GUIDE ON

RESPONSIBLE USE OF BIOMETRIC DATA IN SECURITY APPLICATIONS

SG:DIGITAL

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SAS SECURITY ASSOCIATION SINGAPORE

CONTENTS

INTRODUCTION

INTRODUCTION

With the advancement in technology, more sensors that collect biometric data are being used and deployed in commercial security applications, such as security cameras or Closed-Circuit Television Cameras (CCTVs) for security monitoring and facial or fingerprint recognition systems for ingress to and egress from premises. This Guide is targeted primarily at such security applications that use biometric data.

Recently, the Personal Data Protection Commission (PDPC) has observed more incidents involving the mishandling of such data. As such, this Guide is intended to help organisations, such as Management Corporation Strata Titles (MCSTs), building or premise owners and security services companies, to use security cameras and biometric recognition systems responsibly and safeguard individuals' biometric data where it is collected, used or disclosed. This Guide covers the following:

Part I	Defining key terminology used in this Guide
Part II	Key considerations in implementing security cameras and biometric recognition systems, and industry best practices for data protection
Part III	Obligations and exceptions under the Personal Data Protection Act (PDPA) applicable to the collection, use and processing of biometric data
Annexes	Practical guidance on security cameras for security monitoring and biometric recognition for access control

This Guide is not intended for individuals who use security cameras or biometric systems in personal or domestic capacities[1]. Examples of such activities include the use, by individuals, of home webcams to monitor the safety of elderly household members, biometric locks for residential premises, and facial or fingerprint sensors in mobile or other personal computing devices.

Biometric technology and the use of biometric data are expected to grow. It is not advisable to lay down broad principles in anticipation of real-world applications and issues that will emerge. This Guide is not intended to address organisations' use of biometric data for commercial purposes other than in security applications. Future guidance will be provided for the separate and distinct considerations that apply in relation to other commercial use cases.

This Guide may be read in conjunction with the *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* and the section on CCTVs under *Chapter 4: Photography, Video and Audio Recordings in the Advisory Guidelines on the Personal Data Protection Acts for Selected Topics*.

[1] For more information, please refer to *Chapter 6: Organisations in PDPC's Advisory Guidelines on Key Concepts in the Personal Data Protection Act*.

PART I: DEFINING KEY TERMINOLOGY USED IN THIS GUIDE

WHAT IS BIOMETRIC DATA?

Biometric data refers to biometric samples[2] (i.e. data relating to the physiological, biological or behavioural characteristics of an individual) or biometric templates created through technical processing of biometric samples. Examples of biometric samples include facial images, fingerprints and voice recordings. **Biometric samples** are captured through sensors such as image and audio sensors.

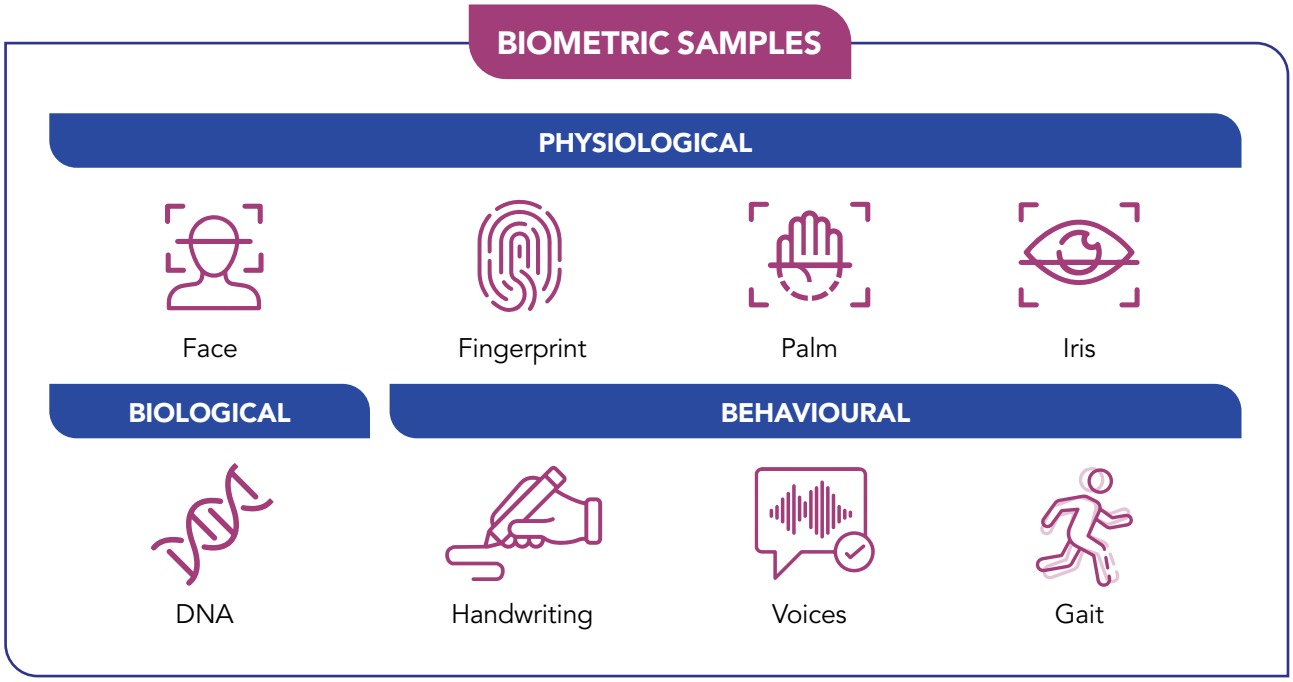


Figure 1. *Illustrations of biometric samples*

Biometric samples captured by sensors may be processed to create **biometric templates** that are used by application systems. For example, employees' facial images or fingerprints are processed to provide biometric templates that are used in office security systems to control access to the office premises.

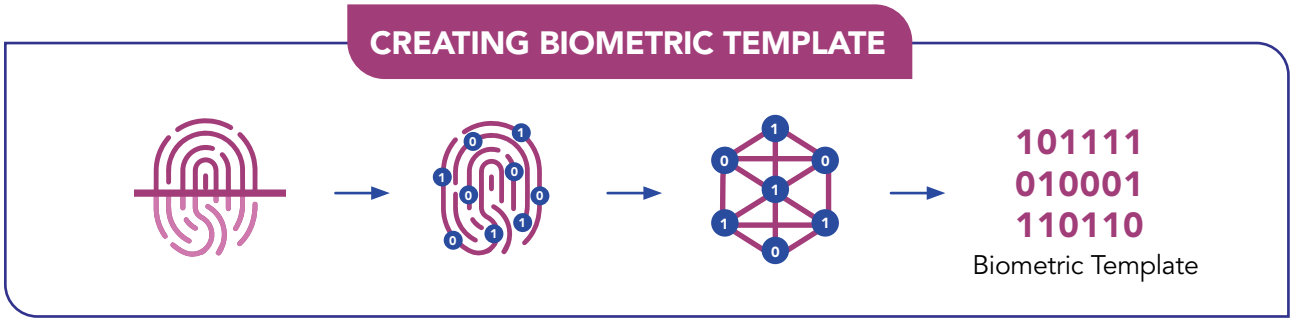
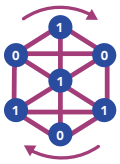


Figure 2. *Transforming a biometric sample (e.g. fingerprint) into a biometric template*

[2] Referenced to *International Organization for Standardization (ISO)'s* definition of biometric data.

Biometric data (i.e. biometric samples and/or biometric templates) when associated with other information about an individual will form part of the personal data of that individual. Examples include the facial image of an employee in the Human Resource Management System (HRMS) and the biometric template of the employee's face used in access control systems for entry into office premises.

Biometric templates (on their own, without associating with any identifying information) are considered anonymised data, as they are binary representations derived from the application of algorithm to biometric samples. Under the PDPA, measures and safeguards are still required to be applied to anonymised data[3] where there could be a possibility that an individual can be re-identified from the anonymised data.



HOW IS A BIOMETRIC SAMPLE TYPICALLY PROCESSED?

During the technical processing of a biometric sample, a digital representation of its features or characteristics is extracted by an algorithm in the biometric system and processed into a biometric template. Typically, for biometric access control solutions, the biometric sample of an individual is first enrolled into the system. The enrolled biometric sample is then processed into a template that is stored and subsequently used for matching against the presented biometric sample (see *Figure 3*).

Biometric data can be used for verification or identification of an individual.

A Verification

An individual presents his or her proof of identity (e.g. passport) and a sensor captures his or her biometric sample (e.g. face or fingerprint). This allows the system to generate a biometric template to match against the enrolled template (refer to *Figure 3* for terminology) of the claimed individual stored in the system (also known as 1:1 matching). Verification is used by some banks to register customers for new accounts. Proof of identity, such as a National Registration Identity Card (NRIC) card number, is entered by the customers as the first level of identity claim. A photograph of the customer's face is then taken and submitted to the system to generate a biometric template. Next, this biometric template is matched against the biometric template of the customer that is retrieved from the Singapore's National Digital Identity (Singpass) database to verify the identity claim.

[3] Refer to *Chapter 3: Anonymisation in Advisory Guidelines for Selected Topics* for more information on anonymisation and *Guide to Basic Anonymisation* for managing re-identification and disclosure risks.

B Identification

An individual does not need to present proof of identity and instead only needs to present his or her relevant biometric sample (e.g. the individual's face) to the system to be processed and matched against templates stored in the database (also known as 1:n matching). A common example is the biometric access control system for entry to premises or buildings for employees. After employees' biometric templates have been stored in the access control system, each time an employee appears at the gantry, the camera captures the employee's facial image, generates a biometric template and matches it against one of the templates stored in its database. Entry is granted once there is a match.

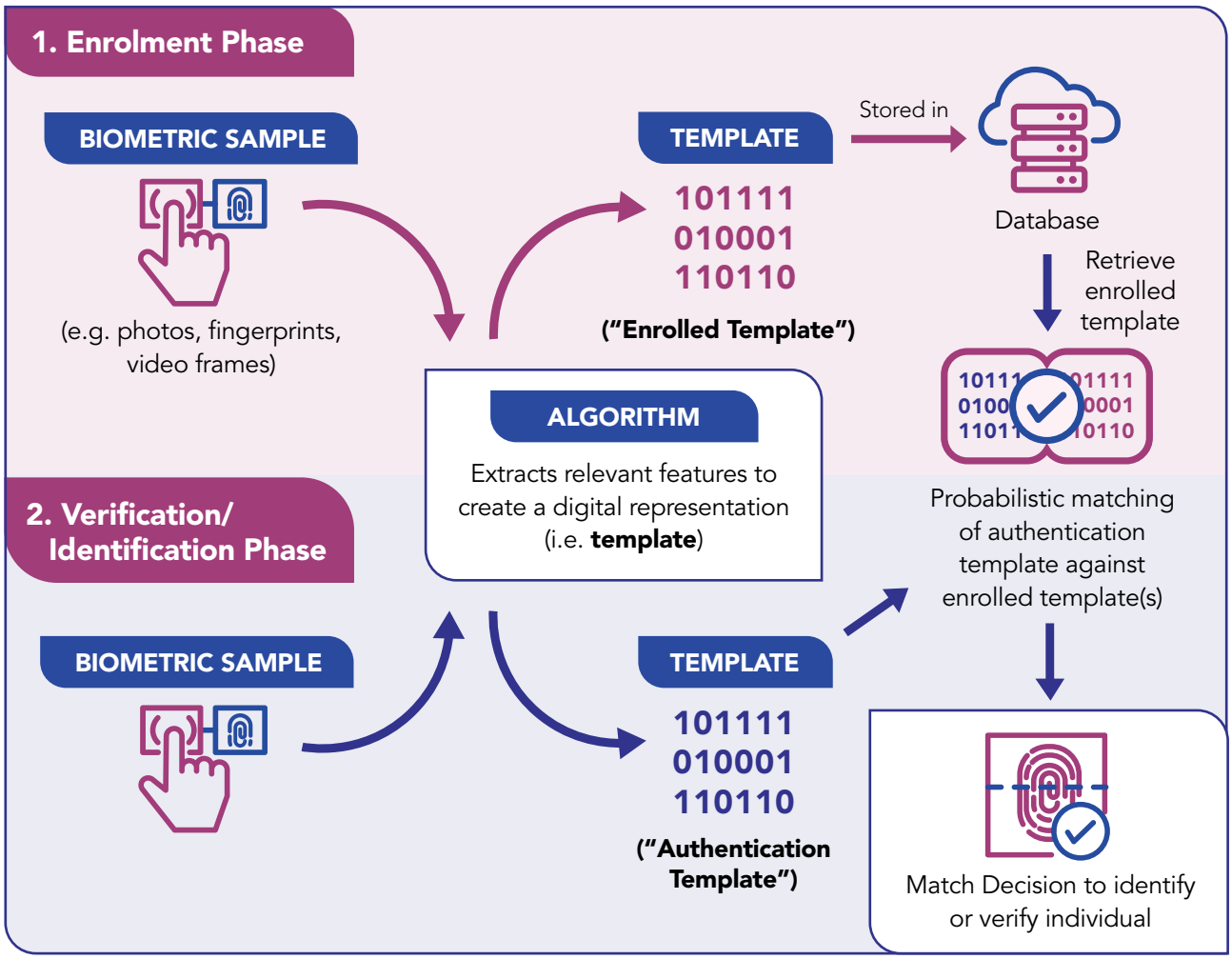


Figure 3. *Illustration of how a biometric sample is processed for verification or identification*

PART II: WHAT ARE THE BEST PRACTICES TO COLLECT, USE AND DISCLOSE BIOMETRIC DATA RESPONSIBLY?

ADDRESSING RISKS UNIQUE TO BIOMETRIC RECOGNITION TECHNOLOGY

Biometric data are generally considered to be immutable, as they cannot usually be changed. This unique characteristic gives rise to some risks. Therefore, it is important to be familiar with what some of these risks are when using biometric data, as well as how systems and processes can be designed to address them. These are recommendations that organisations can consider when they procure or design biometric recognition systems for security applications.

A Identity Spoofing

- **What it is:** Identity spoofing refers to the use of a synthetic object (e.g. synthetic fingerprint, 3D model of a face) to fake the physical characteristics of an enrolled individual in order to obtain a positive match in the biometric system.
- **What organisations can do:**
  - Organisations are encouraged to implement anti-spoofing[4] measures, such as liveness detection, within the system.
  - Situating facial recognition access control points beside a manned security post or regular surveillance by stationing a security officer at the access point can also be considered as a precaution to detect and discourage spoofing attempts.
  - Ensuring end-to-end system integrity with encryption of data-at-rest and data-in-transit will prevent any possible tampering or man-in-the-middle attacks.

B Error in Identification

- **What it is:** As biometric systems rely on probabilistic matching, there is the possibility of a failure to identify an enrolled individual (i.e. false negative) when the threshold for matching is set too high, or wrongly identifying another person as the enrolled individual (i.e. false positive) when the threshold is set too low.

[4] Organisations may wish to refer to industry standards, such as "ISO 30107 - Biometric presentation attack detection" for technical details.

- **What organisations can do:**
  - Organisations are advised to consider how their use cases are affected by false positives or false negatives, in order to set a matching threshold that is reasonable and commensurate with the impact of misidentification. Reasonableness of the threshold will take reference from any relevant industry standard or practice. For example, a higher matching threshold may be necessary for entry into data centres.
  - If organisations require a higher identity assurance or are unable to configure higher matching thresholds, they may wish to supplement biometric data with additional factors of authentication (e.g. requiring access card in addition to biometrics for the verification of an individual).

C Systemic Risks to Biometric Templates

- **What it is:** Generally, a biometric template is unique to the algorithm that is used to generate it. However, the uniqueness of the template declines if the same algorithm is used across several different implementations. This can foreseeably happen if a service provider deploys a common solution across multiple customers. Hence, it is plausible for an adversary to enrol compromised biometric templates into the database of systems that use the same algorithm to gain entry into services or premises.
- **What organisations can do:** Generally, encrypting the biometric template in the database would provide basic protection against such risks. Introducing a salt when encrypting biometric templates can further reduce such risks. Whenever practicable, encryption of biometric templates is recommended as a good practice. Organisations with high security requirements may wish to use customised algorithms.

MEASURES TO GOVERN AND PROTECT BIOMETRIC DATA ACROSS THE BIOMETRIC DATA LIFE CYCLE

Organisations should also consider implementing governance controls and data protection best practices throughout the different stages of the biometric data life cycle to reduce impact on affected individuals in the event of a breach. Periodic audits should be conducted to ensure compliance to their established controls and practices to ensure that these have not eroded over time.

The following table summarises some of the measures that organisations can consider adopting where applicable. The application of these practices will also be illustrated through two common security use cases in Annexes A and B.

Data Collection	**For security cameras:** • Provide proper notification to individuals and ensure appropriate placements of the cameras. **For biometric recognition systems:** • Obtain consent from individuals for collection of biometric data unless an exception applies. • Ensure the system is protected from tampering or man-in-the-middle attacks.
Processing / Use	**For security cameras:** • Limit access to the biometric sample (e.g. video recordings of identifiable individuals). **For biometric recognition systems:** • Where possible, process biometric samples to biometric templates as soon as practicable, and use only the biometric template for recognition. Example: Use only the biometric template to perform recognition of ticket holders for re-entry to places of interest, without identifying the individuals. • Prevent decrypted biometric templates from persisting in the system by carrying out matching processes for biometric templates in temporary storage (e.g. Virtual memory or Random-Access Memory[5]).
Storage	**For security cameras:** • Manage access to the storage databases. **For biometric recognition systems:** • Where possible, minimise the personal data stored in the system by storing only the biometric templates and discarding the biometric samples as soon as practicable. Example: The enrolment process for a facial recognition system may entail collecting a profile photo from visitors. Organisations are encouraged to process the photos into biometric templates as soon as possible and discard the photos from storage.

[5] Random-Access Memory (RAM) is a volatile memory that temporarily stores the data being worked on.

Storage	• Prevent the linking of biometric templates to identifying information of individuals by adopting the following measures where relevant:
	  ○ As good practice, encrypt biometric templates and link the data only to Universally Unique Identifiers (UUIDs) or hashes of identifiers. For additional safeguards of access to sensitive applications, consider using different encryption keys for the biometric templates used by the different applications.
	  ○ Where technically feasible, consider segregating the storage of different types of data. For example, biometric data with links to UUIDs should be stored in a database different from the mapping table of UUID or hashes to individual identifiers or records.
	• Implement relevant safeguards to protect the database:
	  ○ Encrypt the biometric templates and samples (good practice).
	  ○ Introduce a salt when encrypting (good practice).
	  ○ Implement a strong key management system to protect encryption and decryption keys.
	  ○ Implement access control measures and logs to prevent unauthorised access, and assign access rights for each database.

Disposal	• When biometric data (i.e. biometric samples and templates) are no longer required, ensure that the corresponding entries are permanently deleted from the system. Example: When staff leave the organisation, merely revoking their access in the facial recognition system is insufficient. The biometric samples and templates should be permanently deleted from the system too. • When the system storing the biometric samples and templates is decommissioned, use appropriate means to ensure that the data is permanently deleted or destroyed. Example: Perform physical disposal of hard disks or other known methods of destruction of storage media (e.g. degaussing and incinerating) when secure erasure of personal data stored on the electronic media is not possible.

PART III: HOW DO THE PDPA OBLIGATIONS APPLY TO BIOMETRIC DATA?

This section will address how the PDPA obligations may apply specifically for biometric data in security applications.

COLLECTION, USE AND DISCLOSURE OF BIOMETRIC DATA

Generally, organisations may collect, use or disclose personal data for legitimate purposes recognised by the PDPA, or where an individual gives, or is deemed to have given consent for the notified purposes. The following discusses some of these purposes.

Controlling access to a service or a premise

a. When an individual enrols for a service or access to a premise (e.g. physical access to a facility or authentication to mobile banking services), and provides his or her biometric sample for authentication purposes, consent may be obtained, or may be deemed to have been given, as part of the enrolment process for the service or access.

b. Employers may rely on the employment exception where the collection, use or disclosure of the employee's biometric sample is reasonable for the purpose of managing the employment relationship for consistent purposes.[6] Biometric access control of staff entry into the office premises is an example of a legitimate purpose within the employment relationship. Employers should nevertheless notify employees on how their biometric data will be used (e.g. employee contracts, employee handbooks or corporate intranet).

Maintaining a safe working environment

c. Apart from controlling employee access to premises, employers may also rely on the employment exception to use surveillance cameras for monitoring and enforcing workplace safety requirements in order to provide a safe working environment for employees.

[6] Organisations can refer to *Chapter 5: Employment in the Advisory Guidelines on the PDPA for Selected Topics* for more information on the employment exception.

Example: Safe Distancing at Construction Worksite

Construction worksite MNO is required to deploy safe management measures such as safe distancing at the worksite. MNO deploys a safe distancing solution integrated with a security camera system that will alert the safe distancing officer with a screenshot of incidents in which employees fail to maintain safe distancing. The security cameras are deployed at locations of the worksite where employees tend to congregate.

MNO is likely to be collecting personal data because an image of an identifiable individual captured in photographs or video recordings is personal data about that individual. MNO assesses that the purpose for collection of personal data in this circumstance is reasonable for managing the employment relationship. MNO relies on the employment exception to collect employees' personal data instead of seeking consent from employees. As MNO is still required to provide notification to its employees, it mentions that facial images in photographs may be captured for the purpose of ensuring safe distancing at the worksite in the employee handbook.

Security monitoring of a premise and investigations

d. The deployment of security cameras for monitoring and ensuring the safety of premises is a legitimate purpose. Organisations may consider relying on one of the exceptions to consent[7] provided in the PDPA (as illustrated in the following section).

i. Publicly Available Data	
When can an organisation rely on this?	This applies to the collection of biometric samples in locations that are open to the public or where individuals can be observed by reasonably expected means, such as through security cameras and body-worn cameras.
What does it allow?	It allows the collection, use and disclosure of biometric data without consent for security purposes (e.g. monitoring or investigations).
What is required?	It is good practice to put up notices disclosing that the area is under surveillance and whether recording also takes place.

[7] Organisations should refer to the *Advisory Guidelines on Key Concepts in the PDPA* for details on how to apply these exceptions. In addition, for the purposes of contact tracing and other response measures, organisations may refer to the *Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry.*

Example: Use of Security Cameras in Spaces Generally Accessible to the Public

Supermarket STU has encountered a few cases of shoplifting along the snack aisle. The management of Supermarket STU has decided to install security cameras to monitor the aisle. To prevent shoplifters from identifying blind spots, the cameras are discreetly placed.

As the cameras are monitoring an area available to the public, Supermarket STU can rely on the publicly available data exception and does not need to seek consent from its shoppers. However, to provide shoppers with sufficient notification of the security cameras, Supermarket STU placed notices at eye-level stating that security cameras are in operation. In this instance, the notices need not indicate the specific camera locations.

ii. Legitimate Interests	
When can an organisation rely on this?	When the legitimate interests of the organisation or another person in the security use cases outweigh any likely adverse effect on the individual.
What does it allow?	It allows the collection, use or disclosure of personal data without consent. An example of such a use case could be the sharing of images or footage relating to illegal or suspicious activities of perpetrators or suspected perpetrators between organisations in the same industry; this is done for the purpose of improving surveillance and monitoring to safeguard the safety of their assets, businesses, patrons or tenants.
What is required?	The organisation needs to conduct a legitimate interests assessment to: a. Identify any adverse effect that the collection, use or disclosure of personal data is likely to have on the individual; and b. Identify and implement reasonable measures to eliminate the adverse effect, reduce the likelihood that the adverse effect will occur or mitigate the adverse effect. The organisation will need to disclose reliance on the legitimate interests exception through any means that is reasonably effective (e.g. disclosure as part of the organisation's public data protection policy). A pre-filled sample template for using the legitimate interests exception for security facial recognition system is attached in Annex C.

Example: Installing Security Cameras in Areas Not Open to the Public

Events organiser EVT wishes to install security cameras at storage areas and corridors on its premises which are not open to the public, but are accessible to third party retailers who are renting exhibition booths and their suppliers. The purpose of the security cameras would be to monitor the premises as a deterrent against theft. EVT will also be placing prominent notices below each security camera to provide sufficient notification that security cameras are in operation.

Under these circumstances, EVT may consider relying on the legitimate interests exception to consent (subject to EVT satisfying the necessary requirements), in place of seeking consent from every individual who has access to the areas which are not open to the public.

Example: Use of Security Facial Recognition System

Shopping mall SHM has encountered a few cases of fights and illegal gatherings at a more secluded area within its premises. The management of SHM has decided to install a security facial recognition system with Artificial Intelligence (AI) to monitor the premise for any anomalous behaviour within its premises (e.g. fighting, gatherings or other unusual behaviour). The system will collect and analyse biometric samples (e.g. facial images and behaviour) of individuals within its premises to identify potential anomalies. Footage of suspected anomalies will be sent to its Security Department for further investigation and intervention.

Under such circumstances, Shopping Mall SHM need not seek consent from its shoppers by relying on the legitimate interests exception to consent (subject to SHM satisfying the necessary requirements). However, to provide shoppers with sufficient awareness of the security cameras, SHM placed notices at eye-level stating that security cameras are in operation. In this instance, the notices need not indicate the specific camera locations.

Enhancing security operational efficiency for a premise

e. Organisations that have deployed security cameras may make use of past security footage or data when they review their security plans and improve the efficiency of their security operations.

iii. Business Improvement	
When can an organisation rely on this?	Where the use of the data allows the organisation to improve its crowd management and security operations as part of its business or service offerings. Examples: • Use of past security footage to review the adequacy of existing security arrangements and enhance the efficiencies of security operations (e.g. security patrol routes, camera blind spots). • Use of past security footage and extracting biometric samples of customers to develop or enhance effectiveness of fraud and security monitoring tools (e.g. improve accuracy for detecting suspicious behaviour or movement patterns of customers). • Use of biometric templates to develop or enhance effectiveness of cyber security monitoring tools (e.g. improve accuracy for detecting suspicious usage patterns).
What does it allow?	It allows the use of personal data without consent.
What is required?	The organisation needs to ascertain that its purpose cannot be reasonably achieved without having the personal data in individually identifiable form.

Example: Use of Camera Footage to Improve Security Officers' Patrol Routes and Operations

Shopping mall VWX intends to analyse its customers' data captured in security camera footages to derive insights on the footfall during different times of the day. It is doing so to ensure that its outsourced security service company deploys sufficient security officers to the respective buildings and optimises the officers' patrol routes within the buildings. It contracted its security service company to process movement of individuals through biometric recognition technology to monitor individuals' movements within the buildings. This is to provide a better understanding of footfall, etc. to improve its security planning, patrol routes and security operations.

VWX assesses that the use of personal data is necessary for its purpose as there are no other alternative data that can be used to provide the same insights. It may rely on the business improvement exception to use its customers' data captured in security camera footage without consent to derive insights on footfall for its purpose. Once processing is completed, VWX should ensure that its outsourced security service company discards the raw images and only retains the insights from the biometric analytics.

Example: Use of Biometric Data to Train Artificial Intelligence (AI) System for Better Detection of Anomalous Behaviour

Shop XYZ encountered a series of shoplifting incidents. As such, XYZ has deployed an AI system to help its security officers with early detection of anomalous behaviour and potential shoplifters.

To develop and customise the AI system for XYZ, the vendor requires the behavioural data (i.e. biometric samples) from past shoplifting incidents. The vendor will also perform maintenance for XYZ on a regular basis by training its AI system using data from recent shoplifting incidents. XYZ assesses that the use of personal data is necessary for the development and training of the AI system to improve security operations. It may rely on the business improvement exception to use biometric data without consent.

When deploying AI systems, XYZ could also adhere to the processes, practices and measures described in PDPC's Model AI Governance Framework (**"Framework"**), especially the Operations Management section that deals with data and model quality and bias. Since XYZ relies on a vendor for its AI systems, it could require its vendor to adhere to the Model Framework through its contract, and put in place a system for periodic review. Examples from the Model Framework include ensuring datasets used for training the AI model are adequate for the intended purpose, minimising the data that are required for model development and testing (e.g. blurring faces), using technical tools to detect bias, and monitoring and reporting on model performance after deployment.

Once development and/or training is completed, XYZ should ensure that its outsourced vendor discards the biometric samples securely and that the vendor will not attempt to re-identify individuals from the training data.

SECURING BIOMETRIC DATA

The integrity of a biometric system rests on the completeness of the security arrangements that are implemented. While technical considerations play a major role in protecting biometric data, non-technical processes like managing access to biometric data are equally important. Organisations should refer to **Part II** for a list of recommended measures across the biometric data lifecycle.

DISPOSING BIOMETRIC DATA

An important aspect of information security is the disposal of information at the end of its life cycle. Biometric data should not be retained once the purpose of its collection is fulfilled and there is no business or legal requirement for its continued retention.

Organisations may wish to consider any precedents or situations that may require access to such recordings and data to decide on an appropriate retention period. **Part II** of this Guide includes some best practices to dispose data once an organisation no longer has a reasonable purpose to retain the data.

ACCESS TO AND CORRECTION OF BIOMETRIC DATA

Individuals may request access to biometric samples (e.g. facial images) collected by the organisation. For clarity, organisations need not accede to a request for access to the individuals' biometric template as biometric templates are considered confidential commercial information that, if disclosed, will compromise the effectiveness and integrity of the security application. Further, such a request would also be considered frivolous since the data are not reasonably usable by the individual for any purpose outside of the organisations' own biometric recognition system.

For such requests, an organisation is required to provide access to the biometric samples captured of the individual as soon as reasonably possible, unless the request falls within one of the prohibitions under section 21(4) or an exception in the Fifth Schedule to the PDPA. The organisation also has an obligation to allow an individual to request a correction of errors or omissions in the individual's personal data.

Security camera footages containing personal data are often the subject of data access requests and may include third-party individuals. The publicly available data exception[8] would apply in relation to security camera footages captured of areas open to the public, and such footage can be provided without masking the personal data of third-party individuals. Nevertheless, organisations should restrict the data shared to what is necessary to achieve the objective of the access request by an individual. Annex A will provide some practical tips to organisations on how to respond to an access request for video footage.

When relying on the legitimate interests exception, or any other applicable exceptions for disclosure without consent to provide access to security camera footage recorded at private premises, such as a private club, the personal data of third-party individuals need not be masked (refer to the chapter on CCTVs in PDPC's *Advisory Guidelines on the Personal Data Protection Act for Selected Topics)*. If none of the exceptions are applicable, consent will need to be sought.

[8] *Chapter 4: Photography, Video and Audio Recordings in the Advisory Guidelines on the Personal Data Protection Act for Selected Topics* has a section on CCTVs which contains a few examples illustrating the publicly available data exception for data access requests.

The organisation has the option to charge the individual a reasonable fee to recover any incremental costs of responding to the access request. It must give the individual a written estimate of the fee, and the organisation may refuse to provide access to the individual's request until the individual agrees to pay the relevant fee[9].

More information on how to handle access requests can be found in chapter 15 of the *Advisory Guidelines for Key Concepts in the PDPA*, including handling requests from criminal and civil discovery avenues by third parties.

ACCOUNTABILITY AND INTERNAL GOVERNANCE

Organisations should establish a robust Data Protection Management Programme which sets out an organisation's management policies, application of processes and practices, as well as roles and responsibilities of staff in the handling of biometric data. Only decision-making and management of vendors are described here. For more information, please refer to PDPC's *Guide to Developing a Data Protection Management Programme.*

A *Design of Systems and Processes*

It is important that the appropriate levels of decision makers are involved in an organisation's decision and implementation journey. Organisations deciding on the type of biometric sensor or system to adopt may wish to consider the following:

i. Determine the purpose, requirements and alternatives

Before embarking on the implementation of a biometric recognition system, organisations should consider the purpose of implementation, what data they would need to collect and whether the purpose will be addressed by the installation of such a system or would there be alternative solutions or designs of the system that can meet their business purposes without the need to collect biometric data. For example, organisations should also consider leveraging in-built biometric processing capabilities on a mobile phone or the Government's National Digital Identity (NDI) services for biometric authentication, instead of collecting or storing individuals' fingerprints or biometric data centrally.

[9] For more information on handling access requests, please refer to the PDPC's *Guide to Handling Access Requests.*

ii. Collection of data to fulfil the business objective

Organisations are encouraged to consider whether it is possible to use biometric technology to address their business needs while minimising the collection of personal data. For instance, if the business need is to understand customers' browsing behaviours so as to improve product placements and layout, the organisation may decide to integrate facial recognition technology with its security camera system to capture profiles (e.g. age group, gender and ethnicity) and track footfall of its consumers. However, the organisation need not store the facial images. Instead, it can store only non-personal data like anonymised profiles and derived insights, which are the datasets needed for analysis of service improvements.

iii. Perception of individual's privacy intrusion differs across biometric data types

As facial recognition technologies are more widespread relative to iris scans, individuals are likely to be more receptive to having their facial images collected and used for common security applications such as access control for a building. Conversely, individuals may regard iris scans for the same purpose to be more intrusive. As such, organisations may wish to consider such privacy intrusion perception when selecting the type of biometric samples to collect for their security use cases.

iv. Context and frequency when deciding whether the system will be applicable to different groups of individuals

Organisations are encouraged to consider the context and frequency of using biometric systems, especially for identification and verification of different groups of individuals. For instance, an office building may implement a facial recognition system and enrol facial images of its staff to access the office. The staff would be more receptive to this implementation given they go to work every day, and it may be more convenient than using a physical staff pass when entering the building. Likewise, members who frequently visit establishments like clubs, gyms and hotels might be more receptive and appreciate the convenience. However, one-off and short-term visitors may consider the enrolment of their facial images as part of its visitor management system to be less appropriate.

Organisations should also bear in mind that public acceptance may increase as new technologies become more pervasive. Management should periodically review past decisions as public expectations of privacy evolve, until the commercial use cases for new technologies have become more widely accepted.

v. Assessing the potential risks and adequacy of protection mechanisms in the system

As discussed in Part II, organisations should review all potential risks and the impact of these risks to individuals or themselves in order to evaluate whether the protection mechanisms implemented by the system are adequate in addressing or commensurate with the level of potential risks or impact to the individuals and organisations.

B *Managing Vendors*

Biometric recognition or security camera systems are often managed and maintained by vendors (e.g. security firms). Where these vendors process personal data under the direction of and on behalf of an organisation, they would be considered Data Intermediaries (DI)[10] of an organisation. Under these circumstances, the organisation as the data controller is still responsible for ensuring compliance with all of the Data Protection Obligations of the PDPA for the collection, use and disclosure of personal data.

Organisations should refer to the PDPC's *Guide to Managing Data Intermediaries under the PDPA* on how to manage vendors. The following paragraphs highlight salient points relevant to biometric recognition systems:

- Put in place obligations and responsibilities of the DI within the contract for the safeguarding and retention of personal data (e.g. the DI is to put in place proper access control to the security camera footage and to properly overwrite the data every 7 days [or retention period as defined by the organisation] when the footage is no longer required).
- Put in place standard operating procedures (SOPs) for managing access to personal data (e.g. approval levels and procedures to extract the selected section of a video footage that an individual appears in, upon his request).

The case study in Annex A illustrates the importance of these points for organisations outsourcing data processing activities.

[10] The PDPA defines a data intermediary as "an organisation that processes personal data on behalf of another organisation but does not include an employee of that organisation".

ANNEXES

ANNEX A: PRACTICAL GUIDE FOR DEPLOYING SECURITY CAMERAS

Organisations should take note that facial images collected through security cameras are generally considered personal data as it may allow an individual to be identified through his or her facial image. For the use of security cameras for ensuring security of premises, organisations may rely on publicly available exception (only in public places) or legitimate interests exceptions for collecting personal data without consent. The following are some of the best practices that organisations should consider when embarking on such deployment.

Before deploying security cameras:

- Be clear on the problem statement and consider other alternatives where appropriate. For example, if the purpose is solely for taking attendance, then consider if implementing check-in/check-out systems that do not capture facial images would be more suitable alternatives.

When installing security cameras:

Have Notices to Inform Individuals

a. For fixed-position security cameras, place notices at prominent locations to notify individuals that security cameras are in operation. Such notices do not need to identify the exact locations of cameras.

b. For moving security cameras (e.g. robot-mounted or body-worn cameras), raise awareness to individuals through these means:

   i. Ensure that the security camera is in plain sight and provide a visible indicator when it is in operation (e.g. have a blinking light).

   ii. Have the security robot or wearer wear a visible label stating that a security camera is in operation.

   iii. Provide verbal notifications to individuals where appropriate.

   iv. Affix a QR Code or contact information on the security robot for individuals to find out more.

Properly Deploy the Cameras

a. Avoid capturing footage that intrude into spaces where an individual has a reasonable expectation of privacy.

b. Avoid deliberate capture of intrusive footages when using the following devices:

   i. Fixed-position security camera – Pay attention to the camera positioning to ensure private areas and spaces are not captured.

   ii. Robot-mounted security camera – Ensure proper programming of routes to avoid capturing intrusive footage of private areas and spaces.

   iii. Body-worn cameras – Ensure wearers switch off their body-worn cameras before entering locations where a reasonable individual would expect privacy (e.g. washrooms).

c. Minimise incidental capture through the following measures:

   i. Flag locations on the patrol route which carry a high risk of incidental capture.

   ii. Provide clear instructions to operators or wearers on how to operate security cameras at these high-risk locations (e.g. switch off camera momentarily).

   iii. Use software to redact footage of these locations, if captured at the point of data collection.

Protecting the Footages and Database

a. Manage access to the footage and database to prevent unauthorised access by implementing measures such as:

   i. Restricting physical access to the storage facility (e.g. security control room).

   ii. Limiting the number of persons authorised to access the system and databases storing the personal data by having password protection.

   iii. Avoiding password sharing to minimise the risk of undetected inappropriate access and use of the system.

   iv. Where remote access is enabled, implement strong access control mechanisms such as two-factor authentication.

Retention and Disposal

a. Put in place a process to delete or overwrite the footages on a regular basis when they are not required for any investigative purposes or any other legitimate purposes.

b. In the event the security camera system is decommissioned, take steps to ensure proper destruction of the database (e.g. degaussing or physically destroying the storage medium containing the footages).

Governance and Reviews

a. Put in place internal governance structures and measures with effective communication and feedback channels to ensure robust oversight of an organisation's use of the security camera system.

b. Carry out compliance checks and audits regularly to ensure the continued relevance and effectiveness of the safeguards and procedures of the security camera system.

Manage and Train Your Staff and Vendors

a. Reinforce the vendor's data protection obligations through contractual clauses.

b. Provide adequate training to staff and vendors for handling access requests to data.

   i. Document the steps and procedures when an access request is received. For example, ask the individual for the purpose of their request and for further details to identify the relevant footage and determine the most cost-efficient way of meeting the request.

   ii. Establish clear approval processes and authorities for approving access requests.

   iii. Once the relevant footage has been identified, educate staff and vendors on how to determine if the footage includes third-party personal data and whether masking is required. For example, establish if the footage captured is of an area open to the public or a private premise. If the footage is of a private premise, determine if the footage contains third-party personal data and whether any exceptions apply that would allow the organisation to disclose the footage without masking.

   iv. Educate staff and vendors to provide only the security camera footage that is necessary to deal with the access request.

c. Provide documents that staff and vendors can refer to when dealing with access requests (e.g. SOPs and flow charts that can be easily followed at a glance).

Case Study: No DP-1903-B3554: MCST Plan No. 3593 & Others

Case No DP-1903-B3554 (**"Case"**) demonstrates: (i) the importance of managing vendors when outsourcing services and (ii) the importance of training employees.

To summarise the facts of this case, there was unauthorised disclosure of CCTV footage recorded at the premises of MCST 3593 by New-E Security Pte Ltd ("New-E"), a company providing security services at the condominium, to an owner of a unit at the condominium. New-E was engaged to process personal data (i.e. video footage captured by the CCTV network and system) on behalf of MCST 3593. An employee of New-E (**"Security Supervisor"**) retrieved the CCTV footage, recorded it using his mobile phone, and transmitted it to the resident before receiving instructions from the relevant decision makers.

Lessons from this case that are relevant to organisations outsourcing services:

- When outsourcing services, put in place a written agreement with clauses requiring the vendor to comply with data protection provisions under the PDPA; and
- Carry out these contractual obligations through implementing practices like SOPs.

In this case, the contract between MCST 3593 and New-E did not contain any clause relating to the protection of personal data or any reference to the PDPA. There were no written instructions in the contract in relation to the management of CCTV footage.

Although New-E had a practice of only releasing CCTV footage to representatives of the managing agent hired by MCST 3593, this practice was communicated only verbally to New-E's employees and the managing agent. The security supervisor did not adhere to this practice and this may be due, at least in part, to the lack of a written policy which clearly sets out the relevant procedures to be followed before CCTV footage is disclosed. Furthermore, New-E did not have any written policies to instruct and guide its employees with respect to their obligations under the PDPA, particularly the usage of mobile phones to record CCTV footage. New-E also did not provide data protection training to its employees.

Lessons from this case that are relevant to organisations processing data:

- Put in place reasonable security arrangements, which include written policies and proper training; and
- Proper staff training creates data protection awareness amongst employees, inculcates good habits in handling personal data and puts employees on the alert for threats to the security of personal data. This is a necessary complement to an organisation's data protection policies.

ANNEX B: PRACTICAL GUIDE FOR DEPLOYING ACCESS CONTROL SYSTEMS TO BUILDINGS OR APPLICATIONS

Biometric recognition systems are commonly deployed in buildings or used by applications to control access to premises or services. Enrolment of an individual's biometric sample (e.g. facial image) is required to use the system. This entails using sensors (e.g. cameras or fingerprint scanners) to capture the individual's biometric characteristics (e.g. facial features or fingerprint patterns) that the system converts into templates for storage and subsequently recognition. Where organisations are capturing personal data, it is recommended that they seek explicit consent when enrolling users. For managing employees, organisations may rely on employment exception.

Typically for access control systems, in order to manage and identify individuals, each biometric template generated is referenced against some personal or employee data, such as an individual's name or employee number. As such collectively, this set of data is considered personal data and is subject to the PDPA. The following are some of the best practices that organisations should consider when embarking on such deployment.

Before deploying biometric access control system:

Be clear on the problem statement and consider other alternatives where appropriate. These include:

a. Non-biometric access controls like keycards; or

b. Adopting alternatives such as the Singpass or process an individual's biometric information using the in-built biometric capabilities on a mobile phone, to carry out biometric access control.

Some factors that organisations may consider include the context, security requirement and frequency of use of the biometric recognition system. The following non-exhaustive scenarios seek to illustrate this point:

a. An organisation that implements a biometric recognition system to manage ingress and egress for its employees, tenants or visitors.

b. A hotel that implements a biometric recognition system for access to their lifts and rooms for the purposes of facilitating the guests' stay and for security reasons.

Individuals in the above scenarios who are employees or hotel guests are likely to be more agreeable to the use of biometric data due to the frequency of their access to the premises or hotel facilities, as compared to one-time visitors to the premises or hotel. Ultimately, the decision to implement the biometric system rests with the organisation, which is why it is crucial for an organisation to be clear on the purpose of data collection and notify individuals accordingly.

When installing biometric access control system:

Ensure Accuracy and Security of System

a. Depending on the security required, consider implementing liveness detection to identify possible basic identity spoofing (e.g. using photos or videos), to sophisticated spoofing (e.g. 3D masks). Organisations may consider installing the sensor(s) near manned information or security counters, or have security officers conduct regular surveillance to deter spoofing attempts.

b. Set a reasonably high matching threshold to minimise false positives.

c. If a high level of security is required, consider additional factors of authentication (e.g. keycards with biometric recognition) or multi-modal biometric authentication (e.g. face with fingerprint).

d. Ensure that the system is protected from tampering or any man-in-the-middle attack. In implementations where such system resides in the cloud, organisations may consider adopting a secured communication channel to the cloud servers or advanced safeguards such as encrypting the biometric data (e.g. for facial images, a digital watermark could be one such encryption mechanism).

Protect the Database

The following are some measures to protect stored biometric data in the database.

a. Manage access to the footage and database to prevent unauthorised access through:

   i. Restricting physical access to the storage facility (e.g. security control room);

   ii. Limiting the number of persons authorised to access the system and databases storing the personal data and implementing password protection;

   iii. Avoiding password sharing to minimise the risk of undetected inappropriate access and use of the system; and

   iv. Where remote access is enabled, implement strong access control mechanisms such as two-factor authentication.

b. Encrypt stored biometric samples and templates. For applications that require a high level of security, use application-specific keys to encrypt the biometric data.

c. Segregate storage of biometric data from other personal datasets.

d. Where possible, use arbitrary unique identifiers, instead of names of individuals, to reference the templates to personal data.

Retention and Disposal

a. Where possible, do not store biometric samples once these are converted into templates, and only store the templates which are required for processing the access control.

b. When an enrolled individual is no longer valid (i.e. termination of service or leaves the company), the organisation should also cease to retain the template and associated data in the system, rather than merely disabling the individual's access to the premises of service.

c. In the event where the biometric access control system is decommissioned, take steps to ensure proper destruction of the database (e.g. degaussing or physically destroying the storage medium containing the biometric samples and templates).

Manage and Train Your Staff and Vendors

a. Reinforce the vendor's data protection obligations through contractual clauses.

b. Provide adequate training to employees and vendors to deal with access requests to personal data used in the access control system:

   i. Document the steps and procedures when an access request is received.

   ii. Establish clear approval processes and authorities for approving access requests.

   iii. Only provide the biometric sample or the personal data that is required to address the access request by the data subject.

c. Provide documents that staff and vendors can refer to when dealing with access requests (e.g. SOPs and flow charts that can be easily followed at a glance).

ANNEX C: SAMPLE TEMPLATE FOR ADAPTATION BY ORGANISATIONS FOR SURVEILLANCE / SECURITY USE CASES

Under Annex C of the *Advisory Guidelines on Key Concepts in the PDPA*, the PDPC has provided a checklist to guide organisations in assessing whether they may rely on the legitimate interests exception[11]. The checklist has been replicated here and filled up as a sample that organisations may use and adapt for relevant surveillance or security use cases. For other use cases, this sample can still be used as a reference, but organisations may also wish to refer to the instructions in Annex C of the *Advisory Guidelines on Key Concepts in the PDPA*.

S/N	Step 1: Define the context/purpose of collection, use and/or disclosure	
1	What is the purpose of relying on the legitimate interests exception to collect, use or disclose personal data?	*Describe the legitimate interests of the organisation or another person and explain what are the objectives or purposes for collecting, using or disclosing the personal data.* *[Company name]* is relying on the legitimate interests exception to collect, use and disclose personal data of individuals that is required for the operation of a Security Facial Recognition System ("SFR System"). The SFR System will detect and prevent threats to the physical safety and security of the *[Company's premise(s) or premise(s) that the SFR system is to be used in]* [e.g. terrorism and crime prevention ("Security Purpose")].
2	List the types of personal data that will be collected, used and/or disclosed for this purpose.	Facial image of a person-of-interest ("POI") obtained through a screenshot from the *[premise(s)']* CCTV video footage and CCTV recordings of that POI's activities on property. POIs refer to: a. persons that *[Company]* is required to notify the Police if identified on the property pursuant to a direction from the Police; or b. known or suspected terrorists whose photo images are on published terrorist lists. Where the *[Company]* is able to obtain a facial image of the POI, these facial images will be stored in the database of the SFR system.

[11] It is not mandatory for organisations to use this checklist, and organisations may wish to conduct their own assessment to justify their reliance on the legitimate interests exception.

3	Describe how the personal data will be collected, used, and/or disclosed.	Security staff *[and/or any other parties if relevant]* will be alerted (including through the use of the SFR system) when there is a POI on the property. Security staff will manually capture a screenshot of the POI's frontal facial features. The screenshot of the POI's frontal facial features, CCTV footage of the POI and the POI's activity will be archived and stored in the SFR System for the Security Purpose. Should the Security Staff determine through the captured information that the POI is a security risk, for instance terrorism related, they may report the POI to the Authorities *[and/or any other parties – to list where relevant]* (e.g. Police), share information collected on the POI with the Authorities *[and/or any other parties – to list where relevant]* and/or take further steps to ascertain the POI's motivations. If the actions of the POIs also necessitate further monitoring, then the facial features captured will be utilised by the SFR system for future detection purposes should the POI return to the property.
4	Is the collection, use or disclosure on a one-off or a continuous basis?	*If continuous, please state occurrence.* The SFR system will continuously detect when POIs are on property.
S/N	**Step 2: Identify the benefits of collection, use and/or disclosure**	
5	How does the legitimate interests benefit the organisation or another person?	*This should focus on direct benefits arising from the legitimate interests of the organisation or another person. This may also include negative impact on organisation/individuals/groups of individuals if the legitimate interests cannot be carried out.* Keeping the *[premise(s)]* safe from terrorism and crime is beneficial for *[Company]*, the *[Company's]* employees, visitors, guests and the general public. This will protect the company's viability and the jobs of its employees. Ensuring that the *[premise(s)]* is not attacked by terrorists will protect the lives of employees, visitors and guests. Refer also to paragraph 1.
6	Who does this benefit?	*Beneficiaries may include the wider public or segment of the public or organisation such as customers, employees, sector or industries of the economy.* The beneficiaries of this legitimate interest are the employees, visitors and guests of the *[premise(s)]* as well as the general Singapore public. Further, a successful attack on the *[premise(s)]* would cause severe damage to the *[tourism or any other sector where relevant]* industry in Singapore and would impact the perception of how safe and secure a country Singapore is.

S/N	Step 3: Assess whether there is any likely adverse effect to the individual	
	Sensitivity of personal data	
7	Is the personal data being collected, used or disclosed (as listed in Step 1) of a sensitive nature?	No, the personal data of the POIs that are in our CCTV recordings are not sensitive in nature because the POIs' activities on property being monitored are in publicly accessible areas and therefore can be observed by other visitors or even by security staff if present in the *[premise(s)]*. We are merely using surveillance camera technology to improve our ability to detect POIs on property.
	Reasonableness of the purpose of collection, use and/or disclosure of personal data	
8	How extensive is the collection of data?	*Please describe if there is any large-scale collection of data, factoring in both the volume of data collected and number of types of data fields collected.* Only POI's activities, once determined by Security to compromise the Security Purpose, are monitored over time by the SFR system to detect any patterns and collect footage of such POI's activities. Activities of other patrons are not monitored.
9	How reasonable is the purpose of collection, use, and/or disclosure of the personal data?	Reasonable in light of the Security Purpose. This is especially so in this case, because the consent of individuals cannot be obtained and doing so would defeat the purpose of detecting individuals who are motivated to carry out illegal activities or terrorist acts without alerting them.
	Likely adverse effect to the individual	
10	What are the reasonably foreseeable adverse effects to the individual (e.g. financial, social, physical, psychological effect)?	Individual may be alarmed or distressed if they find out, pursuant to their access request, that *[premise(s)]* is using facial recognition technology to monitor their activities on property over time. However, we believe that a reasonable individual, if provided an explanation that the technology is only meant to monitor POIs and the rationale for doing so, would not suffer any psychological distress. There are no adverse financial, social or physical effects that would be caused by such monitoring. Images of other patrons may be inadvertently captured in the CCTV footage on the POI if such patrons are standing next to the POI.
11	Will you use other information from other datasets to make predictions or decisions?	**Y/N** *If yes, please describe the datasets used for merger and whether the individual is aware that you are in possession of the dataset. Please also describe the types of decisions/ predictions that would be made with the data.* No

12	Will the predictions or decisions exclude, discriminate against, defame, or harm the individual?	**Y/N**	*Please state the types of predictions or decisions that would be made with the data and justify why these may or may not be accurate.* No
13	What is the likelihood and severity of any potential impact to the individual?		*You should consider this relative to prevailing social norms. Refer to paragraph 12.69 of the main Advisory Guidelines for a list of considerations.* If a POI is detected by the SFR system, the Security Staff will confirm that the POI is correctly identified and take steps to speak with the POI to ascertain the motivations for his or her behaviour before determining if it is necessary to report the POI to the authorities for further investigation. The Security Staff will not be hindering the POI's movements on the property if the POI does not take active steps to damage property or injure persons. The potential impact to the individual is therefore limited because any investigations of his or her behaviour will have to be conducted by the authorities in accordance with Singapore law.
14	How did you provide the details of a contact who can provide the individual with more details of the collection, use or disclosure of the personal data?		*Please describe how the details are provided.* The *[Company's]* Data Protection Officer's ("DPO") contact is already in the publicly accessible Privacy Notice for patrons to use to contact the DPO for assistance with enquiries. *[To provide website link to access Privacy Notice]*
	Mitigating measures		
15	Can you adopt any measures to mitigate, eliminate or reduce the likelihood of the adverse effect?	**Y/N**	*If yes, please describe the measures and justify how the measures are able to mitigate or reduce the likelihood of the adverse effect.* *If no, please state the reasons for why not.* The SFR system will alert Security if a POI is identified on property. When alerted, Security will verify that the person identified matches the POI image on record. Security will then apply a set of criteria (which is set out in our company's SOP) to assess if CCTV footage of the POIs' activities need to be archived (retention period is as set out in our company's data policy), so as to reduce excessive monitoring of individuals and/or excessive storing of footage on individuals. Access to the CCTV footage of POIs will be restricted to authorised Security personnel only. CCTV footage will be used solely by such Security personnel to assess if the POI poses a security risk to the *[premise(s)]* and for reporting to the Authorities *[and/or any other parties – to list where relevant]* only and will not be used for any other purposes.

S/N	Step 4: Assess likely residual adverse effect	
16	What are the likely residual adverse effects to the individual after applying measures to mitigate the adverse effect specified above?	The only likely residual adverse effect to an individual is in the case where such individual is not actually a security risk but happens to have behaved in a way that results in him or her being classified as a POI and therefore monitored by the SFR System. This also results in footage of him or her being stored by the SFR System. The footage may not however be utilised for any purpose but is kept so that the system can detect patterns of similar behaviour from that individual over time as per its programming.

	Balancing test		
17	Do the identified legitimate interests outweigh the residual adverse effects?	**Y/N**	*If yes, please explain and justify.* Yes, the identified legitimate interest of protecting the *[premise(s)]* and the significance of its protection to Singapore and the general public in paragraph 5 above outweighs the described residual adverse effects in paragraph 16 above.
18	Can you rely on the legitimate interests exception to collect, use and/or disclose personal data for this purpose?	**Y/N**	*If yes, please explain and justify.* See above.
19	Are there any further actions to be taken?	**Y/N**	*If yes, please describe.* Security will use FR to detect POIs in our live CCTV recording in real-time, to facilitate Security in monitoring the POIs. If needed, Security will archive CCTV footage of the POI's activities. Archived CCTV footage of POIs are stored in the existing *[premise(s)']* surveillance system which has established control protocols as recommended by *[relevant dept e.g. IT and Cyber Security]*. Access to the CCTV footage of POI(s) will be restricted to only authorised Security personnel operating at *[place of operation]*, attending to the incident and/or as directed by *[specific authority, e.g. Head of Security]*. If after a reasonable time or after certain investigations are conducted, it is assessed that the individual poses no security risk, Security will purge the POI data. If there is assessed to be security risk, Security may report the POI to the Authorities *[and/or any other parties – to list where relevant]*. All visitors to the property will be notified via a publicly accessible Privacy Notice on the website and physical notice(s) at the entrance of property that *"[insert wording of the signage]"*. Our company website will also notify that the Legitimate Interests exception is being relied upon for these purposes.

20	Outcome date	*<Date of assessment>*
21	Completed by	*<Date of assessment>*
22	Endorsed by	*<Name of officer and designation>* *<Name of DPO officer and designation>*
23	Agreed by	*In line with the Accountability principle, the assessment should be reviewed by the appropriate members of management with sufficient authority.* *<Name of authority and designation, e.g. Head of Security>* *<Name of DPO authority and designation>*

ACKNOWLEDGEMENTS

The PDPC and Security Association Singapore (SAS) express their sincere appreciation to the following organisations for their valuable feedback in the development of this publication:

- AsiaDPO
- CapitaLand
- Law Society of Singapore's Cybersecurity and Data Protection Committee 2021/2022
- Marina Bay Sands Pte Ltd
- NEC Asia Pacific Pte Ltd
- SenseTime
- Smart Nation and Digital Government Group (SNDGG)
- Xjera Labs Pte Ltd
- Yitu

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people — empathy and assurance will be at the heart of all that we do.

JOINTLY DEVELOPED BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SAS SECURITY ASSOCIATION SINGAPORE