reported.

3. **Data Processing Principles**: POPIA introduces eight core principles that guide the processing of personal information. These principles cover aspects such as data minimization, purpose specification, and data quality, ensuring that personal information is processed lawfully, fairly, and transparently.

4. **Cross-border Data Transfers**: In an interconnected world, personal data often flows across borders. POPIA sets out conditions for the transfer of personal information outside South Africa, ensuring that the data remains protected even when processed in other jurisdictions.

5. **Regulatory Oversight**: The Act establishes the Information Regulator, an independent body tasked with monitoring and enforcing compliance with POPIA. The Regulator plays a crucial role in providing guidance, addressing complaints, and ensuring that organizations uphold the principles of the Act.

In conclusion, the Protection of Personal Information Act is not just about setting rules for data processing. It's about recognizing the inherent dignity and rights of individuals in the digital age. It's about ensuring that as technology evolves, the principles of privacy, transparency, and accountability remain at the forefront. Through POPIA, South Africa has taken a decisive step towards creating a framework that respects the rights of data subjects, promotes responsible data practices, and ensures that organizations are held accountable for the trust placed in them by individuals.

3.2 Protection of Personal Information

In the digital age, the protection of personal information is paramount. With the increasing volume of data being processed and stored, it becomes essential to implement robust security measures to safeguard this data against unauthorized access, breaches, and potential misuse. Our organization adopts a multi-layered approach to data protection, leveraging state-of-the-art technologies and best practices.

1. **Encrypted Databases**: We utilize leading cloud service providers, including Azure, AWS, and Google, to host our databases. These platforms come with built-in encryption capabilities, ensuring that data at rest is encrypted. This means that

even if someone were to gain unauthorized access to the physical storage, the data would remain unreadable without the decryption keys.

2. **Environment Variables for Connection Strings**: Storing sensitive information, such as database connection strings, directly in application code can expose it to potential threats. To mitigate this, we store connection strings as environment (ENV) variables. This practice ensures that the connection strings are not exposed in the application's source code and are only accessible to authorized personnel and processes.

3. **Hashed Connection Strings**: To add an additional layer of security, our connection strings are hashed. Hashing is a one-way cryptographic function that transforms data into a fixed-size series of bytes. By hashing the connection string, we ensure that even if an attacker gains access to the ENV variables, they cannot reverse-engineer the original connection string.

4. **Data Encryption with Private Keys**: Beyond encrypting the database itself, individual data entries within the database are encrypted using private keys. This ensures that each piece of data is uniquely protected. Even if an attacker were to bypass other security measures and access the database, the data would remain encrypted and unreadable without the corresponding private key.

5. **Regular Security Audits and Updates**: Technology and threats evolve rapidly. To stay ahead of potential vulnerabilities, we conduct regular security audits of our systems. These audits help identify any weak points and ensure that we are using the latest security patches and updates provided by our cloud service providers.

6. **Access Control**: Access to personal information is strictly controlled. Only authorized personnel with a legitimate need to access the data can do so. We implement role-based access controls, ensuring that users only have access to the data and functions necessary for their specific roles.

In conclusion, the protection of personal information is a top priority for our organization. Through a combination of advanced technologies, best practices, and a proactive approach to security, we ensure that the personal data entrusted to us remains confidential, secure, and protected against potential threats.

3.3 Data We Store

In our commitment to transparency and in compliance with data protection regulations, we provide a clear overview of the types of data we store and how we handle them. Our primary objective is to offer our services efficiently while ensuring the utmost security and privacy of our users' data.

1. **Login History**: To enhance the security of user accounts and monitor account activities, we track and store the login history of our users. This allows us to detect any unusual or unauthorized access attempts, ensuring that user accounts remain secure.

2. **IP Addresses of Devices**: We record the IP addresses of devices used to access our platform. This data helps in identifying and preventing potential security threats, understanding user behavior, and optimizing our services for different regions.

3. **Credit Payments of Customers**: Financial integrity is crucial for our operations. We track and store the credit payment history of our customers. This allows us to maintain accurate financial records, resolve any payment disputes, and offer better support to our customers.

4. **OAuth for Personal Information**: While we do not directly store names or addresses of our users, we utilize OAuth for authentication. OAuth allows users to grant us permission to access specific information without exposing their entire profile or credentials. This ensures a seamless login experience while keeping user data secure.

5. **Payment Processing via Paygate Companies**: We prioritize the financial security of our users. For processing payments, we collaborate with trusted Paygate companies. These companies handle the intricate details of payment processing, ensuring that transactions are secure and compliant with financial regulations. Our role is to verify the transactions via API, ensuring that the payment process is smooth and reliable for our users. Once verified, we store only the transaction ID in our database, without retaining any sensitive financial information.

6. **Data Minimization Principle**: In line with best practices and data protection principles, we adhere to the principle of data minimization. This means we only collect and store data that is essential for our operations and service delivery. By not storing names, addresses, or other sensitive personal information directly, we reduce potential risks and ensure the privacy of our users.

In conclusion, our data storage practices are designed with the user's privacy and security at the forefront. We continuously evaluate and update our data handling procedures to ensure compliance with best practices and regulatory requirements, ensuring that our users can trust us with their data.

3.4 Rights of Data Subjects

The Protection of Personal Information Act (POPIA) underscores the importance of respecting and upholding the rights of data subjects. These rights are foundational to ensuring that personal information is processed in a manner that is transparent, fair, and respectful of the individual's dignity. Here's a breakdown of the key rights of data subjects under POPIA:

1. **Right to be Informed**: Data subjects have the right to be informed about the collection and use of their personal data. This includes the purpose of processing, the identity of the responsible party, and any potential third-party recipients of the data.

2. **Right of Access**: Individuals have the right to access their personal data. This means they can request a copy of the personal data being processed, as well as other supplementary information about how the data is used.

3. **Right to Rectification**: If personal data is inaccurate or incomplete, data subjects have the right to have it corrected. Organizations must take reasonable steps to ensure that the data they process is accurate and up-to-date.

4. **Right to Erasure (Right to be Forgotten)**: Under certain circumstances, individuals can request the deletion or removal of personal data. This is particularly relevant when there is no compelling reason for the continued processing of the data.

5. **Right to Restrict Processing**: Data subjects can request that the processing of their personal data be restricted. This is an alternative to data erasure and might be used when the individual contests the accuracy of the data or when the processing is unlawful.

6. **Right to Data Portability**: Individuals have the right to obtain and reuse their personal data across different services. This allows them to move, copy, or transfer personal data easily from one IT environment to another.

7. **Right to Object**: Data subjects have the right to object to the processing of their personal data in certain circumstances, such as for direct marketing purposes.

8. **Rights Related to Automated Decision Making and Profiling**: Individuals have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

9. **Right to Complain**: If data subjects believe that their personal data is being processed unlawfully or that their rights under POPIA have been violated, they have the right to lodge a complaint with the Information Regulator.

In conclusion, the rights of data subjects form the cornerstone of POPIA. These rights empower individuals, giving them control over their personal data and ensuring that organizations process this data with the utmost care, transparency, and respect for individual autonomy.

4 Contact Information

For any inquiries or concerns related to the content of this manual or our practices, please reach out to:

- **Information Officer**: Ashlin Darius Govindasamy
- **Email**: adg@adgstudios.co.za
- **Phone**: +27605224922

5 Revision History

Date	Revision Number	Description
July 29, 2023	1.0	Initial draft