REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

Guidance Note for Private Security

2025

TABLE OF CONTENTS

DEFINITIONS

"Act" means the Data Protection Act, No 24. of 2019.

"Consent" means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

"Constitution" means the Constitution of Kenya, 2010.

"Data Commissioner" means the person appointed pursuant to section 6 of the Act.

"Data Controller" means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

"Data Subject" means an identified or identifiable natural person who is the subject of personal data.

"Household Use" means ordinarily acquired or intended for personal or domestic or household consumption'.

"Office" means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"Personal Data" means any information relating to an identified or identifiable natural person.

"**Private Security Service Provider**" means a person or body of persons, other than a state agency, registered under this Act to provide private security services to any person.

"**Private security firms**" means a body corporate, including a partnership, which provides private security services.

"**Private Security Services**" means any of the following services whether performed by an individual or firm—

(a) installation of burglar alarms and other protective equipment;
(b) private investigations and consultancy;
(c) car tracking or surveillance; close-circuit television;
(d) provision of guard dog services;
(e) security for cash in transit;
(f) access control installation; locksmiths; or
(g) any other private security service as may determined from time to time by the Board by a notice in the Gazette;

"Private Security Law" - means the Private Security Regulations Act, 2016.

"Processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as:

(a) collection, recording, organisation, structuring;
(b) storage, adaptation or alteration;
(c) retrieval, consultation or use;
(d) disclosure by transmission, dissemination, or otherwise making available; or
(e) alignment or combination, restriction, erasure or destruction.

"**Security Equipment**" means—

(a) an alarm system;
(b) a safe, vault or secured container;
(c) a satellite tracking device, closed circuit television or other electronic monitoring device or surveillance equipment;
(d) a device used for intrusion detection, access control, bomb detection, fire detection, metal detection, x-ray inspection or for securing telephone communications;
(e) a specialised device used to open, close or engage locking mechanisms; or
(f) a specialised device used to reproduce or duplicate keys or other objects which are used to unlock, close or engage locking mechanisms.

"**Security Service**" means or more of the following services or activities—

(a) protecting or safeguarding a person or property in any manner;
(b) giving advice on the protection or safeguarding of a person or property, on any other type of security service as defined in this section, or on the use of security equipment;
(c) providing a reactive or response service in connection with the safeguarding of a person or property in any manner;
(d) providing a service aimed at ensuring order and safety on the premises used for sporting, recreational, entertainment or similar purposes;
(e) manufacturing, importing, distributing or advertising of monitoring devices for interception and monitoring provided for under any written law;
(f) performing the functions of a private investigator;
(g) providing security training or instruction to a security service provider or prospective security service provider;
(h) installing, servicing or repairing security equipment;
(i) monitoring signals or transmissions from electronic security equipment;
(j) performing the functions of a locksmith;
(k) making a person or the services of a person available, whether directly or indirectly, for the rendering of any service referred to in paragraphs (a) to (j) and (l), to another person;
(l) managing, controlling or supervising the rendering of any of the services referred to in paragraphs (a) to (j);
(m) creating the impression, in any manner, that one or more of the services in paragraphs (a) to (l) are rendered.

"Sensitive Personal Data" means data revealing the natural person's race, health status, ethnic or social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, including names of the person's children, parents, spouse or spouses, sex, or the sexual orientation of the data subject.

THE OFFICE

The Office of the Data Protection Commissioner is a government agency established to protect the privacy and security of personal data in our increasingly digital world. It has the responsibility of enforcing data protection laws and policies to safeguard the privacy, dignity, and fundamental rights of individuals. The office is mandated to oversee the implementation and enforcement of the Data Protection Act, 2019, which regulates the processing of personal data of persons located in Kenya by both the private and public sector organisations.

The office of the data protection commissioner plays a vital role in ensuring that individuals have control over their personal data and that organisations respect their privacy rights. The office's work involves monitoring and enforcing compliance with data protection regulations, investigating data breaches, and imposing sanctions on entities that violate data protection laws. In addition, the office is responsible for raising public awareness about data protection issues and educating individuals and organisations on how to protect personal data. With the growing importance of data protection in our digital age, the office of the data protection commissioner is a critical institution in maintaining trust and confidence in our data-driven society.

INTRODUCTION

Security service providers in Kenya are organisations that offer a range of security-related services to individuals, businesses, and government agencies. The security industry in Kenya has grown over the years due to an increasing demand for security services, especially in urban areas, as a result of rising crime rates.

The security services sector in Kenya is regulated by the Private Security Regulation Act of 2016, which mandates the licensing of all security service providers. The act provides for the establishment of a Private Security Regulatory Authority (PSRA) tasked with the responsibility of licensing, regulating, and supervising the private security industry in the country.

Some of the common security services offered by security service providers in Kenya include manned guarding, electronic security, CCTV surveillance, access control, event security, and VIP protection. These services are provided by a wide range of companies, including both local and international firms.

PURPOSE OF THE GUIDANCE

The purpose of this guidance note on the processing of personal data for private security is to provide clear and concise instructions on how to handle personal data in accordance with Act and the Regulations. Private security companies are responsible for collecting, storing, and using personal data for various purposes, such as conducting background checks, managing access to secure areas, and investigating security incidents.

This guidance note outlines the legal framework for the processing of personal data, including the relevant laws and regulations that apply to private security companies. It also provides guidance on how to implement the data protection principles into their processing operations as well as obtain consent from individuals for the collection and use of their personal data, as well as how to ensure that personal data is accurate, up-to-date, and secure.

In addition, the guidance note provides practical advice on how to implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, or destruction. This may include implementing encryption, access controls, and data retention policies.

Private security companies should also be aware of their obligations regarding data subject rights. This includes providing individuals with access to their personal data, allowing them to correct inaccuracies, and providing them with the right to object to the processing of their personal data in certain circumstances.

Finally, the guidance note emphasises the importance of training employees on the proper handling of personal data. This includes providing training on the Act and regulations, as well as on company policies and procedures for the processing of personal data.

Overall, a guidance note on the processing of personal data for private security is an essential tool for ensuring that private security companies comply with Act and the Regulations, while also protecting the rights and interests of individuals whose personal data they collect and use.

BACKGROUND

Private security refers to security services provided by private companies or individuals, rather than by government agencies such as the police or military. Private security can include a wide range of services, such as security guards, bodyguards, private investigators, and security consulting. Private security companies may be hired by individuals, businesses, or government agencies to provide protection and security for people, property, and assets. Some common examples of private security services include providing security for events or concerts, protecting high-profile individuals or executives, or providing security for private residences or businesses.

The private security industry in Kenya has undergone significant evolution over the years. In the early days of independence, private security was not a popular concept, and most security services were provided by the government. However, as the country's economy grew and crime rates increased, the demand for private security services increased as well.

In the 1980s, private security companies started to emerge in Kenya, offering a range of security services such as guarding, escort services, and investigations. These companies were mostly small and privately owned, and their services were primarily utilised by businesses.

In the 1990s, the government of Kenya passed laws to regulate the private security industry, which led to the establishment of the Private Security Regulation Authority (PSRA) in 1998. The PSRA is responsible for licensing and regulating private security companies in Kenya, ensuring that they meet certain standards of training, equipment, and personnel.

Since then, the private security industry in Kenya has continued to grow and evolve, with more companies offering specialised services such as cybersecurity and risk management. The industry has also become more professionalised, with many companies investing in advanced technology and training programs to provide high-quality services to their clients.

Today, the private security industry is a significant contributor to Kenya's economy, providing employment for thousands of people and contributing to the overall safety and security of the country.

In recent years, Kenya has experienced significant growth in the private security service provider sector. This growth has been driven by several factors, including increasing concerns about crime and terrorism, the expansion of the middle class, and the growth of the economy.

One of the main reasons for the growth of the private security sector in Kenya is the high crime rate in the country. Many people feel that the police are unable to provide adequate security, and as a result, they turn to private security companies for protection. These companies provide a range of services, including armed and unarmed guards, access control, surveillance, and alarm response.

Another factor driving the growth of the private security sector in Kenya is the expansion of the middle class. As more Kenyans have become wealthier, they have started to invest in their personal safety and the security of their businesses. Private security companies provide a range of services tailored to meet the needs of this growing segment of the population.

In addition, the growth of the economy has created more opportunities for private security companies. As more businesses and industries have been established in Kenya, there has been a corresponding increase in the demand for security services to protect these assets.

The adoption of Information and Communication Technologies (ICTs) by private security service providers in processing personal data has been on the rise in recent years. Many private security companies in Kenya are now using ICTs to manage and process personal data, such as biometric data, CCTV footage, and other forms of surveillance data.

One of the main benefits of using ICTs in processing personal data is that it allows for more efficient and effective management of security operations. For example, CCTV cameras can be used to monitor a large area and detect potential security threats, while biometric data can be used to control access to secure areas.

Privacy Concerns

There are several privacy concerns for private security service providers in Kenya. Some of these concerns include:

1. **Data collection**: There are several privacy concerns related to data collection by private security service providers. Some of these concerns include; Firstly private security companies may collect personal data without providing individuals with adequate information. This can lead to privacy violations and breaches of data protection laws. Secondly, private security companies collect more personal data than is necessary for the purposes of providing security services. This can lead to the collection of sensitive personal information that is not relevant to the security services being provided. Thirdly, there is a risk that personal data collected by private security companies could be misused or mishandled, leading to privacy violations. For example, personal data could be shared with unauthorised third parties or used for purposes other than those for which it was collected. Fourthly, private security companies are not transparent about their data collection practices or how they use personal data. This can lead to mistrust and concerns about privacy violations. Lastly, Private security companies do not have adequate technical and organisations safeguards in place to protect personal data from unauthorised access, theft, or loss. This can lead to data breaches and other privacy violations.
2. **Data sharing**: Private security companies share personal data with other organisations, such as law enforcement agencies or other security companies. There is a risk that this data could be shared without the knowledge or consent of the individuals involved, leading to privacy violations.
3. **Lack of transparency:** Private security companies may not always be transparent about the data they collect and how it is used. This lack of transparency can lead to mistrust and concerns about privacy violations.
4. 4. **Cybersecurity concerns:** The use of ICTs in processing personal data also raises concerns about privacy and data protection. Private security companies are vulnerable to cyberattacks, which could result in personal data being stolen or compromised. This could lead to privacy breaches and other security risks.

Application

These guidance note shall apply to the following aspects of processing of personal data:

1. The processing of personal data for the provision of security services by private security service providers in the provision of security services, in line with section 48 of the Private Security Regulation Act of 2016.
2. The processing of personal data by building owners for purposes of ensuring the security of the building, where such processing is carried out directly by the building owner or where the building owner has contracted the services of a private security service provider.
3. Private security firms who process personal data for the purposes of offering security services using both automated and non-automated means.

LEGAL FRAMEWORK GOVERNING THE PRIVATE SECURITY SERVICE PROVIDERS

The private security industry in Kenya is regulated by several laws and regulations. Some of the key laws regulating private security service providers in Kenya include:

The Private Security Regulation Act (2016)

This is the main law regulating the private security industry in Kenya. The Act establishes the Private Security Regulatory Authority (PSRA) as the regulator of the industry and sets out the requirements for licensing and registration of private security companies.

Under the Act, private security companies must obtain a licence from the PSRA in order to operate legally in Kenya. The PSRA is responsible for assessing the suitability of applicants for licences, including their financial stability, technical capacity, and compliance with legal requirements.

The Act also sets out the requirements for registration of private security personnel, including guards, investigators, and other security personnel. Private security personnel must undergo training and meet certain standards of competence and conduct in order to be registered.

The Act provides for the establishment of a code of conduct for private security companies and personnel, which sets out the standards of conduct expected of them. It also provides for the establishment of a complaints and disciplinary mechanism to address complaints about the conduct of private security companies and personnel.

The Act imposes various obligations on private security companies, including the obligation to maintain records of their operations, to provide information to the PSRA as required, and to comply with all applicable laws and regulations.

The Private Security (General) Regulations (2019)

The Private Security (General) Regulations (2019) provide detailed guidance on the requirements for licensing and registration of private security companies in Kenya. The regulations set out the standards for training, equipment, and personnel that private security companies must meet in order to operate legally in the country.

Under the regulations, private security companies must obtain a licence from the Private Security Regulatory Authority (PSRA) in order to operate legally in Kenya. The PSRA is responsible for assessing the suitability of applicants for licences, including their financial stability, technical capacity, and compliance with legal requirements.

The regulations set out the requirements for training of private security personnel, including the topics that must be covered in training programs. Private security personnel must undergo regular training to ensure that they are competent and up-to-date with the latest security techniques and technologies.

The regulations also set out the requirements for equipment used by private security companies, including uniforms, weapons, and vehicles. Private security companies must ensure that their equipment is in good working condition and meets the required standards.

The regulations provide for the establishment of a code of conduct for private security companies and personnel, which sets out the standards of conduct expected of them. The regulations also provide for the establishment of a complaints and disciplinary mechanism to address complaints about the conduct of private security companies and personnel.

APPLICATION OF PRINCIPLES FOR DATA PROTECTION IN PRIVATE SECURITY

Lawfulness, Fairness and Transparency

The principle of lawfulness, fairness and transparency requires that personal data must not be processed in a way that is unduly detrimental, unexpected or misleading to the individuals. The private security agency must be clear, open and honest with the people from the start about how you will use their personal data.

Processing personal information lawfully means that private security service providers must ensure that their processing is based on a legitimate legal basis, such as consent, performance of their contractual obligations, carrying out of a legal obligation, vital interest of the data subject or carrying out of a public interest. This ensures that individuals' personal data is not being processed without a lawful justification.

Fairness requires that individuals are treated equitably and that their rights are respected. This means that individuals should be informed about the purposes and legal bases of the data processing, and should be given the opportunity to exercise their data protection rights, such as the right to access, rectify, erase, and object to their data being processed.

Transparency places an obligation on private security service providers to inform individuals about how their data is being processed, in a clear and easily understandable manner. This includes providing information about the identity and contact details of the data controller, the purposes of the processing, the categories of data being processed, and any third parties to whom the data may be disclosed.

Mkarimu, an recently graduated from the University of Character Development has been invited for an interview for the position of CEO in Pwaguzi enterprises Limited, which is scheduled to take place at Happy Plaza in Nairobi.

As Mkarimu enters the building, she is met with employees of Simba Maximum Security Company who have been engaged by the Landlord of Happy Plaza to provide security services. On entering the building, Mkubwa, one of the security officers, gives Mkarimu, an A4 hardcover book, labelled "***Visitors Register***"and demands that she fills in the details.

The details required to be filled out in the book include, Mkarimu's name, Identification number, time of entry and exit, contact information being her mobile number, email address and her residential address including the land registration number. She is also required to provide her gender as well as her relationship status.

Mkarimu fills out the book only providing her name,Identification number and her time of entry on to the premises and returns the book back to Mkubwa to enquire why she is required to provide all the other information. Mkubwa, point to a notice posted at the entrance of the building.

The notice reads; " ***Pursuant to section 48 of the private security regulation 2016, persons entering this building will be required to identify themselves by producing a valid identification document and entering their personal details being their ID No the name and the time of entry into the premises. The information provided shall only be used for the purpose of identification. The information will only be kept for a period of 6 months from the date of record, following which the personal information will be anonymized or deleted.***

Mkarimu further seeks a clarification on why the information required in the visitor's register is more that what is outlined in the notice. In a bid to dismiss Mkarimu, Mkubwa retorts telling her that if she does not provide all the information required he will not allow her to gain access in to the building.

Not wanting the miss the great opportunity that lies ahead, Mkarimu provides the additional information though unclear on why the security officers required all that information to allow her to access the building.

In order for Simba Maximum Security company to be compliant with the principle of lawfulness fairness and transparency, they should ensure that they identify the lawful basis of processing as guided by the privacy notice, they should inform the people accessing the premises, what their personal information is required, what the information will be used for and for how long the information will be kept and the safeguards adopted to protect their personal information.

Simba Maximum Security Company should also limit the amount of personal information collected to what is required. Where there is no lawful basis for collection personal information, they should cease such collection and delete the information.

From the above example, it is clear that the processing practices of Simba Maximum Security Company are not in line with the lawful fairness and transparency principle.

The Notice provided at the entrance of the premises clearly outlines the information the security company is required to process as well as the lawful basis of such processing. However, the security company has not aligned its processing to the notice. In order to ensure that their processing is lawful, fair and transparent, the Security company should ensure that there is a lawful basis for each of their processing operations, that individuals are informed why their personal information is required and how their personal information will be used.

Lastly, the personal data must be processed in a transparent manner, meaning that the data subjects must be informed about how their data is collected, processed and used, including, providing clear and concise information about lawful basis as well as the retention period of the personal data.

Purpose Limitation

The principle of purpose limitation requires that personal data should only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with the initial purpose of collection.

This means that the purposes for which personal data is collected must be clear and specific, and must be communicated to individuals at the time their data is collected. Any further processing of personal data beyond the original purpose must be compatible with the original purpose and must be based on a legal basis.

In a stroke of unprecedented and unseen luck, Mkarimu successfully secures her positions as the youngest CEO of Pwaguzi enterprises limited. The news is pushilsied wideliy on both social media and traditional media channels.

In a bid to attract more business their way and to create raptor with the newly appointed CEO, Simba maximum security company, sends out a congratulatory message to Mkarimu, given that they already had her contact information, indicating their willingness to work and collaborate with her. In a bid to show off their connections Simba Maximum Security Company also publishes the personal information they have on Mkarimu on their social media platforms to show that they know the "right" people,

As a result of this, Mkarimu is flooded with alot of unwarranted messages, some of which are marriage proposals noting that she indicated her relationship status as "single".

From this, it is clear that simba maximum security company used the personal information that Mkarimu had provided to them for a different purpose, other that that which was indicated at the point of collection. In order for Simba Maximum Security Company to ensure that they are in compliance with the purpose limitation principle they need to define the purpose or purposes for which personal data is collected, and they must not use the personal information for any other purpose that is incompatible with the original purpose.

Purpose limitation is important because it helps protect the privacy rights of individuals by ensuring that personal data is not used for purposes that they have not consented to or that are not necessary for the provision of a particular service or product. It also helps prevent the misuse of personal data for unlawful or unethical purposes.

The purpose limitation principle protects individuals' privacy and aids in the prevention of personal data misuse. It ensures that personal information is only collected and used for legitimate purposes, such as contract fulfilment, service provision, or compliance with a legal obligation as in the example above.

Any other use or processing of personal information, such as marketing or research, must have a separate legal basis and not be incompatible with the original purpose of processing.

Data Minimization

The principle of data minimisation is closely related to the broader concept of data protection, which is the practice of safeguarding personal data from unauthorised access, use, disclosure, or destruction.

The data minimisation principle requires that private security service providers should limit the collection of personal information to what is directly relevant and necessary to accomplish the specific purpose of processing.

This means that private security service providers should only collect, process, and store the minimum amount of personal data required to achieve a specific objective.

From the assessment of the personal information collected by Simba Maximum Security Company, we note that they collect the following details from people visiting Happy Plaza where they provide security services.

They require the visitor's name, ID no, Contact information, including her mobile number, email address and well as her residential address, including the Land reference number. They also require information relating to the visitor's gender as well as their relationship status.

However, there is a concurrent privacy notice posted at the entrance of the premises that outlines what personal information should be collected and the lawful basis of such collection. The notice reads; "***Pursuant to section 48 of the private security regulation 2016, persons entering this building will be required to identify themselves by producing a valid identification document and entering their personal details being their ID No the name and the time of entry into the premises. The information provided shall only be used for the purpose of identification. The information will only be kept for a period of 6 months from the date of record, following which the personal information will be anonymized or deleted.***

Where visitors seeks a clarification on why the information required in the visitor's register is more that what is outlined in the notice. Mkubwa is quick to dismiss them claiming that he will not allow anyone to gain access in to the building if they refuse to provide the information as indicated in the visitors book.

In order to be compliant with the data minimisation principle, Simba Maximum Security Company should implementing data minimisation into your data processing operations by adopting the several : steps: they should identify the personal information being collected and processed, and determine whether it is necessary to achieve the purpose of processing.

Secondly, they should review their data processing operations to ensure they only collect and process the minimum amount of personal data necessary for the provision of security services. Thirdly, they should consider implementing techniques such as pseudonymization or anonymization to further reduce the risk of data breaches. Fourthly, they should establish policies and procedures for data retention and disposal, to ensure that personal data is not retained any longer than necessary and, lastly, they should train their staff on the principles of data minimization and the importance of protecting personal data.

In practice, data minimisation requires private security service providers to carefully consider the personal data they collect and the purposes for which they collect it. They must ensure that the data collected is relevant, accurate, and necessary for the purpose it was collected. They must also ensure that the data is processed securely and is only accessed by authorised individuals.

By implementing data minimisation, private security service providers can reduce the risk of data breaches and other data protection violations. It also helps to protect the privacy of individuals and ensures that personal data is used responsibly and ethically.

Accuracy and Accountability

Personal data collected by security service providers must be accurate and be kept updated, with necessary steps being taken to ensure that inaccurate data is erased or rectified without undue delay.

Compliance with the principle of accuracy will help security service providers to ensure that the personal data in their custody is reliable and up-to-date.

Upon publication of Mkarimu's visitor log entry on Simba Maximum Security Company social media platforms, individuals visiting Teleposta Towers decided to be a bit more reserved in giving out their personal information. Where Mkubwa is insistent on information being provided, individuals tend to give out inaccurate information.

Most recently, an individual identified as Mkora visited teleposta towers for a meeting with the Mkarimu. On entering the building, Mkubwa handed Mkora the visitor's book for him to fill it out. Mkora filled out all the details required in the visitor's book. At no point did Mkubwa required Mkora to produce his ID card to verify the details that he had provided.

Following which, Mkora was granted access to Mkarimu's office where he managed to steal electronic equipment worth Kshs. 3,100,000. In investigating the incident, Simba Maximum Security Company in collaboration with the police noted that the information that was provided by Mkora was not accurate. In making further enquiry into the incident, they noted that Mkubwa had not requested for Mkora's ID to verify the details as provided.

Simba Maximum Security Company has an obligation to ensure that the personal data they process is accurate noting that they are accountable for all the data in their custody. To ensure that they implement the principle of accuracy and accountability they should: Establish clear policies and procedures for data accuracy and accountability, including guidelines for data collection, storage, and use. Train their staff on the importance of data accuracy and accountability, and ensure that they understand their roles and responsibilities in maintaining accurate data. Implement measures to ensure the accuracy of personal data, such as data validation checks, regular data cleansing, and quality assurance processes, and establish procedures for responding to data subject requests, including requests for access, rectification, and erasure of personal data.

In addition to these steps, it is important for Simba Maximum Security Company to establish a culture of accountability within their organization, where staff are encouraged to take ownership of their work and to be transparent about their actions. This can be achieved through regular training and communication, as well as by establishing clear lines of reporting and escalation for data protection issues.

Overall, implementing the principles of accuracy and accountability in data processing operations requires a proactive approach that prioritizes data protection and privacy at every stage of the data lifecycle.

Some of the ways in which Security Service Providers can ensure that the principle of accuracy is observed is by collecting accurate data. Security Service providers should ensure that the personal data they collect is accurate, relevant and limited to what is necessary for the intended purpose.

Security Service providers should also verify the personal data collected. Security Service providers should verify the accuracy and completeness of personal data and take any steps to correct any errors. This should be done by requiring the production of identification documents for purposes of verifying the identity of the individual seeking access to the premises.

Security Service providers will also be expected to regularly monitor the personal data in their custody to ensure that it is accurate and identify any potential errors or discrepancies.

Storage Limitation

The storage limitation principle provides that personal data should only be kept in a form which permits for the identification of the data subject for as long as is necessary for the purpose for which the personal data is processed. The Act does not provide for or define specific retention periods. Therefore, entities providing private security services must justify a defined retention period and should not keep any personal data on a 'just-in-case' basis.

Upon the end of her term as CEO, Mkarimu decided to pay a visit to the security desk as she was checking out of the office, in order for her to get cleared and hand over her employee access card. On reaching the security desk she met with Mkubwa who insisted on serving her.

Mkubwa took her through the procedure of clearing as an employee and handing over her employee access card. Afterwards, Mkubwa also informed her that she would be required to sign out and provide her the details of her exist, being her last day in the Office. To her surprise, Mkarimu was give the visitor's book she signed during her initial visit when she had come for the interview of her positions as CEO

On signing the visitors book, Mkubwa informed her that they still had the details from the initial visit to the premises. Mkubwa also informed her that the first entry to the visitors book was made in 1986.

On enquiring why the book has never been changed, Mkubwa responded that the book will only be changed once all the pages have been filled up. On further enquiry as to whether they comply with what is provided for in the privacy notice, Mkubwa responded that purpose of the notice is to appease the masses, but in practice the retention period is not observed.

From the above illustration, it is clear the Simba Maximum Security Company has not complied with the storage limitation principle. In order to ensure their compliance, they should: Identify the personal data that they are required to process in achievement of the purpose of processing. They should also review their data processing operations to ensure that you are only collecting and processing the minimum amount of personal data necessary for the identified purposes.

Simba Maximum Security Company should also establish policies and procedures for data retention and disposal, to ensure that personal data is not retained any longer than necessary. The Company should also implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or destruction. Lastly, the Company should ensure that its staff are trained on the principles of data minimization and the importance of protecting personal data.

Guidance: Ensuring that personal data is erased or anonymized when it is no longer required reduces the risk of it becoming irrelevant, excessive, inaccurate, or out of date. Aside from assisting security service providers in adhering to the data minimisation and accuracy principles, it also reduces the risk that security service providers will use such data incorrectly, to the detriment of all parties involved.

Personal data that is kept for an inordinate amount of time is, by definition, unnecessary. Security service providers are unlikely to have a legal justification for such retention. More practically, storing more personal data than necessary is inefficient, and there may be unnecessary costs associated with storage and security. Good storage limitation practice, with clear policies on retention periods and erasure, is also likely to reduce the burden of dealing with retention queries and individual erasure requests.

There are a number of reasons why storage limitation is important for data protection. Firstly, it helps to minimise the amount of personal data that organisations hold, reducing the risk of data breaches and unauthorised access. Secondly, it ensures that personal data is accurate and up-to-date, as organisations are required to regularly review and delete data that is no longer needed. Finally, it gives individuals greater control over their personal data, as they can be confident that their information is not being held for longer than necessary.

Overall, the storage limitation principle is an important aspect of data protection that helps to ensure that personal data is treated with respect and kept secure, while also providing individuals with greater control over their personal information.

a) Confidentiality and Integrity

Confidentiality and integrity are two important aspects of data protection that ensure the privacy and security of personal information.

Confidentiality refers to the principle of keeping information private and protected from unauthorised access. It involves ensuring that only authorised individuals or entities have access to the data, and that the data is not disclosed to others without permission. Confidentiality measures include encryption, access controls, and secure data storage.

Integrity, on the other hand, refers to the principle of maintaining the accuracy, completeness, and consistency of data throughout its lifecycle. This involves protecting the data from unauthorised modification or deletion and ensuring that it remains reliable and trustworthy. Measures to ensure data integrity include backups, version control, and checksums.

One day Mkubwa decided to take the visitors register with him home just out of curiosity. But instead of of heading home directly, he decided to join his friend in a pub, where he ended up losing the visitor's register.

Later on Simba Maximum Security Company came to discover that the visitor's register was missing and the personal information contained within it had been published on an illegal website and all the personal information was being used to defraud individuals. Needless to say, this was a clear case of non-compliance with the integrity and confidentiality principle in data protection.

In order to ensure compliance, Simba Maximum Security Company will be required to; identify the personal data that they are collecting and processing, and determine the level of sensitivity of each type of data. Implement appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, or alteration, such as encryption, access controls, and regular backups. Establish policies and procedures for data security, including guidelines for data access, storage, and use. Train your staff on the importance of data security and confidentiality, and ensure that they understand their roles and responsibilities in maintaining the integrity and confidentiality of personal data. Conduct regular audits and risk assessments to identify potential vulnerabilities in your data protection practices, and take steps to address them.

Guidance: Both confidentiality and integrity are essential components of data protection and are often implemented together to provide comprehensive security for personal information. They help to ensure that personal information is protected from unauthorised access, theft, and manipulation, and can be trusted by those who rely on it.

In integrating confidentiality and integrity into their processing operation private security service providers should ensure access controls have been implemented. Implementing access control policies and procedures that restrict access to sensitive data to authorised personnel only. Access control mechanisms like authentication, authorization, and multi-factor authentication should be in place to ensure that only authorised personnel can access the data.

Private Security Service Providers should also ensure that they validate the data they collect. Implementing data validation will ensure that the data being processed is accurate and complete.

To implement integrity and confidentiality effectively, it is important to establish clear policies and procedures for data security. This may include establishing access controls and authentication mechanisms to ensure that only authorised personnel have access to personal data.

In addition to technical measures, it is important for Private Security Service Providers to establish a culture of confidentiality within the organisation, where staff are encouraged to take ownership of their work and to be transparent about their actions. This can be achieved through regular training and communication, as well as by establishing clear lines of reporting and escalation for data protection issues.

Overall, implementing integrity and confidentiality in data protection requires a proactive approach that prioritises data protection and privacy at every stage of the data lifecycle. By implementing these principles effectively, organisations can protect the privacy of individuals, reduce the risk of data breaches, and demonstrate their commitment to responsible data protection practices.

LAWFUL BASIS FOR PROCESSING PERSONAL DATA

Compliance with a Legal Obligation:

Private Security Agencies may rely on legal obligation as a lawful basis for processing personal information. To properly satisfy this legal obligation, a private security agency must demonstrate that the processing is necessary for compliance with a legal obligation to which they are subject. This means that the processing must be directly related to the legal obligation and it must be provided in a statutory provision or legislative framework, or an interpretation of the law by a Court.

Example:

Juma wishes to enter Crocs Towers for the purposes of visiting a friend, Musa, who works in CGI Consultants. Juma encounters a Simba Maximum Security Company security guard, Daudi, who requests that Juma provide a form of identification so as to verify Juma's identity. Juma is informed that his identification document will be kept for the duration of his visit and handed back to him as he leaves Crocs Towers.

Daudi notifies Juma of the purpose of collection, that the collection is to be done in line with the Private Security Regulation Act, that it is mandatory exercise, the safeguards that will be used to protect the data and the duration of retention of the data, in the event that Juma's information is recorded.

Juma is aware that Musa's Office will also require this information, and advises Daudi of this. Given the circumstances, Daudi allowed Juma to retain his identification document. However, Juma produced his ID and Daudi recorded the details contained on Juma's ID in a visitors book that is only accessible to the guard and other authorised personnel of Simba Maximum Security Company and Crocs Towers management.

Guidance: Under section 48 of the Kenyan Private Security Regulation Act, 2016 private security agencies or security guard/ officer can, at the entry of any premises or property within the control and care of a private security agency, request a person to identify themselves, register the time of entrance and exit of the person and retain temporarily the identification document of such person. Additionally, private security agencies have the power to record or copy the details in the identification documents of persons' entering into any premises.

Consent:

Where consent is relied upon for the processing of personal data by private security agencies or guards, consent will only be an appropriate lawful basis if the individuals whose information is to be processed are offered **a genuine choice** to accept or decline the collection and further processing of any or part of their personal data, without detriment.

Therefore, where a private security agency processes personal data on the basis of consent from an individual, they must ensure that the consent is valid and that the consent was freely given, specific, informed, and unambiguous.

Example 1

Simba Maximum Security Company processes personal data of regular entrants into a building using facial recognition technology to verify the identity of individuals entering a secure area within Crocs Towers. Before collecting and processing the personal data, Simba Maximum Security Company must inform individuals of the purpose of the processing, the basis to be relied upon, the types of personal data collected, the safeguards adopted and the length of time the data will be stored. Simba Maximum Security Company must also obtain explicit and informed consent from the individuals it collects facial recognition data from. Where an individual does not consent to the collection and further processing of their facial recognition data, Simba Maximum Security Company must verify the individual's identity using the normal modes of identification. That is, rely on the legal obligation and collect their identification details

It is important to note that individuals have the right to withdraw their consent at any time. Simba Maximum Security Company must provide individuals with clear and easy-to-understand information on how to withdraw consent, and must comply with such requests promptly and effectively.

Example 2

Crocs Tower has contracted Simba Maximum Security to manage multiple access to its building using a facial or fingerprint recognition method. People can only use this way of access if they have given their explicitly informed consent beforehand.

To ensure the lawfulness of the processing, Simba Maximum Security must always offer an alternative way to access the building to regular entrants, without biometric processing, such as badges or key access.

The Office has published a Guidance Note on Consent which is available on www.odpc.go.ke .

Legitimate Interest:

Private security agencies may process personal data if it is necessary in order to meet the purpose of a legitimate interest pursued by the private security agency or the entity that has contracted the private security agency to provide private security services. The legitimate interest would only apply where the aforementioned interests are not overridden by the data subject's interests or fundamental rights and freedoms.

A private security agency can only proceed with processing personal data where it has a compelling legitimate interest which does not override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. This could be the case where there is a legitimate interest in protecting the safety and security of a building or property, as well as protecting the assets within the building.

Private security agencies are required to make a determination of whether there is a real and hazardous situation, such as processing personal data so as to protect property against burglary, theft or vandalism can constitute a legitimate interest.

The legitimate interest must not be fictional or speculative and must be a real and present issue. A real-life situation of distress needs to be at hand – such as damages or serious incidents in the past –

before processing personal data on this basis. For example, capturing facial recognition information for access into a building, which may be deemed excessive in many cases.

Example

Simba Maximum Security Company on behalf of the owner and occupants of Crocs Towers is collecting facial recognition data for all parties entering into Croc Towers. The collection is done on the basis of legitimate interest. Crocs Tower has not had any security incidents, nor does an objective assessment show that Crocs Towers is at risk of any security incidents that would warrant the collection of more than just the identification details of the individuals entering the premises.

On this basis, the processing of facial recognition information for general security requirements cannot be regarded as legitimate interest overriding the interests or fundamental rights and freedoms of the data subject. However, the processing of biometric data (such as facial recognition data) can be justified as a required tool securing the property and/or individuals, where there is evidence, on the basis of objective and documented circumstances, of the concrete existence of a considerable risk.

Example

Simba Maximum Security Company uses CCTV to monitor entry access and exits to a building, in order to prevent unauthorised entry, protect the safety of building occupants and the property. The use of CCTV must be proportionate to the risk, and the private security agency must have a legitimate interest in using the technology for this purpose. Simba Maximum Security Company must also inform individuals that CCTV is in use and provide a contact person for any questions or concerns.

Public Interest:

In some cases, processing personal data may be necessary in the public interest, to protect the safety of building entrants and occupants. For example, CCTV cameras may be used to monitor **public areas** of a building or property to prevent crime or respond to emergencies. In such cases, the lawful basis for processing personal data would be the public interest in promoting safety and security. It is important to ensure that such processing should be proportionate, necessary and respects the rights and freedoms of individuals.

Guidance:

Public interest has been defined by the Black's Law Dictionary as "…the general welfare of the public that warrants recognition and protection, something in which the public as a whole has stakes".

Therefore, the monitoring or government building using CCTV where entry is to the general public can be deemed to be of public interest. This would not apply to private or commercial property where capturing personal data through CCTV footage would either be by consent or on the basis of a legitimate interest of the building owner or occupants.

GENERAL CONSIDERATIONS WHEN PROCESSING BIOMETRIC DATA BY BUILDING OWNERS AND PRIVATE SECURITY AGENCIES

The use of biometric data such as fingerprint and facial recognition pose a significantly heightened risk to the rights and freedoms of individuals whose data is being captured. The use and adoption of such technologies processing such sensitive personal data (biometric data) must take into consideration the lawfulness, necessity, proportionality, confidentiality and integrity and data minimization principles as set out in the Act.

Many organisations deem the processing of such sensitive personal data using facial recognition and fingerprinting technologies to be very effective. However, entities wishing to employ such technologies must always assess the impact on fundamental rights and freedoms and consider less intrusive means to achieve their legitimate purpose of the processing.

The use of biometric recognition functionality installed by private entities for their own purposes (e.g. monitoring, statistical, or even security) will, in most cases, require explicit consent from all data subjects (*see above discussion on consent*). However, organisations, in exceptional and justifiable circumstances, can use legitimate interest to process such data (*see above discussion on legitimate interest*).

Processing of Biometric Data or CCTV usage in the Workplace

Employers may, in certain circumstances, have legitimate reasons for installing biometric access entry technology and CCTV. Conversely, employees also have legitimate expectations that their privacy will not be intruded upon disproportionately. In this case, employees should be given a clear notification that CCTV monitoring is taking place and informed as to where and why it is being carried out. Further, where biometric access technology has been implemented, employees consent must be obtained - unless there is a real risk relating to the safety and security of the premises.

If the use of CCTV or biometric access technology has been justified for a specific purpose such as security or health and safety, it should not be used for a further purpose such as monitoring staff attendance or performance. The use of CCTV and biometric access technology in the workplace can be contentious and should not be viewed as an appropriate tool to monitor staff attendance or performance.

However, situations can arise where an employer needs to use CCTV footage or biometric access technology data for a purpose other than one identified at the outset such as to investigate an allegation of gross misconduct or other disciplinary matter. This would be strictly on a case by case basis. Further, it must be justifiable as a legitimate interest and carried out based on necessity and proportionality to achieve the given purpose.

The employer must be able to demonstrate why the use of such data is necessary to provide evidence in a disciplinary matter, and that their access to the CCTV footage or biometric access data is proportionate and limited in scope to the investigation of a particular matter. In such cases, the rights of the employee and their expectation of privacy will not be seen as overriding the interests of the employer, and the employee's data protection rights should not be seen as presenting a barrier to the investigation of serious incidents.

Household Exemption

The processing of personal data by a natural person in the course of a purely personal or household activity is out of the scope of the Act as stated in section 51(2)(a). This exemption only relates to the activities carried out in the course of private or family life of individuals. In determining whether processing is purely for household purposes, individuals must consider the following:

(a) Whether the individual processing personal data has some kind of personal relationship with the data subject,
(b) whether the scale or frequency of processing could suggest some kind of professional activity; and
(c) whether the processing has the potential to have an adverse impact on the data subjects.

Example

Juma has inserted CCTV cameras to monitor and record his own property and garden. The property is fenced and only Juma and his family enter the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not capture any public space or the neighbouring property.

RIGHTS OF A DATA SUBJECT

Right to be informed

Every data subject has the right to be informed of the use to which their data is to be put.

In the processing of personal data for private security purposes, individuals have the right to be informed about how their data is being used, what types of data are being processed, the purposes of the processing for which the personal information is intended to be used and who is processing the data.

SCENARIO - 1

Simba Maximum Security Company (*'Simba'*) is a private security company with operations not only in Kenya but in the whole of East and Central Africa. The private security company has a reputation for its reliability and effectiveness which is true to its tagline of **'There When you Need Us'** and **'You INVEST, We PROTECT'.** Simba has also transformed the words, **' One Call Away '** from its usual use in the romantic parlance into a business operational tool that portrays the effectiveness and efficiency that the company ascribes to. It offers timely security solutions. To say the least, Simba Maximum Security Company is the King in the private security companies' jungle.

In terms of clientele, Simba Maximum security has a huge clientele ranging from private Clients, Corporate clients, and even government institutions. It offers all manner of security solutions ranging from the usual security guards, bodyguards, private investigations, Biometric security solutions, facial recognition software solutions, video surveillance in form of installation and maintenance of CCTV cameras, and advanced intelligence solutions that aid in undercover operations such as profiling of criminals.

This right provides individuals with transparency and control over their personal data, allowing them to make informed decisions about how their data is being used.

Example 1.

When Simba Maximum security, is using CCTV cameras to monitor a public area, individuals have the right to be informed about the presence of the cameras, the purpose of the surveillance, and how long the footage will be retained. This information can be communicated through signage marked "CCTV Surveillance" or other means to ensure that individuals are aware of the surveillance and can make informed decisions about their activities in the area.

Example 2.

When Simba Maximum Security, is processing personal data, such as biometric information, for access control purposes, individuals have the right to be informed about what types of data are being collected, how it will be used, and who will have access to the data.

This information can be communicated through privacy notices or having a security guard to inform the individuals entering the building of the data collection process or other means to ensure that individuals understand how their personal data is being used.

Example 3.

When Simba Maximum Security is processing personal data for investigative purposes, such as conducting background checks on employees or clients, individuals have the right to be informed about what types of data will be collected, how it will be used, and who will have access to the data. This information can be communicated through privacy notices or other means to ensure that individuals understand the purpose and scope of the investigation.

Right to access personal data

Data subjects are entitled to view their personal information that is being held by the Private security Companies.

In the processing of personal data for private security, data subjects have the right to access information about the personal data being processed by the private security company. This right allows individuals to obtain information about their personal data held by the private security company, including the purposes of the processing, the categories of personal data being processed, any recipients of the data and if at all possible, the anticipated time frame for which the personal data might be stored, or, if that isn't practicable, the factors that went into deciding that time frame.

Example 1:-

Individuals have the right to access the personal data contained in the CCTV footage belonging to Simba Maximum Security

The data subjects can request information about the purposes for which the CCTV footage is being processed, the categories of personal data being processed (such as their physical appearance, movements, and location), any third parties who have received or will receive the data e.t.c

Example 2.

In the event Simba Maximum Security, uses a facial recognition technology to identify individuals, the data subjects have the right to access information about the processing of their personal data. They can request information about the purposes for which the facial recognition system is being used, the categories of personal data being processed (such as their facial features and biometric data), any third parties who have received or will receive the data e.t.c.

Example 3:-

If Simba Maximum Security has not adopted the use of technology as in the above two examples but it requires the data subjects to fill their details in an 'access book' in order to be permitted to access the building (s) or premises where the private security company is offering their security services, the data subjects have a right to access the personal data that they gave out whilst filling in the 'access book'.

In this case, Simba Maximum security will extract the data subject's details from the 'access book' and avail it to the data subjects. The personal information given should solely be for the requesting data subject and not for any other person who might have filled in the same page that the requesting data subject had filled in the "access book"

In relation to this right, it is important to note that the private security companies must provide clear and concise information to the data subjects about their processing activities and respond to any requests for access to personal data within a reasonable time frame.

The Private security companies should comply with all requests for access of personal data within seven (7) days of the request.

Right to object to all or part of their personal data being processed.

Data subjects/ Individuals have the right to object to processing of all or part of their personal data for private security purposes. The objection can be in relation to a specified purpose or to a specified manner.

The private security company shall comply with the request for objection within fourteen (14) days of the request.

Example 1.

In the above example where Simba Maximum Security used facial recognition technology to identify individuals who enter a building. The individuals may object to the collection of their personal data through this technology, as it may be seen as intrusive or unnecessary.

In this case, the individuals have the right to object to the processing of their personal data through facial recognition technology, and Simba Maximum Security must stop collecting their data in this way. Simba should comply with this request for objection within fourteen (14) days of the request.

SCENARIO 2:-

Kaziwa Company has contracted Simba Maximum Security to instal CCTV cameras in their offices to monitor their employees' activities. One of the employees, Matata, protests and objects to the installation of the Cameras at the workplace as according to her it infringes into her privacy. According to her, the CCTV cameras are being used as a micromanaging tool and have been installed to monitor them as employees and not for security purposes as it is being said by Kaziwa Company Management.

In this case, the employee, Matata, has the right to object to the processing of their personal data, and the company must stop collecting her data through the security cameras installed by Simba Management Company.

When it comes to the installation of CCTV cameras, the cameras should be placed at vantage points which ensure security.

N/B;- The right to object is not an absolute right and is subject to certain limitations e.g. lawful basis and public interest.

Example.

In the above example where a data subject has objected to the processing of personal data by Simba Maximum Security, If Simba Maximum Security can demonstrate that the processing of the personal data is necessary for the performance of a task carried out in the public interest, the data subject's right to object may not be upheld.

Right not to be subjected to automated decision making

This right is to the effect that individuals have the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

In relation to the processing of personal data for private security, the right not to be subjected to automated decision-making means that individuals have the right to human intervention in the decision-making process, this is more so where the decision has legal or significant effects on the individual.

In the event the private security company makes an automated decision that has legal repercussions e.g. criminal involvement, or has a significant effect on the data subject, the private security company must notify the individual as soon as practicable that the decision was made solely on automated processing and that the individual may, after a reasonable period of receiving the notification, request the private security company to reconsider the decision.

Example 1.

In the event Simba Maximum Security uses scanners to capture biometrics and subjects the information captured to an algorithm for purposes of profiling to assess the risk of criminal behavior by individuals in a particular area. The algorithm may produce a decision that an individual is a high-risk potential criminal, leading to increased surveillance and monitoring. In such a case, the individual has the right to challenge the decision and seek human intervention to ensure that the decision is not based solely on automated processing.

Example 2.

Simba maximum security is using facial recognition to identify individuals entering Crocs Towers. On one evening, thieves managed to make way into the tower and stole from one of the offices. Fortunately as the thieves were escaping the face of one of them got captured by Simba Maximum Security systems. Simba Maximum Security used the captured face to create an algorithm and ran it through Simba Maximum security database to reveal who the thief was . Upon running of the facial image through the system the facial image matched that of Mdosi who at the time the theft was occurring was chairing a board meeting and as such the results were erroneous as Mdosi was not among the people involved in the theft.

From this example, in as much as Simba Maximum Security is using facial recognition software to identify individuals entering the premises where it is offering private security services, it should not entirely rely on the system for identification and other purposes as there is a possibility of it having erroneous results. Simba Maximum security must provide for the element of human intervention to ensure that the decisions/ results arrived at are fair and accurate.

In this case, implicating Mdosi into the theft that had occurred is inaccurate as he was in a meeting and as such he had witnesses who were present in the board meeting the time the theft was on-going. Different people have some sense of resemblance.

Mdosi has the right not to be subjected to the decision based solely on automated processing by the Simba Maximum security facial recognition.

Simba Maximum security must provide a human intervention to ensure that the decisions are fair and accurate.

Right to rectification of personal data

This right allows individuals to request that any inaccurate, incomplete, outdated or misleading personal data held about them be corrected or updated by the data controller.

In relation to the processing of personal data for private security purposes, data subjects have the right to request the rectification of their personal data if it is inaccurate, incomplete, outdated or misleading.

The personal data that can be rectified include personal data that is used to identify individuals.

Example:-

In addition to the use of technology in providing security to Crocs Tower, Simba security also requests individuals to give out their identification numbers as they enter into the building.

One morning John, an employee at Crocs towers was denied access into the building simply because the last digit of his identification number was not correct. Instead of the last digit reading 1, Simba Maximum security had captured it as 7 in their system which in itself is another person's identification number. This forced John to contact his supervisor, Mr. Mtiaji to come and talk to Simba Maximum Security personnel for him to be able to be allowed into the premises.

Upon gaining entrance John lodged a request to Simba Security, requesting them to change the identification number that they had in their system to reflect his correct and accurate identification number.

As such John' request is within his right to request that his personal data be corrected or updated by Simba Maximum Security to reflect his correct identification number.

Right to erasure

This right is also known as the right to be forgotten. It allows individuals to request for the deletion or removal of their personal data by a data controller/ data processor.

Individuals can ask a private security company to delete or stop using any of their personal data held by them in the following situations: (a) the data is no longer required for the purpose for which it was collected e.g. if the data collected by the Private security company was for purposes of accessing a building and the person has vacated and or relocated from the building; (b) the data subject withdraws their consent, which was the legal basis for keeping the personal data; (c) the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing; (d) the processing of personal data is unlawful and the erasure is necessary to comply with a legal obligation.

Example 1.

If individuals request the erasure of their personal data, from Simba Maximum biometric systems and scanners, it must comply with their request unless there is a legitimate reason for retaining the data.

Example 3.

Before employing Matata, Kaziwa Company contracted the Services of Simba Maximum Security to conduct background checks on Matata. Later on after leaving employment with Kaziwa Company, Matata became aware of this an wrote to Simba Maximum Security to erase his personal data from their databases.

With regards to this request, Simba Maximum Security should honour it and delete Matata's personal data unless there is a legal requirement or legitimate interest for the company to retain it.

The instances where Simba Maximum Security can retain the personal data for a long time than the required period include instances such as:-

- It is required by and or authorised by the law;
- The retention is reasonably necessary for a lawful purpose;
- The further retention is authorised and consented by the data subject; and
- If the information is for historical, statistical, journalistic literature and art or/research purposes.

Right to data portability

This right gives individuals the right to receive a copy of their personal data in a structured, commonly used, and machine-readable format, and the right to transmit that data to another data controller without hindrance.

In relation to processing personal data for private security, the right to data portability may be relevant where individuals wish to have access logs ported to another security provider or other relevant party such as a lawyer.

Example 1.

Matata was dismissed from Kaziwa Company over serious misconduct which involves being a chronic late comer.

To Matata, she has been coming to work in time and this is witch-hunt. To her all the reasons for her dismissal is fabricated and as such she wants to file a claim against Kaziwa Company for unlawful termination.

In order to prove her case, Matata's lawyer told her to that under the data protection Act, 2019 she has a right to request the timestamped CCTV footage and biometrics information from Kaziwa Company.

Matata exercises this right and requests for the CCTV footage and the biometrics information.

As such, Matata's request is valid and Kaziwa Company should port a copy of the CCTV footage and the biometrics captured in a structured and machine-readable format to Matata for her to be able to take the same to her lawyer. This should be done within 30 days of receipt of the request for data portability.

Example 2.

At his palatial home, Matata wants to change his home security system provider from Rex Security to Safi security. In addition to the change of the security system provider he also wants to transfer his personal data such as his contact information, address, and security preferences from Rex Security to Safi security. With the right to data portability, Matata has the ability to obtain and transfer his personal data in a structured and machine-readable format from Rex Security to Safi security without any hindrance.

COMPLIANCE OBLIGATIONS / IMPLEMENTING DATA PROTECTION MEASURES.

Duty to Notify

One of the key principles of data protection is transparency. The personal data processed by an entity in the private security sector shall be processed fairly and in a transparent manner. Therefore, at the time of collection, entities must comply with the obligations under Section 29 of the Act. This provision requires that data controllers and data processors notify data subjects of their rights specified in the Act; inform them that personal data is being collected, state the purpose of the collection; disclosing any third parties who may receive the data and the safeguards adopted; provide the contacts of the data controller or data processor and disclose whether any other entity may receive the data; describe the technical and organisational security measures taken to ensure data confidentiality and integrity; state if the data is being collected pursuant to any law and if it is voluntary or mandatory; and outline the consequences if data subjects fail to provide all or part of the requested data.

The above information should be provided to data subjects to enable them to understand how their personal data is used. The duty to notify should be contained in a **data protection policy**. The Data Protection Policy acts as a notice to individuals whose data is to be collected or otherwise processed. This policy must be brought to the attention of all individuals prior to the collection of their personal data or as soon as possible soon after where information is not collected directly. The data protection policy should also be provided to individuals upon request.

When drafting a privacy policy, there are several practical tips and considerations that should be taken into account to ensure it effectively communicates to data subjects how their personal data will be used, these include:

1. the policy should be written in clear and plain language that is easy to understand. Technical or legal jargon should be avoided as much as possible to ensure that data subjects can easily comprehend what the policy says.
2. the policy should be transparent and comprehensive, covering all the relevant information that data subjects need to know about the processing of their personal data. This includes information about the rights of data subjects under the Data Protection Act, the fact that personal data is being collected, the purpose for which the personal data is being collected, the third parties to whom the data may be transferred, and any safeguards in place to protect the data.
3. the policy should be accessible to data subjects. This can be achieved by making it available on the data controller's or data processor's website, or by providing a copy upon request.
4. the policy should be reviewed and updated regularly to reflect any changes in data processing practices or in relevant laws and regulations.

To make privacy policies easy for data subjects to understand, it is important to use plain language and avoid technical jargon. Visual aids such as infographics and diagrams can also be used to help convey complex information. In addition, using a question and answer format or breaking down the policy into shorter sections with clear headings can make it more digestible for data subjects. Providing examples of how personal data may be used in practice can also help data subjects to understand the policy and the implications of sharing their personal information.

Example 1.

Maximum Security has been contracted to provide security services for a building located in Nairobi. The company is responsible for collecting data on all individuals entering the building. To comply with their obligation to notify individuals about the collection of their personal data, the company has erected a notification banner at the building's reception area containing a privacy notice. The privacy notice includes information such as the reason for collecting personal data, the type of data being collected, the methods used for data collection, the basis of collection, how Maximum Security protects the collected data, the length of time the personal data will be stored, and the rights individuals have regarding their personal data.

The data protection policy is an external facing document and is not to be confused with any internal policies that an entity develops to ensure internal practices align with the data protection Act. The common practice of demonstrating compliance with the laws and regulations among controllers and processors is through privacy policies and notices on websites. The information in a data privacy policy must be provided in simple and clear plain language, appropriate language for the target audience and be provided free of charge. The data privacy policy must be kept up to date to meet any changes in your approach to processing data.

Data Protection by design and by default

The Data Protection Act, in section 41, outlines the requirement for data controllers and data processors to implement appropriate technical and organisational measures to ensure effective implementation of data protection principles and necessary safeguards in data processing. Additionally, the act requires that only necessary personal data is processed, taking into account the amount of data collected, the extent of its processing, storage period, accessibility, and cost of processing.

Data protection by design is an approach that ensures data entities in the private security sector consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. Data protection by default requires data controllers and processors to ensure that only data that is necessary to achieve your specific purpose is processed. Data protection by default requires entities to ensure that data protection issues have already been considered and protection methods incorporated into existing systems and practices. This could be achieved by data controllers and processors specifying the personal data required before the processing starts, appropriately informing individuals and only processing the personal data needed for the specific purpose. Applying appropriate security measures to such data, and its processing environments both at rest and in transit, is vital to ensure the personal data is protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing.

Entities in the private security sector should take appropriate security measures to ensure against accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. These measures include: training in privacy and security; access controls; confidentiality agreements; and physical controls.

Private security firms should consider the following organisational and technical measures to protect the personal data in their possession:

(a) A training and awareness program for employees (guards) on data protection laws and their responsibilities in regards to ensuring safety of personal data.
(b) Risk Assessment and Management: This includes conducting a comprehensive security risk assessment to identify potential security threats to personal data and developing an appropriate security plan to mitigate those risks.
(c) Developing an internal policy for Information security and supporting policies such as data retention policy, records management policy and incident management policy.

(d) Implement appropriate access control measures such as passwords, access cards, or biometric systems to control who has access to personal data.
(e) Use of data encryption techniques which involves encoding personal data in a way that it can only be read by authorised personnel, thereby protecting it from unauthorised access.
(f) Private security firms should conduct regular security audits and reviews to identify any vulnerabilities in the security systems and take corrective actions.
(g) A well defined Incident Response and Reporting plan to quickly respond to any data breaches or security incidents, and reporting them to the relevant authorities. Personal data breaches should be reported to the Office of the Data Protection breaches.
(h) Data Minimization through limiting the collection of personal data to only what is necessary and relevant to the service being provided.

Private security firms which rely on manual processing of visitors' records should consider the following measures:

(a) Restricted access: The logbook should be kept in a secure location, accessible only to authorised personnel.
(b) Limited use: The logbook should only be used for its intended purpose - to record the names and details of visitors to the facility.
(c) Data protection: Visitors' personal information must be protected and kept confidential. This includes ensuring that the logbook is not left in public areas and that the information is not shared with unauthorised individuals.
(d) Monitoring and auditing: Regular monitoring and auditing should be conducted to ensure that the logbook is being used correctly and that no unauthorised access has occurred.
(e) Disposal: When the logbook is no longer needed, it should be disposed of securely, such as through shredding or incineration.
(f) Training and awareness: Staff who have access to the logbook should be trained on the importance of data protection and security, and be made aware of the procedures in place to protect visitors' personal information.

Example 1

Proctor Security Services offers guarding services to residential areas in Nairobi and takes data protection and privacy seriously. The company uses a Visitor Management System and has established various security measures to guarantee the safety of residents' personal information, such as restricted access to personal data, encryption of electronic records, staff training on data protection laws, regular data audits, and an incident response plan for any potential data breaches. Additionally, all records containing personal data are disposed of securely through shredding. By prioritizing data protection, Proctor Security Services instills trust in its clients and ensures their personal data is secure and their privacy is protected.

Example 2:

Neema Security Services is a professional security firm that provides security services to malls. They take the security and privacy of visitors' personal data very seriously, especially given that they use manual processing for visitor details. Neema Security Services has implemented several measures to ensure the protection of visitors' personal data:

Access to visitor personal data is restricted to authorized personnel only. Staff members are required to maintain strict confidentiality regarding visitor information and must not disclose it to unauthorized individuals. All visitor books are stored in secure locations to prevent unauthorized access or tampering. After the defined retention period has lapsed, the book is securely disposed of through shredding. Security personnel who handle visitor information are trained on data protection policies to ensure that they handle personal information appropriately. Neema Security Services conducts regular audits to ensure that visitor information is being handled in accordance with its data protection policy. The storage area where the visitor books are locked is monitored by security cameras and access is restricted to authorized personnel only.

Through these measures, Neema Security Services ensures that visitors' personal information is protected, their privacy is maintained, and their data is secure, despite using manual processing for visitor details.

Engagement of data processor

To assist with this, the Act sets out that where an entity engages a vendor or service provider (processor) to process information on its behalf, there must be a written contract stipulating that the processor acts only on the controller's instructions and is bound by the obligations of the controller. Further, both parties should take all reasonable steps to ensure that any person employed by or acting under the authority of the data controller or data processor complies with the relevant security measures.

The Data Protection Act and related regulations specify that a contract between a data controller and data processor should include key elements, such as the subject matter of processing, the type of personal data, the nature and duration of processing, security measures, and situations requiring prior authorization from the controller. The contract must also outline the obligations of the processor to ensure staff confidentiality, assist the controller in meeting its obligations under the Act, and delete or return personal data at the end of the contract. The contract should include provisions for auditing and inspection, as well as liability in case of failure to meet obligations or acting outside the controller's instructions.

Example 1.

- **Data Controller (DC):** A land owner in Nairobi who provides parking services.
- **Data Processor (DP):** A private security firm that provides parking security.
- **Third party contractor:** A cloud computing service provider that the DP has contracted to manage their customer data through a smart car parking system.

Contract Terms: The contract between the DC and the DP includes the subject matter of processing, which is the processing of customer data, including their name, address, phone number, Vehicle number plates and payment information. The contract authorises the DP to contract a third party contractor for the management of a smart car parking system. The DP remains liable to the DC for compliance of any third party they engage. The DP shall ensure that its staff and third party contractor processing the data are subject to a duty of confidence, and appropriate measures to ensure the security of processing will be taken, including encryption of the data. The contract also stipulates that any personal data breach will be promptly reported to the DC. The DP is obliged to delete or return all customer data to the DC at the end of the contract, and the DC has the right to audit and inspect the DP's data protection measures. The contract also outlines the liability of the DP if it fails to meet its obligations, including compensation for any damages caused to the DC or its customers due to a breach.

Notification and Communication of Breach

Data Controllers have to report personal data breaches to the ODPC without delay within 72 hours of becoming aware of the breach. Where there has been an unauthorised access, players within the private security sector are required to communicate to the affected data subjects in writing within a reasonable period, unless the identity of the data subject cannot be established.

Entities are required to report data breaches to the Office and provide certain information about the breach. This information includes the date and circumstances in which the data breach was discovered, a chronological account of the steps taken after the breach was discovered, and details on how the breach occurred. Additionally, entities must provide the number of data subjects affected, the personal data or classes of personal data affected, and the potential harm to affected data subjects. The entity must also provide information on any action taken to mitigate the harm and remedy any failure or shortcoming that contributed to the breach, and how affected individuals can mitigate potential harm.

Example 1.

Maximum Security, which utilizes a cloud-based system for managing visitor access, discovered unauthorized access during a routine security check. The security administrator promptly reported the breach to senior management, who instructed the team to investigate the cause and extent of the breach. Upon determining that it was a notifiable data breach, Maximum Security notified the building owners within 48 hours and they, in turn, informed the Office of the Data Protection Commissioner within the required 72-hour period. To rectify the situation, the team took corrective measures, such as updating system passwords and disabling inactive system accounts. The building owners sought legal assistance in drafting a message to notify affected individuals and provided guidance on how to prevent any potential harm.

Example 2.

John, a security guard at the XYZ building, discovers that the visitor logbook used to document the names of visitors entering the building is missing. This logbook contains personal data of visitors who have accessed the building within the past year. John promptly informs the security firm's management of the situation, who in turn notifies the building owner within 48 hours. Upon receiving the report, the building owners consults with the company's legal counsel, who advises them to report the data breach immediately to the Office of the Data Protection Commissioner within 72 hours.

Data Protection Impact Assessments

The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of data subjects*". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controllers and processors implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

The Act and the Data Protection (General) Regulations, 2021 deems certain activities to be a high risk to the rights and freedoms of individuals, these include: the processing of biometric or genetic data (this would include fingerprint and facial recognition data) and systematic monitoring of publicly accessible areas. Therefore, building owners and entities providing private security services that collect such data are advised to carry out a DPIA in accordance with the Act and submit the same to the Office for any new processing activities.

The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke The Guidance Note includes the form in which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.

Example 1.

A mall located in Nairobi is thinking about installing CCTV cameras throughout its premises, including the parking area, building perimeter, entrances, exits, and all floors. As this will result in significant surveillance, which will result in high risk to the rights of individuals. The Data Protection General Regulations requires that entities involved in systematic monitoring of a publicly accessible area on must conduct data protection impact assessment (DPIA). The mall's owners have enlisted a consultancy firm to conduct the assessment. The consultancy firm is using the guidance note provided by the Office of the Data Protection Commissioner to evaluate the potential risks involved with extensive surveillance. In addition, the firm recommends certain measures, such as access control and training and awareness, encryption, to mitigate the identified risks. The firm advises the mall owners to submit the DPIA report to the Office of the Data Protection Commissioner at least 60 days before commencing data processing.

Registration

Private security agencies providing CCTV technology or any entity contracted to provide CCTV technology solutions and maintain the same are expected to register as a data controller and/or data processor. Additionally, any building/property management company would also be required to register as a data controller and/or data processor. Further, the above named entities are subject to mandatory registration regardless of their size and/or their annual turnover/ revenue.

The Office has published a Guidance Note on Registration of Data Controllers and Data Processors which is accessible through www.odpc.go.ke. The Guidance Note includes a step by step guide on how

to complete the registration process and the information required during the registration process available here

APPENDIX - SUMMARY CHECKLIST OF ACTIONS

	Question	Yes	No	Comments/Remedial Action
Lawfulness	Have you identified an appropriate legal basis for our processing under Section 30 of the Data Protection Act (DPA).			
	If you are processing sensitive data, have you identified permitted grounds under section 44 of the DPA.			
	Are you subject to mandatory registration? If so, have you registered with ODPC and have you provided accurate and up-to-date information concerning our processing activities.			
Fairness	Have you considered how the processing may affect the individuals concerned and can justify any adverse impact. Do you handle data about individuals in ways they would reasonably expect, and can you provide an explanation of why any unexpected processing is justified?			
Processing personal data based on consent	Have you reviewed your organisation's mechanisms for collecting consent to ensure that it is freely given, specific, informed and that it is a clear indication that an individual has chosen to agree to the processing of their data by way of a statement or a clear affirmative action?			
	Do you have procedutres in place to analyse whether data subjects are required to give consent? Are procedures in place to demonstrate that an individual has consented to their data being processed? If needed?			
	Are procedures in place to allow an individual to withdraw their consent to the processing of their personal data?			
	Do you provide induvials with a fair understanding of what their data will be used for? Do you enable them to			

	access information relating to what their data will be used for when and as requested?			
Processing children's personal data	Are procedures in place to verify the age of a child. Have you obtained consent from a parent/ legal guardian?			
Processing personal data based on legitimate interests	If legitimate interest is a legal basis on which personal data is processed, has an appropriate analysis been carried out to ensure that the use of this legal basis is appropriate? (That analysis must demonstrate that 1) there is a valid legitimate interest, 2) the data processing is strictly necessary in pursuit of the legitimate interest, and 3) the processing is not prejudicial to or overridden by the rights of the individual)			

	Question	Yes	No	Comments/Remedial Action
Access to personal data	Is there a documented policy/procedure for handling Data Subject Access Requests?			
	Is your organisation able to respond to Data Subject Access requests within 14 days?			
Data portability	Are procedures in place to provide individuals with their personal data in a structured format, including a machine readable format?			
Deletion and rectification	Are there controls and procedures in place to allow personal data to be deleted or rectified (where applicable)?			
Right to restriction of processing	Are there controls and procedures in place to halt the processing of personal data where an individual has on valid grounds sought the restriction of processing?			
Right to object to processing	Are individuals told about their right to object to certain types of processing such as direct marketing?			
	Are there controls and procedures in place to halt the processing of personal data where an individual has objected to the processing?			
Profiling and automated processing	If automated decision making, which has a legal or significant similar affect for an individual, is based on consent, has explicit consent been collected?			
	Where an automated decision is made which is necessary for entering into, or performance of, a contract, or based on the explicit consent of an individual, are procedures in place to facilitate an individual's right to obtain human intervention and to contest the decision?			

Restrictions to data subject rights	Have the circumstances been documented in which an individual's data protection rights may be lawfully restricted?			

Accuracy and Retention

	Question	Yes	No	Comments/Remedial Action
Purpose Limitation	Are personal data only used for the purposes for which they were originally collected?			
Data minimisation	Are the personal data collected limited to what is necessary for the purposes for which they are processed?			
Accuracy	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
Retention	Are retention policies and procedures in place to ensure data are held for no longer than is necessary for the purposes for which they were collected?			
	Do you have procedures in place to ensure data are destroyed securely, in accordance with your retention policies?			

Transparency Requirements

	Question	Yes	No	Comments/Remedial Action
Transparency to data subjects	Are individuals fully informed of how you use their data in a concise, transparent, intelligible and easily accessible form, using clear and plain language?			
	Where personal data are collected directly from the individuals, are procedures in place to ensure you have complied with your duty to notify?			
	Are procedures in place to ensure personal data are kept up to date and accurate and where a correction is required, the necessary changes are made without delay?			
	If personal data are not collected from the subject but from a third party (e.g. shared due to legal obligation) are procedures in place to provide a data protection policy to the individuals?			
	When engaging with individuals, such as when providing a service or CCTV monitoring, are procedures in place to proactively inform individuals of their data protection rights?			
	Is information on how the organisation facilitates individuals exercising their data protection rights published in an easily accessible and readable format?			

Other Data Controller Obligations

	Question	Yes	No	Comments/Remedial Action
Data Processor Agreements	Have agreements with data processors (such as suppliers and other third parties) processing personal data on your behalf been reviewed to ensure all appropriate data protection requirements are included?			
Data Protection Impact Assessments (DPIAs)	If your data processing is considered high risk, do you have a process for identifying the need for, and conducting of, DPIAs? Are these procedures documented?			

Data Security

	Question	Yes	No	Comments/Remedial Action
Appropriate technical and organisational security measures	Have you assessed the risks involved in processing personal data and put measures in place to mitigate against them?			
Documented security programme	Is there a documented process for resolving security related complaints and issues that specifies the technical, administrative and physical safeguards for personal data?			
	Is there a designated individual who is responsible for preventing and investigating security breaches?			
	Are industry standard encryption technologies employed for transferring, storing, and receiving individuals' sensitive personal information?			
	Are personal data systematically destroyed, erased, or anonymised when they are no longer legally required to be retained.			
	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?			

Data Breaches

	Question	Yes	No	Comments/Remedial Action
Data Breach Response Obligations	Does the organisation have a documented privacy and security incident response plan?			
	Are there procedures in place to notify the Office of the Data Protection Commissioner of a data breach?			
	Are there procedures in place to notify data subjects of a data breach?			
	Are plans and procedures regularly reviewed?			
	Are all data breaches fully documented?			
	Are there cooperation procedures in place between data controllers, data processors and other partners to deal with data breaches?			