CATHEXIS PRIVACY GUIDE

PROTECTION OF PERSONAL INFORMATION ACT

11 February 2021

Contents

Disclaimer
Cathexis has made every effort to ensure the accuracy of this document, but the information contained within it is for general information purposes only. The reader should not rely on the said information as a basis for making any legal or other decisions. While Cathexis will endeavour to keep the information up to date and correct, it makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, or suitability, with respect to the information contained in this document. Any reliance risk placed on such material therefore lies strictly with the reader and or recipient of the information.

1. CathexisVision VMS and privacy compliance

This Privacy Guide provides guidelines for understanding personal information protection when using CathexisVision software, particularly in complying with the Protection of Personal Information Act. The **Protection of Personal Information (POPI) Act** was signed into law in South Africa in November 2013, with various sections coming into effect in the years that followed. The POPI Act requires South African institutions to conduct themselves responsibly when collecting, processing, storing and sharing personal data by being accountable for any abuse or compromise of this information. This document outlines the key features of POPI so that customers understand their data protection responsibilities when using CathexisVision software.

Three key themes of the POPI Act are respect for consumer privacy, provision of transparency on information processing, and provision of security as it relates to cybersecurity and identity theft (see *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa* by Dronamraju, Xulu, McLacklan and Uys, p. 15). By developing an organisational culture underpinned by cybersecurity compliance and respect for your customers' privacy rights, your company can protect its brand and gain a competitive advantage. For your company to plan its POPI compliance, it will be helpful to:

- Find out how your business interacts with the legislation
- Gather a team, designate an Information Officer and deputy, and register them with the Information Regulator
- Devise a plan and implement it.
- Depending on the company size and data processing scale, set up a budget for POPI compliance.

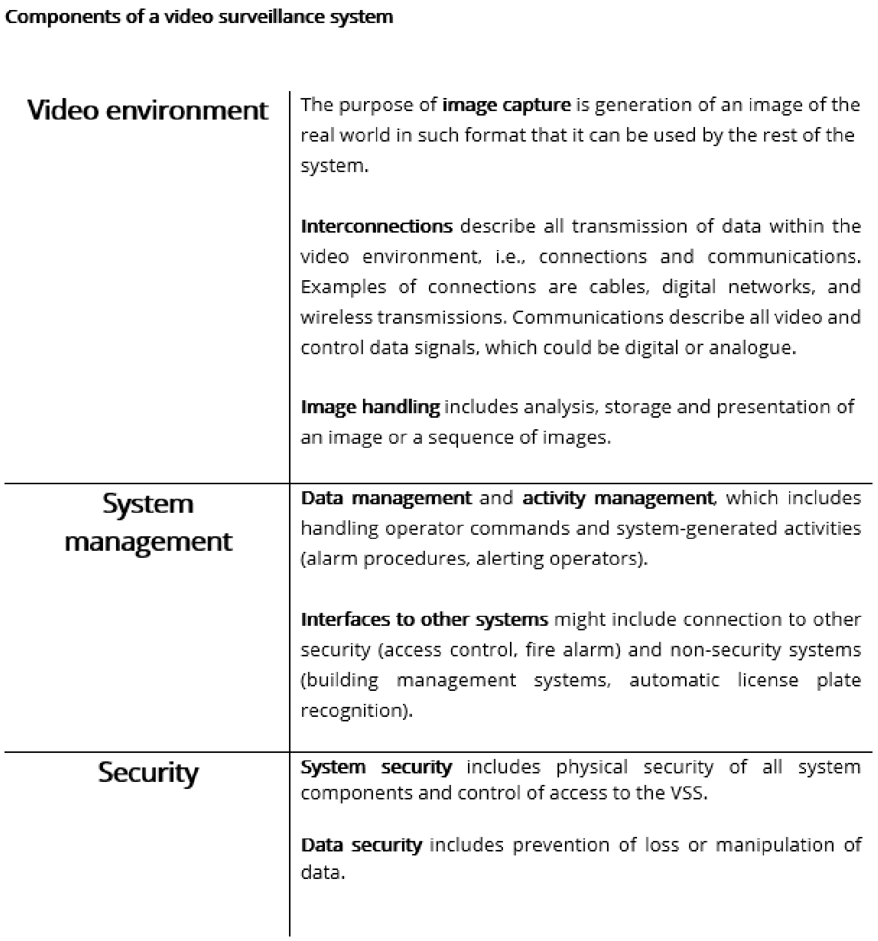
The deadline for registering the Information Officer and deputy is **31 March 2021**, and the deadline for enforcement of the POPI Act by the Information Regulator is **1 July 2021**.

1.1 What parties are involved?

POPI Act applies to any organisation operating in South Africa, or organisations operating outside South Africa which offer products and services to customers or businesses within South Africa. These are the relevant parties in privacy compliance as it relates to video surveillance:

- **Data subject**: the person whose personal information is collected and used. In video surveillance, data subjects are the individuals viewed.
- **Responsible party:** defined in the Act as "a public or private or any other person which, alone or in conjunction with others, determines the purposes of and means for processing personal information". The responsible party must "ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures".

1.2 Video surveillance system definitions



Components of a video surveillance system

Video environment	The purpose of **image capture** is generation of an image of the real world in such format that it can be used by the rest of the system. **Interconnections** describe all transmission of data within the video environment, i.e., connections and communications. Examples of connections are cables, digital networks, and wireless transmissions. Communications describe all video and control data signals, which could be digital or analogue. **Image handling** includes analysis, storage and presentation of an image or a sequence of images.
System management	**Data management** and **activity management**, which includes handling operator commands and system-generated activities (alarm procedures, alerting operators). **Interfaces to other systems** might include connection to other security (access control, fire alarm) and non-security systems (building management systems, automatic license plate recognition).
Security	**System security** includes physical security of all system components and control of access to the VSS. **Data security** includes prevention of loss or manipulation of data.

The definitions in the table above are from the *European Data Protection Board Guidelines 3/2019 on processing of personal data through video devices*, page 25.

The European Data Protection Board provides helpful definitions of terms relating to video surveillance and privacy.

A **video surveillance system** (VSS) consists of analogue and digital devices, as well as software, for the purpose of capturing images of a scene, handling the images and displaying them to an operator.

1.3 Privacy compliance while using CathexisVision VMS software

A product, in itself, is not said to be POPIA compliant: a company cannot declare whether or not VMS software is compliant. Compliance depends on the combination of an organisation's access to and use of personal data in its use of products. Your company is legally liable to account for the ways in which it uses, stores and protects personal information.

It is essential that companies ensure that their use of CathexisVision software falls within the regulations set out by the POPI Act. This Privacy Guide is available to help Cathexis clients understand how they can do this.

2. Understanding POPIA

2.1 Protection of Personal Information Act

POPIA is a comprehensive law which seeks to which seeks to safeguard the personal information of natural persons and, where applicable, juristic persons. Organisations are mandated to judiciously handle the capture, processing, and storage of personal information within the framework set out in the Act. Non-compliance could have dire consequences for an organisation.

Personal information is defined by the Act as meaning:

1. Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
2. Information relating to the education or the medical, financial, criminal or employment history of the person;
3. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
4. The biometric information of the person;
5. The personal opinions, views or preferences of the person;
6. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
7. The views or opinions of another individual about the person; and
8. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

The Act's preamble selects these aspects as the most important:

- To promote the protection of personal information processed by public and private bodies;
- To introduce certain conditions so as to establish minimum requirements for the processing of personal information;
- To provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000;
- To provide for the issuing of codes of conduct;
- To provide for the rights of persons regarding unsolicited electronic communications and automated decision making;
- To regulate the flow of personal information across the borders of the Republic;
- And to provide for matters connected herewith.

2.2 The 8 POPIA Conditions

One of POPIA's main principles is "**privacy by design**". Privacy and security need to be embedded within all of the organisation's processes and systems. Privacy is necessarily about security: for information to remain private, it must also be held securely. Eight conditions form the foundation of compliance and determine how personal information may be legally gathered, processed and held under the Act.

ACCOUNTABILITY: a responsible party must be selected to carry out the task of ensuring compliance within the organisation.

PROCESSING LIMITATION: the personal information must be obtained directly from the data subject, who must be aware of this. The organisation must obtain consent from the data subject for their information to be gathered, including when the information has been gathered by a third party and is being used by your organisation. The amount of information being gathered and stored must be for a specific purpose and not be "excessive". The data subject must also consent if the organisation gathers personal information for "future processing".

PURPOSE SPECIFIC: the purpose of collecting personal information must be lawful, adhered to, and documented. The data subject has the right to know the reason for gathering their information. Personal information may only be held for a specific time period linked to its purpose. The organisation must give a date on which the information will be destroyed, and show how this destruction prevents the information's reconstruction after the authorised period of retention.

FURTHER PROCESSING LIMITATION: to use information gathered for a specific purpose for a later secondary purpose, the organisation must have the data subject's consent. The organisation must inform the data subject of the purpose as well as the period for which it will be used and held.

INFORMATION QUALITY: the responsible party in the organisation must ensure that the personal information is reliable and accurate, even if the information must be sent back to the data subject for validation. Data subjects must be given details of how to withdraw their consent to the holding of the information, as well as details on how they may update their information, on a regular basis.

OPENNESS: data subjects must be informed of the gathering of personal information at the time it is collected, and they must have given their consent. The data subject must be informed of the party in the organisation who is responsible for data protection, their rights as laid out in the Act, and details on how they may lodge a complaint.

SECURITY SAFEGUARDS: the personal information kept by the organisation must be secured against loss, unlawful access, interference, modification, unauthorised destruction and disclosure. The organisation must perform a risk assessment (to prevent a breach) and set a procedure for what to do in the event that data security is breached. There needs to be a strict policy regarding which employees have access to personal data. If personal information privacy safeguards are breached, the data subject and the Information Regulator need to be informed.

DATA SUBJECT PARTICIPATION: the data subject may ask whether their information is being held and this request may not be declined or charged for. The data subject may correct their stored personal information at any time or withdraw their consent to it being stored, at any time.

Five steps to take to ensure POPI compliance within your organisation:

1. Appoint an information officer within the organisation.
2. Become familiar with the Act and create awareness of the Act within the organisation on all levels, especially with key personnel and decision makers.
3. Carry out a personal information impact audit to assess the current level of data protection compliance within the organisation.
4. Develop a compliance framework, which can include processes and policies, and manuals to document these in order for everyone in the organisation to become familiar with the Act and the consequences of non-compliance. A manual should include the organisation’s policy regarding:
    - Data collection (type of data, purpose, consent, legal aspects, minimality, and transparency), data access and accuracy (correct, complete, reliable and process of updating information).
    - Data usage and restrictions (purpose, relevance, restrictions, legality, permission, limitations).
    - Data storage (physical, off-site, electronic, back-up, cloud storage).
    - Data security safeguards (physical, electronic, network, password control, disaster recovery) and disclosure (legality, consent, data subject awareness, data request handling).
    - Responsibilities (all directors, top management, information officer, personnel dealing with personal information, vendors, contractors, suppliers).
    - Complaints (process, handling, legalities, transparency).
    - Retention (retention schedule), destruction (destruction schedule), implement staff awareness training (all current staff, new appointees and regular refresher training).
5. Put procedures in place to implement the framework.

2.3 Differences between POPIA and GDPR

South Africa's data protection laws compare quite favorably to those of other countries. Although the POPIA and General Data Protection Regulation's fundamental conditions for lawfulness of processing personal information are close and the terminology is fairly similar – for example, the data controller (GDPR) is the equivalent of a responsible party (POPIA), and the data protection officer (GDPR) is essentially the same as the information officer in POPIA terminology and substance – there are differences which may become greater or lesser, depending on the respective future court decisions and precedents. Here are some key differences:

- Where applicable, POPIA includes the personal information of **juristic persons** (a juristic person is a non-human legal entity entitled to rights and duties in the same way as a human person). The GDPR, by contrast, does not protect legal entities.
- POPIA distinguishes that **consent** is "subject to interpretation regarding what constitutes a voluntary expression of will".
- POPIA does not include the concept of a **data processor** and thus legal responsibility solely falls on the party responsible for controlling the data. The GDPR states that both the controller and processor "shall implement appropriate technical and organization measures to ensure a level of security appropriate to the risks represented".
- The GDPR's **Supervisory Authority** monitors compliance with the GDPR, whereas under POPIA, parties need to seek authorisation from the **Information Regulator** to process unique identifiers of data subjects for purposes different to those originally intended, information on criminal behaviour on behalf of third parties, and information related to credit reporting. Furthermore, the Information Regulator needs to authorise the transferal of special personal information or children's personal information to a third party in a foreign country that does not have necessary protections in place for processing personal information.
- POPIA's **Information Officer** and GDPR's **Data Protection Officer** are comparable roles. However, the Information Officer is responsible for making sure the organisation complies with POPIA, while the Data Protection Officer is an independent consultant who supervises the company's compliance with GDPR.
- POPIA stipulates that a **Deputy Information Officer** assists the Information Officer with their tasks, but GDPR does not set out an equivalent role.
- POPIA includes information about criminal offenses within the category of **special personal information** (special categories of personal data under GDPR), whereas GDPR does not.
- In the **justification** of processing personal information, POPIA allows for the legitimate interests of third parties.
- In the instance of a **data breach**, there are no criminal offenses under the GDPR, but it does stipulate far larger fines than POPIA.
- The GDPR exempts certain SMEs from having to **keep data records**, whereas POPIA does not.
- The GDPR has various "**extras**" which POPIA currently does not – a definition of generic data, the requirement that data controllers do data protection impact assessments, and clauses dealing with the right to be forgotten and data portability.

2.4 The importance of compliance

There are risks to non-compliance with the POPI Act: damage to the company's reputation and enforcement action by the Information Regulator. Criminal penalties are possible but unlikely, unless violations of POPI become frequent – this would likely happen as a result of ineffective or negligent organisational behaviour in dealing with POPI provisions.

The risks of non-compliance are generally higher for *business-to-consumer* companies (businesses that sell directly to the consumer, such as banks, retail, social media entities, real estate agencies, debt collection, and membership organisations) than for *business-to-business* companies (such as industrial companies, mining, tech companies servicing business such as cloud hosting companies, accounting firms, and law firms). However, service-based business to business companies may also be high-risk, such as those involved in data collection.

Although the Information Regulator is mandated to treat all entities equally, there are still entities at a higher risk of enforcement: for example, large companies (those with an annual revenue of more than R500m, process more than 500k consumer records, employ more than 100 personnel, and use contractors to manage your technology), especially those with fairly constant interaction with consumers. According to *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa,* business-to-business companies "with lower customer footprint" are at a significantly lower risk of enforcement, "so long as they conduct meaningful privacy impact assessments" (p. 29).

As the limits of the Protection of Personal Information Act have not yet been tested by the courts and Information Regulator, the best business plan is to act to mitigate risks.

3. Personal information and using CathexisVision software

3.1 What is personal information?

Under the POPI Act, **personal information** is broadly defined as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular consumer.

Personal information should not be confused with *personally identifiable information*. Personal information encompasses far more than personally identifiable information: for instance, personal information includes biometric data, racial and social profile data, personal opinions, email or correspondence, and views or opinions of a third person. Although most privacy laws consider *personally identifiable* information as a basis for privacy, POPIA is based on personal information.

If the data can be de-identified from the consumer, such data is exempted from being considered personal information. But it may not be re-identified. Any data that cannot be directly or indirectly linked to a consumer is also exempted. (*The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa*, pp. 151-2)

When using CathexisVision, personal data could include the processing of video footage and location information, facial recognition, automatic number plate recognition, or access control systems.

Personal information does not only apply to the subject viewed in footage. The operator must consider whether their interaction with user data – such as activity logs, timestamps, and metadata – constitutes the processing of personal information.

3.2 Online identifiers

Online identifiers include internet protocol (IP) addresses and cookie identifiers. Other examples which may constitute personal information include:

- MAC (Media Access Control) addresses
- Advertising IDs
- Pixel tags
- Account handles, and
- Device fingerprints

Real-world examples falling within this category of personal information would include:

- An individual's social media 'handle' or username is still considered personal information as it is able to identify the individual and distinguish them from others.
- Cookie technologies involve the processing of personal information if used to create a profile of the individual.

Facial recognition technologies for the purpose of identifying an individual would constitute the processing of personal data, in that they record features which distinguish the individual from other individuals.

3.3 Special categories of personal information

Section 26 lays out prohibitions on processing special personal information (concerning a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information, or the data subject's criminal behaviour). Chapter 3 discusses authorisation concerning each of these areas.

In video surveillance, special categories of personal data can potentially arise when the system is set up near prisons, hospitals or clinics, mines, places of worship, universities and other political, social, labour or legal institutions.

3.4 Pseudonymisation and anonymisation

Pseudonymisation is merely a security measure. Pseudonymised data is still personal information and thus subject to POPI requirements. An example of pseudonymisation is using a reference number for an individual, with the information tying the data to the individual held separately. Operators can still re-link the information with the data subject, but this method can reduce the risks to the data subject resulting from breaches. Organisations often classify their data as **anonymised** when it is merely **pseudonymised**. For data to be anonymised, it must no longer be able to be used to identify or *re-identify* the individual. It is recommended that organisations anyonymise data, where possible, as a way to limit risks to both the operator and the data subject.

3.5 What to do when uncertain about the status of information

When there is uncertainty as to whether the data is personal information, it is a matter of good practice to treat the data with care, hold and dispose of the data securely, protect the data from unlawful disclosure, have a clear and lawful original purpose for processing the data and maintain transparency about how the information is being collected.

4. Guidelines for responsible parties/operators

The responsible party or operator must know and document what data it holds, the data source, who the data is shared with, and how it is used.

✓ Assess data flows with information audits.

✓ Maintain documentation of personal data processing.

Major tasks to be performed for POPI Act compliance:

Note: give each task an owner to take accountability to complete the task.

- Appoint an Information Officer and deputies.
- Complete a POPI Privacy Impact Assessment.
- Assess the impact on marketing and direct marketing.
- Train the Information Officer and deputies.
- Evaluate and engage with POPI consulting vendors (however, avoid signing long-term agreements with POPI vendors).
- Evaluate and deploy Data Subject Access Request intake software.
- Collect Data Collection Categories.
- Collect Data Collection Purpose.
- Collect Data Collection Sources.
- Collect third-party categories (that you sell to).
- Create a list of partners and customers.
- Applications that store personal information (inventory).
- Determine the scope of privacy APIs for service providers.
- Create generic privacy amendments.
- Website disclosures and changes.
- Execute communication plan.
- Top 20 Security control assessment.
- Assess data security tools vendors and deploy.
- Assess POPI training and get training for the team.
- Audit all activities.

The above list is from *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa* (Dronamraju, Xulu, McLachlan & Uys, 2021, p. 82).

POPI regulations and requirements can be classified into the following categories:

1. **Notices and policy changes** (notice to consumers of personal information collection and the categories of info you collect, and the purpose for the collection as well as the source)

- On the website have link/s to the list of categories of information you collect, purposes of collection, collection sources, link to your privacy policy, and Data Subject Access Request form.
- Organisations are required to have a privacy policy notice on their websites. (**Recommended**: have a version in plain English, an audio download of that version, and one in English but in the legal vernacular. If other languages are used with clients, have policy notice in those languages too.)
- A note re: direct marketing: POPI forbids the buying or licensing of personal information for direct marketing purposes. All information must be collected directly by the first party, otherwise the processing is deemed unlawful.

2. **Response to privacy requests** (see 5.6 below)

3. **Data lookup and access**

DATA MAPPING TOOLS: find out where your data is

DATA DISCOVERY TOOLS: use the data map to classify the type of data and sensitivity of that data

DATA LOOKUP AND ACCESS TOOLS: read, modify or delete data.

4. **Data security**

Two areas to consider:

- Implementing “reasonable security procedures” to address the breach of unencrypted and non-redacted personal information. (See the Center for Internet Security (CIS) critical security control list and implement all 20 controls – not implementing them may be seen as a lack of reasonable security.)
- Anonymisation of data upon request for data deletion from a consumer.

5. **Data as a service business**

“Service providers, specifically software companies, need to add a new privacy data lookup service to their offering. It is best to provide this using Privacy APIs.”

- Give your team clear goals: 1. Avoid enforcement action by Information Regulator; 2. Protect company reputation; 3. Prevent data breaches and security incidents; 4. Be on budget 5. Be on time (30 June, 2021).
- Give your team the scope, schedule, and resources to make this possible.

The above information is from *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa* (Dronamraju, Xulu, McLachlan & Uys, 2021, pp. 37-8 and 75-9).

The best strategy to be ready for POPI compliance is to:

- be transparent with your privacy policy and data collection
- provide a webpage for DSAR requests
- ask your partners and service providers the right questions
- know your data
- be responsible for protecting your data from exfiltration

Items to budget for with initial (and to some extent ongoing) costs:

1. Legal help.
2. Data assessment, mapping and discovery.
3. Request processing each year.
4. Security assessment.
5. Privacy request intake software (annual licences).
6. Data lookup (using internal teams will reduce this cost).
7. Data security (per year).
8. Cyber liability insurance (ongoing).
9. Ongoing compliance costs.
10. Costs of training own staff (internal POPI team) at the start to reduce costs of hiring these things out to contractors (especially doing training to reduce the cost of request processing, which can be a significant cost).

The above information is from *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa* (Dronamraju, Xulu, McLachlan & Uys, 2021).

4.1 Organisational procedures

The organisation needs to demonstrate a culture of data protection compliance. Responsible parties and operators must implement proportional organisational and technical measures. Organisations need an **internal framework** and set of **policies** which implement compliance. Safeguards to data and privacy should be built into not only the design specifications of the technology, but also the organisation's practices and culture.

✓ Organisations should aim for technical solutions which enhance data and privacy security and are thus "privacy-friendly": for example, allowing masking or scrambling irrelevant areas or editing out third-person images.

Responsible parties should implement the technical and organisational measures needed for data protection *before* they begin processing footage.

4.1.1 Staff

All staff members within the organisation must be aware of and obligated to adhere to the principles of data privacy and protection.

✓ Train the organisation's staff in data protection policy.

4.1.2 Information Officer

It is mandatory to appoint an Information Officer at every business or public entity that processes or stores personal data of South African residents. Regardless of the size or type of entity, there is a need for an Information Officer. While the organisation's CEO is ultimately responsible for POPI compliance, the Information Officer may be held criminally liable for breaching the Act. Penalties can include fines or imprisonment of up to 3 years.

✓ Appoint an Information Officer within your organisation.

Who should be the Information Officer (and deputy)?

When hiring or designating an Information Officer and deputy, it is important to consider the role's range of responsibilities and the necessary areas of knowledge:

1. Data subjects and the understanding of the business to process DSAR requests.
2. Data stores, the mapping, and understanding of systems.
3. Range of processing, including an understanding of interaction with vendors and service providers.
4. Data protection and security understanding of framework and principles.
5. Have a legal framework and understanding of lawful data processing.

A background in business process and information technology is more important than legal knowledge when appointing an Information Officer. It is helpful to use the organisation's existing managers as Information Officers, as they know the business, and to hire a deputy Information Officer who has expertise in the data protection aspects of the role (monitoring data subject access requests, data protection, compliance and IT).

The Information Officer may have more than one deputy.

When the organisation installs a video surveillance system or updates its video surveillance system, the Information Officer should advise this process so that any updates comply with the POPI Act.

The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa by Dronamraju, Xulu, McLacklan and Uys, outlines the Information Officer's responsibilities (p. 47):

- Bring the business or public entity in compliance with the POPI Act.
- Develop a policy on how the business or public entity should implement the lawful processing of personal information.
- In the case of public entities (provincial and national departments), issue notices and encourage employees to implement lawful processing of personal information.
- Define clearly and generally provide a reasonable opportunity to the consumers to conform to data subject access request process (DSAR), wherein any reasonable DSAR request will not be denied or rejected.
- Oversee, monitor, and govern the DSAR request processing.
- Ensure the compliance framework is developed, implemented, monitored, and maintained.
- Periodically conduct privacy impact assessments.
- Develop and maintain a PAIA manual.
- Develop measures to process DSAR requests for information access.
- Conduct internal awareness and training.
- Support the Information Regulator in their investigations.
- Submit to the Information Regulator an annual report on activities related to the POPI Act compliance.

✓ Keeping a running overview and maintain records of data processing activities.

4.2 Setting up a video surveillance system

4.2.1 Technical and security measures

CathexisVision supports encryption for all external site connections and offers four selectable encryption levels. It also has secure IP camera connection and data encryption.

Cathexis has increased the level of video "signing" to explicitly associate the signatures with the source, providing more detail in the archive player of the video verification results.

4.2.2 Video Surveillance Policy

✓ Before processing, the organisation, in consultation with its Information Officer, needs to outline the purpose of its video surveillance and ensure that it complies with POPI.

System and data security measures:

- Protection of the entire VSS physical set-up (including cameras, cabling, and power supply) against physical interference and theft.
- "Protection of footage transmission with communication channels secure against interception".
- Data encryption.
- Use of both hardware and software solutions such as firewalls and antivirus.
- "Detection of failures of components, software and interconnections".
- "Means to restore availability and access to the system in the event of a physical or technical incident".

Access control measures:

- Keeping secure from unauthorised third parties the premises where the monitoring of the surveillance footage is carried out and the footage is stored.
- Positioning monitors which are in open areas so that only authorised staff may view them.
- "Procedures for granting, changing and revoking physical and logical access are defined and enforced".
- Keeping user authentication methods, such as passwords, updated and implemented.
- "User performed actions (both to the system and data) are recorded and regularly reviewed".
- Weaknesses in the system are identified and addressed timeously by monitoring and detecting access failures regularly.

A detailed privacy policy should have the following sections (see *The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa*, p. 90):

- Types of information collected
- Purpose of collection
- Sources of information collection
- Direct marketing policy
- Information protection
- Your rights and choices
- Children and consent from guardians
- Changes to policy

4.2.3 Personal Information Impact Assessment

Before your organisation installs and operates a video surveillance system, you need to assess whether the system will comply with the POPI Act and data protection laws. Depending on the outcome of the assessment, the organisation might discontinue its plans, or carry out further data security and privacy compliance measures.

Does the video surveillance system affect the data subject's rights? If so, does it violate their rights? This has to be **balanced** against the operator's needs and legitimate interest. Consider, for example, a video surveillance system which was installed to prevent theft from within a parking lot, and the filming of the parking lot is also protecting the data subjects' interest by protecting their cars while parked in the lot. If the filmed area is not being used by the data subject for recreational purposes, the **legitimate interest** of the operator to secure the parking lot with video surveillance overrides the data subject's right to not be monitored.

The potential abuse of video surveillance can violate data subjects' rights, such as:

- Sharing footage with users without access rights
- Recording data subjects' activities without consent
- Using footage to intimidate or coerce data subjects
- Monitoring the behaviour and actions of employees

4.2.4 Cameras

Ensure that camera functions that are not necessary for the initial processing purpose are deactivated to prevent accidental non-compliance. These might include zoom capability, unlimited movement of cameras, analysis and audio recording functions.

4.2.5 Boundaries of surveillance

Generally, the surveillance must end at the property's boundaries in the event of it being used for the security surveillance of that premises. However, if filming goes beyond the boundaries of the premises, the operator should block out areas not needed for security surveillance, using means such as pixelating non-relevant areas.

Physical areas where data subjects' rights and legitimate interests will often override the operator's legitimate interests to film are those used for recreational activities, and public areas typically used for "recovery, regeneration, and leisure activities", as well as sitting areas, restaurants, parks, and fitness facilities.

When creating video surveillance policies and procedures, consider the following:

1. The role and person responsible within the organisation for the management and operation of the VSS.
2. The purpose of the video surveillance.
3. Where and when the video surveillance is allowed and not allowed – for example, in the case of hidden cameras.
4. Transparency and information obligations.
5. How video is recorded and for what duration (this would include procedures regarding archiving stored footage relating to security incidents).
6. Which staff need to be trained in relation to these changes, and when.
7. Who within the organisation has access to the footage, and for what purposes?
8. Operational procedures, such as what response is followed in the event of a data breach.
9. Procedures for data access requests.
10. Procedures for VSS "procurement, installation and maintenance" (*EDPB Guidelines*).

4.3 Right to be informed

✓ Operators should have a lawful and documented purpose for which they collect personal information.

✓ Operators must ask for the consent of data subjects, record that consent, and carry out a review of the way in which it requests, records and manages consent.

✓ As an operator, it is your company's responsibility to provide information about its data protection activity to data subjects. This includes the following actions:

✓ Provide information on-site where data will be collected from data subjects

The operator should adopt a layered approach of methods to ensure transparency. The first layer is the **notice** to the data subject that they are being filmed or observed "using automated data capturing devices or data capturing software such as cameras" (EDPB guidelines, page 21). The second layer should be accessible to data subjects without entering the monitored area.

For more information on the on-site *Privacy Notice* see Appendix 1: Document Templates.

4.3.1 Data breach

For a data breach to lead to action from the Information Regulator, each record must have 2 or more pieces of personally identifiable information (*The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa*, p.35).

Consequences to natural persons due to a data breach could include:

- Loss of control over their personal data
- Limitation of their rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy

✓ Operators must have an information security policy which has procedures to identify, report, manage and resolve personal data breaches.

4.4 Data Subject Access Requests

Section 24 of the POPI Act states that a data subject may request a responsible party to:

a) Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
b) Destroy or delete a record of personal information about the data subject that the responsible party is no longer authorized to retain in terms of section 14.

There are several types of Data Subject Access Requests (DSAR), relating to data subjects' rights:

- Right to access personal information
- Right to know personal information
- Right to correct personal information
- Right to object to processing
- Right to direct marketing opt-out
- Right to direct marketing opt-in
- Right to repeal the rejection of request
- Right to delete personal information

Note that unlike the General Data Protection Regulation, POPIA does not broadly support the *right to be forgotten* – the data subject needs to motivate how the request meets one of the criteria set out in Section 24(1)(a).

These rights enable individuals to know the operator's purpose in using their personal data and allows them to check that the operator is carrying out this purpose lawfully. Generally, most of this information will be in the initial privacy notice or warning signs given before gathering the data.

✓ Operators need to have a procedure for responding to requests by data subjects.

Actions to take for settings up DSAR requests:

1. Select and deploy DSAR request intake software
2. Deploy two methods for intake (web-form and toll-free number)
3. Do email and OTP verification of requests
4. Have your email reply templates ready
5. Define your workflow for each type of request.

The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa (p. 107)

All businesses will need a privacy data subject request **intake management system**. A good tool for this can help increase overall productivity of your business. It is highly recommended that the company buys DSAR intake request management software from a third-party vendor to automate the DSAR intake process.

- Diligent verification is crucial, as responses to the wrong consumer may be considered a data breach, which could result in an investigation by the Information Regulator. Consider using a one-time pin (OTP), email verification or similar two-factor authentication.
- With businesses that have a consumer-facing location, a DSAR intake method must be also be able to be done on-site. or email verification.
- When transmitting persona information to data subjects, be vigilant about security. Verify the email, verify the address (in the case of a letter), and if the response is carried out using a portal ensure appropriate security (HTTPS, firewall etc.) and that the account to access the portal is authenticated.

Data Subject Access Request process:

1. VERIFY REQUEST: email, OTP or location verification with your visitor's IP address available in your website analytics tool; eliminate requests from outside SA with a one-time location tracking tool when the requestor submits the request. Verification is important because if you give the information out to the wrong person this is a data breach.
2. ASSIGN REQUEST: with automation, a 1-2 person team is sufficient to deal with all requests; training for DSAR requests is necessary under POPI regulations.
3. FETCH DATA: data integration and third-party APIs help collate and collect all data needed.
4. LEGAL REVIEW: for 3 types of request and exceptions add legal review process to reduce risk.
5. RESPOND: keep an audit trail of this. POPI requires request be processed within 30 days; the clock starts upon receipt of request; a good DSAR process should have the request processed within 5 days.

The POPI Act Compliance: Navigate Privacy and Security Compliance in South Africa (p. 97)

* NOTE: For POPI compliance a requestor is a SA resident.

4.4.1 Access, correction and restriction of processing

If data is filmed in real-time and not held beyond the moment of filming, the operator would only be able to give the data subject information that no data is being held.

When a data subject wants to see footage containing persons in addition to the data subject, viewing such footage would constitute additional processing of the personal of the other data subjects, which would adversely their rights and freedoms. However, this hurdle may not be used by the operator to prevent data subjects' legitimate claims to their data from being fulfilled. Technical measures – such as image editing via masking or scrambling – should be used to fulfil such access requests.

If the operator would have to search through a significant amount of stored footage, the operator may not always be able to find the footage of the data subject. It is advisable that the data subject gives the operator a **specific time frame** within the footage in which to find the data subject, and the operator needs to notify the data subject regarding the **qualifiers** needed to assist the search through stored data. If the search is still futile, the operator must **notify** the data subject.

For more information on *Data Subject Access Requests*, see Appendix 1: Documents.

✓ When data is transferred, security measures need to be in place. (See Exporting data.)

4.4.2 Deleting data

✓ Dispose of data securely.

✓ Operators must retain video footage for as long as it meets the stated purpose of the surveillance system, and dispose of personal data securely once it is no longer needed.

✓ If data needs to be deleted, the information must be deleted from both live and backup systems.

In a video surveillance system, it is not reasonable to erase an individual from video footage, but it is possible for the operator to select how long recordings are kept.

CathexisVision 2020 offers optional database shredding, which enables permanently destroying video older than the user-defined recording limit.

4.4.3 Right to object

If a data subject objects to the surveillance, the operator will need to show that it has a ***compelling*** legitimate interest (see Video Surveillance Policy) that is sufficient to override the rights of the data subject, or that the surveillance is needed for a legal claim. In the case of surveillance for security purposes, there needs to be a “real-life situation of distress” at hand which would mean a past event proves a need for security surveillance. The European Data Protection Board advises that “given a real and hazardous situation, the purpose to protect property against burglary, theft or vandalism can constitute a legitimate interest for video surveillance”.

✓ Operators should have procedures for handling data subjects’ objections to the processing of their personal data.

A data subject may object to the filming at any point from before entering until after leaving the monitored area. Without both compelling and legitimate grounds, the operator’s monitoring of the area is only lawful if the operator can immediately stop the processing of personal data if requested. Alternatively, it is only lawful if the area is restricted so that an operator can be assured that the data subject has given approval before entering. Thus the restricted area cannot be an area that a data subject has a right to access by way of their citizenship.

4.5 Security and storage

4.5.1 Storing data

Personal data should not be stored longer than necessary for the purpose for which it is being processed. The storage period needs to be set and defined for the particular purpose.

The longer footage is stored, the greater the argument needed to justify the necessity of storage and the legitimacy of its purpose.

Storage of footage can be approached in various ways to avoid risk for data subjects, and for the organisation to prevent accidental breaches of POPI provisions. The "Black Box" approach allows for footage to be automatically deleted (after a set storage period) but still available to be accessed in the event of an incident. Another solution might be to opt not to record and use "real-time monitoring" of the footage.

✓ Implement security measures to protect the personal data being held.

4.5.2 Exporting data

✓ **Security measures when transferring data:**

- Have proper systems in place to record Subject Access Requests.
- Train staff who will handle SARs.
- Before responding to a request, check addresses.
- When sending information electronically, it is advisable to provide it in an encrypted form.
- Send a passphrase separately to the individual.
- If sharing a hard copy of information, using a courier or special delivery is good practice.
- Providing remote access to a secure system, so that the data subject can download a copy, can support the secure transfer of information.

4.5.3 Biometric data

It is advisable to design a system which either does not capture, or minimises the capturing of footage revealing sensitive personal data.

Processing special categories of personal information means that the operator needs a far higher level of caution and security.

Biometric data use, and particularly facial recognition “entail heightened risks for data subjects’ rights” and the operator must carefully assess the impact on the rights of the data subjects, and even consider other means of surveillance.

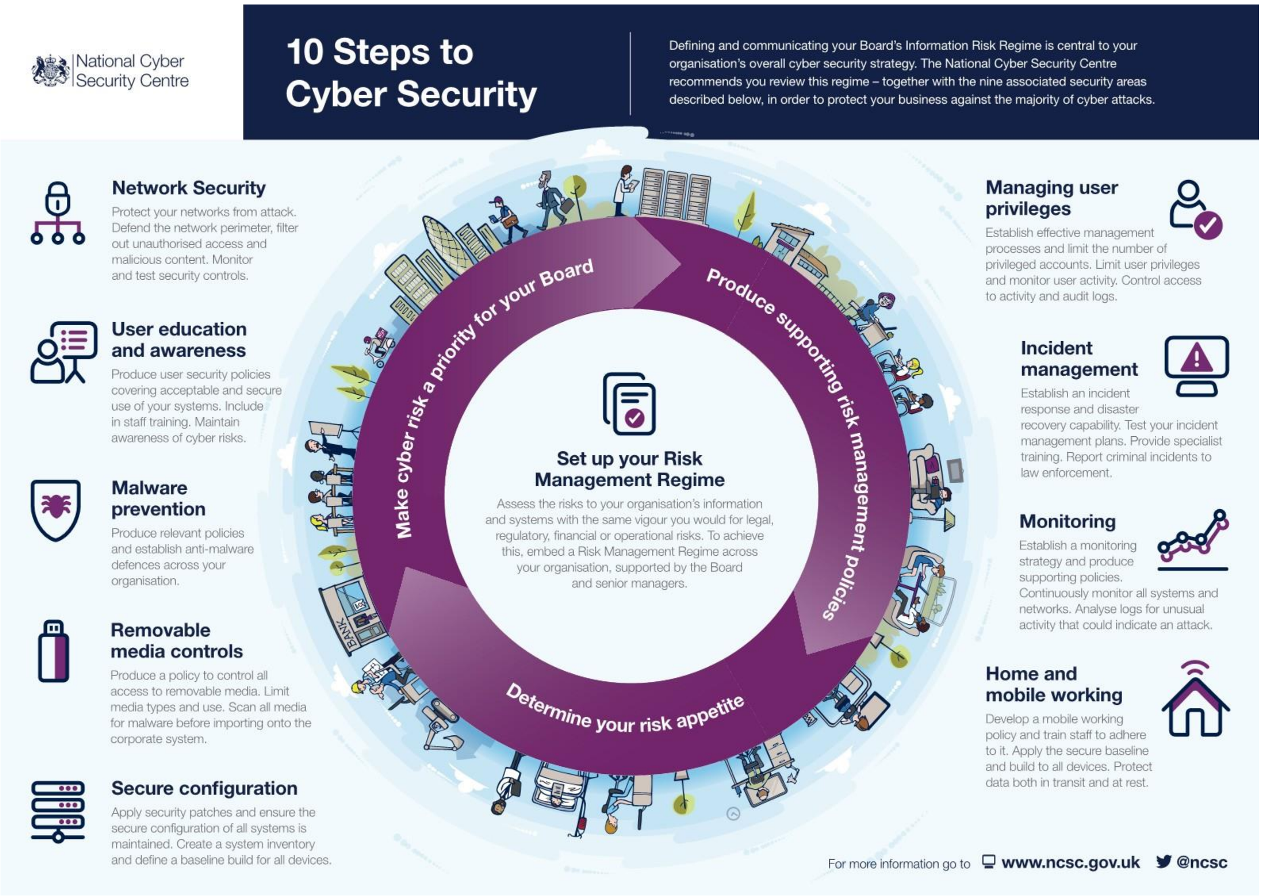
The operator must not make consent to biometric processing a condition to making use of and accessing its services. There must always be an alternative authentication solution available for the data subject, which does not involve biometric processing and does not involve additional costs or restraints for the data subject.

The EDPB suggests the following to minimise risks while processing biometric data:

1. DATA MINIMISATION: only extract data from the digital image which is required for the purpose.
2. DATA PROTECTION: ensure that templates cannot be “transferred across biometric systems”.
3. DATA STORAGE SECURITY: such a setup may need to include “encrypting the template using a cryptographic algorithm” but either way, measures must be taken to avoid unauthorised access to the template’s storage location.
4. ACCOUNTABILITY: steps must be taken to preserve the “availability, integrity and confidentiality” of the data being processed.
    a. “Compartmentalise data during transmission and storage,
    b. store biometric templates and raw data or identity data on distinct databases,
    c. encrypt biometric data notably biometric templates,
    d. define a policy for encryption and key management,
    e. integrate an organisational and technical measure for fraud detection,
    f. associate an integrity code with the data (for example signature or hash), and
    g. prohibit any external access to the biometric data”.
5. DELETION OR ERASURE OF DATA: ensure that the raw data is effectively deleted. The risk is that a biometric data base can be derived from the raw data and must then also be deleted. In the case where the raw data needs to be retained it must be kept in such a way that a biometric template cannot be created again – for instance by using a “noise-additive method” such as watermarking. If there is a security breach and unauthorised access to stored biometric data takes place, then such data must be deleted. The operator must also delete any data not needed for processing “at the end of the biometric device’s life”.

4.5.4 CathexisVision cybersecurity

By strengthening their organisation's cybersecurity measures, operators can strengthen their compliance with the POPI Act.



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

The National Cyber Security Centre is a UK government organisation that advises the public and private sector on how to prevent threats to computer security.

To ensure that video footage does not get into the public domain, CathexisVision has the ability to:

- Archive video that can only be played back under password control.
- Overlay a watermark on the video to depict the source of the information (for example, user info).

Communication between CathexisVision components

CathexisVision ensures secure communications between its components, including Recording servers to clients, other recording servers, video walls, and alarm management gateways. The security of communication between these components is achieved by the following measures:

1. All external site connections support encryption of varying levels:
   - Disabled
   - Minimal (only critical connections encrypted)
   - Secure (the default option, which encrypts all connections except those with high-volume video)
   - All (all connections encrypted, including high-volume video links)
2. Passwords are never stored as plain text and instead are hashed using SHA512 (from CathexisVision 2017).
3. Login credentials are negotiated using Diffie-Hellmann key exchange and signed with an RSA private key (supports 1024 and 2048 RSA keys).
4. Encryption on network channels is performed using AES128/GCM with unique cipher keys negotiated per connection.
5. HMAC is used for integrity verification.
6. Public Key Infrastructure (PKI) is managed internally by Cathexis for added security.

Archiving

1. The integrity of the videos is secured using dual RSA1024 keys (for signing).
2. Optional encryption is performed using AES128 block encryption with a randomised IV per block and a user-generated pass-phrase.
3. Video can be watermarked to indicate the source of the information (i.e. user info)
4. The video footage and metadata can only be played via a proprietary Cathexis Archive Video Player.
5. Exported/archived video may be restricted to password-controlled playback.

Further information on CathexisVision archive security can be found in Appendix 2: Cathexis Security.

4.5.5 System and third-party security

Peripheral equipment

Cathexis works with technology partners and other industry players to increase the security of the products and protocols to which CathexisVision connects. In general, connection with IP cameras includes the following:

Camera configuration	• HTTP: hypertext protocol • Encryped ssl/tls • Supported by CURL (client-side URL transfer library).
Camera control	• RTSP – real time streaming protocol. • HTTPS encrypted camera connection control (where supported by the manufacturer).
Video streaming	• RTP – real time transport protocol. • Encrypted video streaming (where supported by the manufacturer).

IT considerations

Network access: the first step in any system is to ensure that access to the network is properly controlled. There are various techniques for this, which should be adopted by any networking company. These include firewalls, Intelligent Network Switches, Managed networks, and controlling "physical" access to the network.

Operating System lockdown: in order to attack software, access must be gained through the operating system on the system on which the software is running. It is important to ensure that the OS is "locked down" to prevent unauthorised access. This can be done in several ways, including:

- Preventing the opening of unauthorised ports enabling use of items such as ftp, telnet, email. If any communication needs to occur via these means, then one needs to ensure that security protocols like SSH/SFTP are utilised
- Disabling "root" access to the OS
- Ensuring strong password levels
- Adding anti-virus and anti-malware software, which is continuously updated
- Restricted internet access.

5. Conclusion

If an organisation installs a CCTV system, it needs to carry out a **Personal Information Impact Assessment**, which would identify and document the impact the installation would have on the privacy rights of data subjects or individuals affected. The organisation also needs to review whether CCTV is the **best security solution** in the context of those rights.

The organisation needs to **nominate** someone within it to be responsible for the operation of the CCTV system, and to draw up a **policy** covering the use of the system, including the relevant POPI-required procedures. **Staff training** needs to be carried out to educate staff on how to operate the CCTV system and deal with requests for footage.

Procedures need to be in place to respond timeously to **data subject access requests** to view the CCTV footage. The footage must only be **retained** for the necessary amount of time. What constitutes a "**necessary**" period of time needs to be set out and pre-defined within the policy concerning the use of the footage. The footage needs to be clear and of a high quality, and stored **securely**. Only **authorised** individuals should have access to the footage. To comply with the terms of fair processing and transparency, the organisation must **inform** individuals of its use of CCTV.

5.1 Useful links

- The POPIA website.
- A guide to POPI Act compliance.

Appendix 1: Documents

Data Subject Access Request

✓ The information requested must be disclosed to the data subject securely and in an accessible, concise, intelligible format.

For example, if the DSAR was made electronically, the operator should provide the requested data in a commonly used electronic format. It is good practice to establish which format the data subject would prefer before fulfilling the subject access request. It is possible to provide other options, such as the data subject accessing their information remotely and downloading the copy themselves. In the case of a verbal request, a verbal response may be given if the identity of the individual can be assured. It is essential to keep a record of this interaction – the date of the request, the date of the response, and the details of the individual and information given to them.

Privacy Notice

FIRST LAYER OF INFORMATION

The Privacy Notice is the primary way that an operator will communicate to the data subject that they are being filmed.

- It is advisable to use a **symbol or icon** as part of the warning sign, which conveys the fact of the filming to all potential data subjects.
- The warning sign information should be **positioned** while data subjects are still merely *potential* data subjects in that they can recognise where the filming is about to commence and as such make the decision as to whether to enter the monitored areas before they have entered it. Eye-level positioning of the sign is advisable.
- In order for a data subject to be able to avoid surveillance if they wish, there must be absolute clarity on the extent of the demarcated **area** being surveilled. However, it is not crucial for the data subject to know the actual positions of specific cameras or surveillance equipment.
- As the first layer of communication with the data subject, the warning sign must contain all of the most relevant **content** regarding the data collection, such as the purposes of filming or processing, the operator's identity, the data subject's rights, and the largest impacts of the processing.
- For example, the warning sign could include the legitimate interests of the operator or a third party as well as the Information Officer's contact details, and, crucially, should refer to where the second layer of information can be found.

- In addition, if there is something **unusual** or which could be reasonably surprising to a data subject, this should also be included in the warning sign, such as information regarding the storage period or the transmission of the data to third parties outside of the EU. Without such information, the data subject should be able to assume that the filming is merely a live monitoring, with no recording or transmission occurring.
- It is advisable for the first layer information to refer to a **digital** source for the second layer information, such as a website or QR-code. However, such information must also be available in a non-digital format.

SECOND LAYER OF INFORMATION

- This information must be made easily **accessible** to the data subject – for example, as a "complete information sheet available at a central location (e.g. information desk, reception or cashier)".
- The data subject must be able to access the second layer of information **without entering** the monitored or surveyed area, possibly by way of a phone number or link.

Appendix 2: Cathexis Security

Archive Security

In addition to the existing login configuration options for up to 30 user types, Lightweight Directory Access Protocol (LDAP) and Windows Active Directory for enterprise level are supported. This allows for the standardisation and control of access within a customer's existing network management framework. For increased security and accountability, users can be assigned to archive profiles for which default watermarks and password protection may be set according to the user levels. Archives can be watermarked to determine the archiving user, and password protected to restrict access to archive review to desired user levels only.

Watermarks: Site users are assigned to archive profiles according to their access levels. Administrators can assign watermarks to archive profiles. When a site user performs an archive and their archive profile has had a watermark configured, the archive is watermarked by default. On review, the archive watermark will be displayed from top left to bottom right.

Password protection: Archives with password protection require the correct password to be entered in order to review. The addition of password protection to an archive can be forced in the creation of a profile. On the creation of an archive, the user has the ability, from within the selected profile, to add password protection. There are 3 password options available to the user – Custom, Fixed and Random. Multiple password options can be assigned to archive profiles. Password requirements will have to be met by all users wishing to review the archive in the CathexisVision Archive Viewer. Lost passwords are not recoverable and the archive will need to be recreated.

Signing: Archives retain an overall archive signature linking them to the source NVR. Additionally, critical portions of audio/video are independently signed and can be explicitly linked to the archiving NVR. Sub-archives (archive of already archived footage) do not contain any signatures generated by the original NVR that sourced the video data. The authenticity of these archives cannot be determined.

Verification: The verification feature produces a report on the authenticity of an archive. An archive verification report will determine whether or not the archive signature is valid and indicate whether the archive is or is not verified according to this information. Because sub-archives (archive of already archived footage) do not contain any signatures generated by the original NVR that sourced the video data, sub-archives will *fail* the verification as their authenticity cannot be determined.

Auditing: Audit logging of the archive client on each NVR sourcing data for an archive is included.

Encrypted Archive Files: CathexisVision uses AES 128 encryption and RSA 256 signing for all archives. Only the CathexisVision Archive Player can review CathexisVision Archive files.

Privacy Policy – website

Cathexis is committed to protecting your privacy. By accessing the website, users accept and agree to the terms of this Privacy Policy. "Cathexis" refers to Cathexis Technologies (Pty Ltd), Cathexis Africa (Pty Ltd), and all of their direct and indirect subsidiaries.

When Visiting the Cathexis website: you may be required to provide personally identifiable information. Alternatively, you may elect to not provide Cathexis with personal data. The personal information you provide may include your name, company, job title, address, e-mail address, your business, profession, and product preferences. Cathexis's web servers may automatically collect website usage information from you. Website usage information informs Cathexis about how visitors and subscribers use and navigate the websites. This includes the number and frequency of users to each page, their IP addresses, and the length of their stays.

Personal data: Cathexis will not collect any personal information about you through our website, or any other means, unless you have given your consent or provided it to us of your own volition. You have the option to give your consent when registering on our website. User data is captured on registration and users have access to their information.

Use of information collected: The personal information collected on the website will be used to operate the website and to provide the services, or carry out the transactions, you have requested. Cathexis may combine the information you have provided with other accessible information about you, including website usage information and information from other sources. Cathexis may use this information to process, validate, and verify requests for products and services. Your personal data may also be used for the purposes for which you specifically provided the information; to enhance your experience of the website; to improve and develop new products, features and services; to alert you to new products, services, and special offers; to provide marketing with aggregate information about the user base and usage patterns; and to allow Cathexis to personalise advertising for users based on their personal characteristics or preferences.

Information for our newsletters and sales force: Users have the option to agree to this upon registering on our website, and have the option to opt out.

Do we share your personal data with our partners? No.

Information required for legitimate purposes: Cathexis may disclose any information about you to law enforcement agencies, government officials, or other authorities, as Cathexis, in its sole discretion, believes necessary or appropriate in the circumstances.

Retention policy: There is no expiration to the retention of your personal data. Cathexis reserves the right to retain your data for the purposes outlined in this Privacy Policy as permitted by law.

Cookies: Cathexis automatically collects information and data through the use of cookies. A cookie is a small text file that is placed on your hard disk by a web page server, which enables a website to recognise repeat users, facilitate the user's ongoing access to, and use, of the website, and allows a website to track usage behaviour and compile aggregate data that will allow content improvements and targeted advertising. A cookie will not provide Cathexis with personal information. If you have not supplied Cathexis with any personal information, you can still browse the website anonymously. You have the ability to accept or decline cookies, and you can modify your browser settings to decline them. If you choose to decline cookies, you may not be able to fully experience the interactive features of the Cathexis website or other websites you visit.

How we ensure the security of your data: The personal data we collect about you is stored in limited access servers. Cathexis maintains safeguards to protect the security, integrity, and privacy of these servers and your data. In particular, SSL and Cloudflare protect you against information theft.

IP address: the IP address will be automatically collected and logged as part of the connection of your computer to Cathexis's web server and may be used to determine the total number of visits to each part of the website. If there is a security breach, the relevant IP Address will be identified by the Internet Service Provider and the user may be contacted.

Using our mobile application: Cathexis does not collect any personally identifiable information from clients who use our mobile application. We do send anonymous crash reports that include, among other data, the type of mobile device you are using and your operating system. These crash reports are only sent with your consent.

Video management system (VMS): The CathexisVision VMS does not collect any personally-identifiable data. In keeping with the Cathexis ethos, our VMS prioritises your privacy, safe-guarding the sensitive data and information of our clients.

Links to other websites: external links are not subject to this Privacy Policy. Cathexis recommends that you review the privacy policy of each website to determine how it impacts you.

Policy updates: Cathexis may amend this Privacy Policy from time to time, and will post any changes. Notwithstanding the right to amend the Privacy Policy, Cathexis will not use your personal information in a manner materially different from this Privacy Policy without your prior consent.

Comments and questions: If you have any questions regarding our privacy policy or data collection process, want to withdraw consent, or edit your details, please fill in the Contact Us form. Cathexis reserves the right to contact you at any time regarding problems or questions. Cathexis may also notify you of changes to the Privacy Policy, or to other policies or terms that affect you, but it is not obliged to do so.

This Privacy Policy is subject to the terms and conditions of use of the Cathexis website.