Case 202400056

Enforcement Order

The Proprietors, Strata Plan No. 273

12 December 2024

SUMMARY

An owner of units (the Complainant) within the Pinnacle Condominiums (the Pinnacle) submitted a complaint to the Ombudsman under the Data Protection Act (2021 Revision) (DPA)[1] against the Proprietors, Strata Plan No. 273 (the Strata). The Complainant claimed that the Strata was processing personal data through its on-site CCTV system in an unlawful manner.

They raised concerns that the purposes for which the CCTV footage was being used were excessive and some of the cameras were located in unnecessarily intrusive areas, such as the owners' lounge, gym and pool. They also claimed there was no signage in place to let people know that CCTV was in use. The Complainant stated that the Strata's CCTV Policy (the Policy) did not make clear how long footage was to be stored, or what security measures were in place to protect the data that was being collected.

The Complainant had also issued a notice under Section 10 of the DPA requesting that the Strata cease processing their personal data via the CCTV system, and they were dissatisfied with the Strata's response to this notice.

The Ombudsman investigated the matter and found that the Strata has breached the First data protection principle by failing to have an appropriate legal basis for all of the purposes listed in the Policy. The Strata has also breached the third data protection principle as it has been processing excessive personal data in relation to the purposes which fail to meet the necessity test. It is also a breach of the third principle to capture footage from locations which are unnecessarily intrusive.

[1] In this decision, all references to sections are to sections of the Data Protection Act (2021 Revision), and all references to regulations are to the Data Protection Regulations, 2018, unless otherwise specified.

The Strata is likely to be retaining personal data for longer than is necessary for the stated purposes, which is a breach of the Fifth data protection principle. The Strata has also breached the Sixth data protection principle, as its response to the Complainant's Section 10 notice was not valid, as well as breaching the Seventh principle by failing to have appropriate contracts in place with its data processors.

The Ombudsman ordered the Strata to review the Policy to ensure that the CCTV footage is only used for lawful purposes, to clarify the roles of the Strata and its data processors, and to define the retention periods for the data more clearly. The Policy must also be clearer about the circumstances in which covert monitoring can be used, when monitoring of staff might take place, and in which circumstances data can be shared with third parties.

The Strata must also ensure that suitably detailed signage is in place at all points of entry to the property, if it is not already, and that it is reviewed regularly to ensure accuracy. The locations of the cameras must also be reviewed to ensure they are only sited in areas where they are necessary for the lawful purposes.

The Strata must review its response to the Complainant's Section 10 notice, and it must put in place contracts with its data processors that meet, at a minimum, the requirements of Paragraph 3, Part 2 of Schedule 1 of the DPA.

The revised Policy must be submitted to this office for review once the required amendments have been made.

A. BACKGROUND

[1] In this case we have had no direct contact from either the Complainant or the Strata, as all correspondence has been conducted via each party's attorneys. For ease of reading, we reference 'the Complainant' and 'the Strata' below as having sent correspondence, but this has always been via their attorneys.

[2] In September 2023 the Complainant asked the Strata a number of questions about its processing of personal data through the CCTV system, including requesting a copy of a written policy and for details of how the footage was managed.

[3] On 2 October 2023 the Strata responded confirming that no written policy could be found, but one had now been produced. A copy was supplied to the Complainant. Details were also provided on the location of the cameras and the management of the footage.

[4] The Complainant followed up on 1 November 2023, raising concerns about the legal basis for the use of the CCTV system and how it was being managed. This letter contained a notice under Section 10 of the DPA requiring the Strata to "cease collecting and processing video footage" of the Complainant via the CCTV system.

[5] The Strata responded to this letter on 21 November 2023, making the argument that the Strata owners had voted unanimously in 2017 to install the CCTV system, and stating that the Complainant should have raised their objections at that point. The Strata also refused to comply with the Section 10 notice, claiming that the processing is necessary for the performance of a contract to which the Complainant as a data subject is a party.

[6] The Complainant sent a further response on 18 January 2024 refuting the Strata's reasoning for the refusal to comply with the Section 10 notice. They also detailed a number of specific concerns they had with the use of CCTV system, alleging failures to comply with the data protection principles. Finally, they set out a list of reasonable controls that they felt should be put in place before they would consent to the collection of their personal data through the system.

[7] The Strata did respond to this on 25 January 2024 stating that it would undertake a review of the CCTV policy and the Complainant's proposed controls, but it is not clear that this review ever took place.

[8] On 26 January 2024 the Complainant sent a complaint to the Office of the Ombudsman, including copies of previous correspondence, the Policy and the Strata By-Laws.

[9] The Policy confirms that the CCTV system is used for the following purposes:

- the prevention, reduction and detection of crime;
- the safety of personnel, property and third parties;
- the monitoring of potential breaches of processes or regulations, including Strata Corporation bylaws, rules and regulations;
- the monitoring of appropriate use of any and every facility, property, privilege or amenity of the Strata Corporation (such as the parking, the fire lanes, the gymnasium, the owners lounge, the tennis or pickleball court, the swimming pool and the two adjacent spa pools, the adjacent water features, beach and patio areas, including any equipment or furniture or fittings in connection therewith such but not limited to audio-visual equipment in the lounge, audio-visual equipment and exercise equipment in the gym, and life, fire and safety equipment about the property, such as fire extinguishers, defibrillators and otherwise);
- the observation and monitoring of vehicular and pedestrian traffic and/or numbers of people;
- the observation of and monitoring for hazards, including as to drainage, escape of water, downing of trees, the parking gate operations, the garbage and recycling area, the propane tanks and connected system supplying the north side Kohler emergency generator, the safe propane bar-b-que use at the north and south sides of the property;
- for damage, obstructions or breakdowns, including for weather, storm and hurricane preparedness, their impact, and for continuity and recovery, and generally for site safety, security and integrity of Strata Corporation property (including the common property thereof);
- the health, welfare and safety of individuals; and
- the proper care and control of leashed or unleashed pets and animals, and the observation and preservation of evidence in any matter of litigation, including without limitation civil matters such as for alleged personal injury, torts and negligence, employer liability, workers' compensation or otherwise in the ordinary course of the affairs and the undertaking of the Strata Corporation, or in any other legal proceeding whereby the Strata Corporation or the CCTV Manager or others for

whom the Strata Corporation may be or become at law responsible, or as may be or become, or be at risk of becoming, an alleged defendant, third-party, contributor, indemnitor or be alleged to be otherwise responsible at law.

[10] The complaint raised several specific issues about the processing of personal data via the CCTV system, which cover the following topics:

- The purposes for the CCTV footage listed in the Policy are too broad and do not meet the necessity test.
- There is live monitoring of the footage, which the Complainant feels is more intrusive than simply recording.
- Some of the locations covered by the cameras, including the owners' lounge, gym and pool, are intrusive and unnecessary.
- There is no signage in place and therefore data subjects have not been able to provide unambiguous and freely given consent for the processing of their personal data.
- The retention periods for the data are unclear and there are no written guidelines covering when data will be stored for longer than normal.
- The security measures in place to protect the data are not made clear in the Policy.

[11] The complaint also reiterated the list of reasonable controls that the Complainant felt should be implemented, namely:

- Properly defined and compliant purposes for the CCTV system.
- Clear access controls for the data.
- Removal or redirection of the cameras in the lounge, gym and pool area.
- No real time monitoring.
- Restricted time periods for data storage.
- Documented guidelines and reasons for which data can be stored beyond the agreed time period.
- Adequate system and data security measures.
- Data subject right to review the software access logs.
- Adequate signage on the premises in relation to the use of CCTV cameras.
- Use of masking techniques when providing video data to data subjects in response to right to access requests.
- No covert monitoring.

- Documented regular review of risks, security policies and measures to ensure appropriate levels of security are in place.

[12] The complaint also raised issues about the alleged dismissive attitude of the Strata and around the ownership of copyright in the images. As these do not relate to compliance with the DPA, we cannot address them in this notice. It should be noted that it is our understanding that ownership of copyright in the footage obtained by CCTV cameras would generally lie with the operators of the system. However, this is not a matter on which we can make any determination.

[13] On 24 June 2024, we notified the Strata that we had received a complaint against it under Section 43. We asked a number of questions relating to the concerns raised by the Complainant. We also asked the Strata to describe how the system was being operated and how this was being done in compliance with the DPA.

[14] The Strata responded to this on 31 July 2024, providing answers to our questions along with attachments detailing the locations and signage of the cameras; details of a prior criminal investigation where footage had been shared with RCIPS; a response from the provider of the CCTV system; and an extract of the contract between the Strata and the company that manages the CCTV system on its behalf.

[15] The locations of the cameras were listed as follows:

Internal [Indoors]:

- Management Office [North Building]
- Maintenance Room [North Building]
- Guard House [Centre Driveway]
- Gym [South Building]
- Owner's Lounge [South Building]

External [Outdoors]:

- Beach North
- Beach South
- Pool Left Side
- Pool Right Side
- Boundary Walkway North

- Boundary Walkway South
- South Garages 1
- South Garages 2
- South Gate
- South Parking
- South Elevator [Lobby] Area
- South BBQ Area
- South Pathway
- South, Behind Garage
- North Garages 1
- North Garages 2
- North Parking
- North Elevator [Lobby] Area
- North Entrance to the former resident manager's apartment
- North Pathway
- North BBQ
- North Pathway
- North Entrance.

B. CONSIDERATION OF ISSUES

[16] Section 43 states:

> *43. (1) A complaint may be made to the Ombudsman by or on behalf of any person about the processing of personal data that has not been or is not being carried out in compliance with the provisions of this Act or anything required to be done pursuant to this Act.*
> *…*
> *(3) On receiving a complaint referred to in subsection (1), or on the Ombudsman's own motion, the Ombudsman may conduct an investigation.*

[17] Section 45 states:

> *45. (1) If the Ombudsman is satisfied that there are reasonable grounds for believing that a data controller has contravened, is contravening or is likely to contravene any provision of this*

Act, the Ombudsman may, with a view to effecting the data controller's compliance with the provision, by way of an order served on the data controller, require that data controller to —

(a) take specified steps within a specified time, or to refrain from taking specified steps after a specified time;

(b) refrain from processing any personal data, or any personal data of a specified description;

(c) refrain from processing data for a specified purpose or in a specified manner, after a specified time; or

(d) do anything which appears to the Ombudsman to be incidental or conducive to the carrying out of the Ombudsman's functions under this Act.

[18] Section 2 defines "data controller" as follows:

"data controller" means the person who, alone or jointly with others determines the purposes, conditions and manner in which any personal data are, or are to be, processed…

[19] Section 2 defines "data processor" as follows:

"data processor" means any person who processes personal data on behalf of a data controller…

[20] The First data protection principle in Paragraph 1, Part 1 of Schedule 1 states:

First principle

1. Personal data shall be processed fairly. In addition, personal data may be processed only if —

(a) in every case, at least one of the conditions set out in paragraphs 1 to 6 of Schedule 2 is met

[21] Furthermore, Paragraph 2, Part 2 of Schedule 1 requires that certain information be provided to data subjects:

First principle: specified information at relevant time

2. For the purposes of the first principle personal data shall not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum —

(a) the identity of the data controller; and
(b) the purpose for which the data are to be processed.

[22] The third data protection principle in Paragraph 3, Part 1 of Schedule 1 states:

Third principle
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

[23] The Fifth data protection principle in Paragraph 5, Part 1 of Schedule 1 states:

Fifth principle
Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

[24] The Sixth data protection principle in Paragraph 6, Part 1 of Schedule 1 states:

Sixth principle
Personal data shall be processed in accordance with the rights of data subjects under this Act.

[25] Section 10 states:

(1) A data subject is entitled at any time, by notice in writing to a data controller, to require the data controller to cease processing, or not to begin processing, or to cease processing for a specified purpose or in a specified manner, the data subject's personal data.

(2) The data controller shall, as soon as practicable, but in any case within twenty-one days or receiving a notice under subsection (1), comply with that notice unless –
(a) the processing is necessary for the performance of a contract to which the data subject is a party or the taking of steps at the request of the data subject with a view to entering into a contract;
(b) the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
(c) the processing is necessary in order to protect the vital interests of the data subject; or

(d) the processing is necessary in such other circumstances as may be prescribed by regulations

and the data controller shall state to the data subject the reasons for the non-compliance with the notice.

[26] The Seventh data protection principle in Paragraph 7, Part 1 of Schedule 1 states:

Seventh principle
Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

[27] Furthermore, Paragraph 3, Part 2 of Schedule 1 requires that a contract be in place with data processors:

Seventh principle: processing contract to ensure reliability
3. If processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall not be regarded as complying with the seventh principle unless the processing is carried out under a contract –
(a) that is made or evidenced in writing;
(b) under which the data processor is to act only on instructions from the data controller; and
(c) that requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

Identity of the data controller

[28] Section 5(4) states that

Subject to section 17, a data controller shall comply with the data protection principles that relate to the personal data that the data controller processes, and shall ensure that the data protection principles are complied with in relation to the personal data that are processed on the data controller's behalf.

[29] It is therefore important that we clearly identify the roles of the parties involved in the processing of the personal data in this case. According to the Policy, the CCTV system is owned by the Strata, but it utilizes two third party organizations to manage the system on its behalf. Knight Security Services (Cayman) Limited is defined as the 'CCTV System Manager' and BCQS Property Management Limited is defined as the 'CCTV Manager'. The Policy clearly states that the Strata is the data controller and the third parties are data processors.

[30] We were concerned by the statement in the Policy that the CCTV System Manager is the "sole entity which may create additional users, or amend user access, on the surveillance system". We have been assured by the Strata that any decisions on user access are made by the Strata alone, and that the CCTV System Manager acts under the Strata's instructions when carrying out these functions. We accept that the CCTV System Manager is acting as a data processor.

[31] The Policy describes the CCTV Manager as the "person responsible for the overall management and operation of the CCTV and surveillance system, including all aspects of installation, recording, reviewing, monitoring and compliance with this policy". If the Strata is the data controller then it should be responsible for at least some of this, and certainly for compliance with the Policy.

[32] There are several areas of the Policy where the CCTV Manager is described as being responsible, even though the specific functions would normally be part of a data controller's obligations and duties under the DPA:

- "…undertaking a data protection impact assessment, for and on behalf of the Strata" should there be any extension of the CCTV system;
- "…ensuring that the signs are adequate and are erected in compliance with…the code of practice issued by the Information Commissioner's Office (UK)";
- being the point of contact for questions about compliance with the Policy;
- authorizing the conduct of covert monitoring;
- authorizing retention of images and data for more than 30 days;
- approving access to images and data;
- handling requests for access to images and data from police officers;
- receiving data subject rights requests made under the DPA.

[33] The Strata provided us with an extract from its contract with the CCTV Manager, which includes the following text (with the CCTV Manager referred to as 'the Company' and the Strata referred to as 'the Client'):

> *Without limitation, from time to time under this agreement, the Company may be a 'data controller' and/or 'data processor' in regard to 'personal data' (and rarely, but possibly also 'sensitive personal data') under the Act pertaining to 'data subjects' in connection with the Client, its constituent strata lot owners, vendors, suppliers, employees, contractors, tenants and others. For itself and for the benefit of the Client, the Company will observe, keep and perform all of the Company's respective obligations under the Act of a 'data controller' or 'data processor' in regard to such 'data subjects', as above.*

[34] So it appears that while the Strata is of the view that the Strata "*remain the Data Controller and they remain Data Processors, as at any time it is within our right and control to remove them from their role as processor and we can direct how they act and they act at all times under our instruction*", the contract they have signed with the CCTV Manager is less clear on this distinction. It may be that the CCTV Manager only processes personal data as a data controller on a limited basis for its own purposes, such as the management of the relationship with its client. However, this is not clear from the documentation we have been provided.

[35] We accept that the distinction between data controllers and data processors can sometimes be difficult to determine in certain complex business relationships. We also understand that the Strata is run on a voluntary basis and relies on the technical expertise of its suppliers to ensure compliance with laws and standards. However, the Strata should be careful to ensure that the decision-making discretion it allows to its data processors does not extend to the overarching decisions on what personal data is to be processed, how it will be processed, and what it will be used for. Authorizing covert monitoring, access to images and data, and extensions to standard retention periods are certainly areas where the discretion has the potential to go too far.

[36] **The Policy and the contract must be reviewed to ensure that they are much clearer as to when the CCTV Manager is acting under the instructions of the data controller. In areas where the CCTV Manager is given responsibility for carrying out certain tasks and taking decisions on behalf of the Strata, it should be made clear that ultimate authority for those decisions rests with the Strata, as data controller. Controls should be put in place to ensure that the Strata does exercise that authority, even though it is relying on the expertise of its processors. It must also be made clear that the CCTV Manager cannot use any of the images or data that are captured by the CCTV system for its own purposes.**

First data protection principle – fair processing

[37] The standard approach to meeting the fair processing requirements of the First principle for CCTV systems is to have clear and visible signage that contains, at a minimum, the information that is required under Schedule 1 Part 2 Paragraph 2 of the DPA. The Complainant claimed that, around the time of the complaint, there was no signage in place to indicate the presence of CCTV cameras in the location.

[38] In response to our queries, the Strata provided confirmation that signage is now in place, although it was not confirmed when this was erected. Photographs were provided showing the signage in situ at a number of locations throughout the property. Some, but not all, of the signs contain the relevant information that is required by the DPA.

[39] It is best practice in meeting this transparency requirement to ensure that full information is available to data subjects when they enter the site, before they are captured by cameras. The signs that contain the required information should be placed at all points of entry to the site, so that data subjects are aware of the existence of the cameras before they enter.

[40] **The Strata must ensure that suitably detailed signage is in place at all points of entry to the property, if it is not already, and that it is reviewed regularly to ensure accuracy.**

First data protection principle – legal basis

[41] The other requirement for compliance with the First principle is that the processing must meet one of the conditions in Schedule 2 of the DPA, known as the legal basis for processing.

[42] Initially, when refusing to comply with the Complainant's Section 10 notice, the Strata claimed reliance on the legal basis in Schedule 2 Paragraph 2 of the DPA, which applies where:

> *The processing is necessary for –*
>
> *(a) the performance of a contract to which the data subject is a party; or*
>
> *(b) the taking of steps at the request of the data subject with a view to entering into a contract.*

[43] In its response to our queries dated 31 July 2024, the Strata further claimed that it also relies upon the condition in Schedule 2 Paragraph 6, which states that:

The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

[44] Finally, in their complaint, the Complainant states that the Strata "cannot and should not process data without consent". They also refer to the requirement for clear signage being important "as it allows a data subject to provide consent".

[45] Schedule 2 Paragraph 1 is the relevant legal basis for consent, and applies where:

The data subject has given consent to the processing.

[46] The Complainant is incorrect in stating that personal data cannot be processed without consent, as consent is only one of six valid legal bases contained within Schedule 2.

[47] Section 2 of the DPA defines consent as:

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the said data subject.

[48] Furthermore, Schedule 5 sets out conditions for valid consent, including in Paragraph 4, the stipulation that:

Where there is a significant imbalance between the position of the data subject and the data controller, consent shall not provide a legal basis for the processing.

[49] Given the imbalance between the data controller and the data subjects in this situation, and the sheer impracticality of having to obtain consent from every person to enter the site every time they enter, along with the inability for such systems to cope with someone withholding consent, this is not an appropriate legal basis to consider for the processing of personal data via CCTV systems. We have not considered this point any further.

Necessity

[50] The two legal bases under consideration both require the processing to be 'necessary' for the stated purposes. The capture of images of identifiable individuals by the CCTV system must therefore meet the test of necessity for either of the stated legal bases to apply.

[51] In our guidance on the legal basis for processing[2] we explain when processing might be considered necessary:

> *This means that the processing must be a targeted and proportionate way of achieving the purpose. The legal basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.*
>
> *It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.*

[52] The Strata has claimed that the processing of personal data via the CCTV system is necessary for it to meet its obligation under paragraph 31(1) of the by-laws, wherein it is required to "control, manage and administer the Common Property for the benefit of all Proprietors". When asked to explain, for each of the purposes listed in the Policy, why it is necessary and proportionate to use CCTV to achieve that purpose, the Strata explained that: "For each purpose the use of the CCTV system is necessary as no other feasible means to achieve the purpose exists, as the only alternative that exists is the use of large numbers of security personnel. It would [be] vastly uneconomic and cost prohibitive to have at the same time watchmen at every same vantage point 24/7, when the job can be done, or as an adjunct to the watchmen's job, by way of camera."

[53] The Strata also claimed that as there was a unanimous vote of the owners in 2017 in favour of the installation of the CCTV system, this also demonstrates its necessity.

[54] The Policy refers to a document produced by the UK Information Commissioner's Office (ICO) called 'In the picture: A data protection code of practice for surveillance cameras and personal information'. This code of practice has been superseded in recent years by the 'Surveillance Camera Code of

[2] https://ombudsman.ky/data-protection-organisation/legal-basis-for-processing

Practice'[3], produced by the UK Surveillance Camera Commissioner, and the ICO guidance on Video Surveillance[4]. These resources also make clear that the use of surveillance systems must be a necessary and proportionate response to a problem, only to be used when other, less intrusive methods are not available. Principle 1 of the Code of Practice states that:

> *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.*

[55] In its response to our questions, the Strata failed to identify why each of the purposes listed in the Policy were necessary as a pressing need, relying simply on the assertion that it needed to conduct these activities under its by-law obligation, which is worded very broadly. It has failed to explain why each of the purposes is necessary and why it must process personal data to achieve them. The only argument the Strata made for necessity was a financial one, claiming that it would need to employ more security personnel to carry out the same tasks as the CCTV system. However, this argument presupposes that each of the purposes is necessary in the first place, which the Strata has failed to demonstrate. We do not agree that the use of a CCTV system to achieve all of the listed purposes is necessary and proportionate.

[56] We accept that there is a pressing need to protect property and people from crime, such as theft or damage, particularly as there have been incidents of crime experienced on the site previously. We also accept that, on an exceptional basis, there is an argument that footage could be stored as evidence for the defence of legal claims. However, many of the purposes listed do not appear to meet a pressing need, and it is therefore hard to see how they can meet the test of necessity.

[57] In addition to this, given that the Strata has confirmed to us in its response that "there is no active live monitoring of the system, and the live feed does not appear on screen at all times and only when switched on", it is questionable as to whether the CCTV system would even allow the Strata to meaningfully achieve many of the listed purposes. A number of them refer to observation and monitoring, which could not be achieved without active live monitoring of the system. Therefore, the tool that is being used is not the appropriate one to achieve the purposes, even if they were justified to meet pressing needs.

---

[3] https://assets.publishing.service.gov.uk/media/619b7b50e90e07044a559c9b/Surveillance_Camera_CoP_Accessible_PDF.pdf

[4] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/

[58] It is possible that some of the purposes for which the CCTV system is used will not involve the processing of personal data relating to identifiable individuals, such as monitoring for hazards, damage or obstructions. As long as no personal data is used for these purposes, they would be allowable under the DPA.

Legal basis – necessary for the performance of a contract

[59] Looking at the first claimed legal basis, there are two steps that must be met for this to legitimately apply: (i) there must be a contract to which the data subject is a party; (ii) the processing must be necessary for the performance of that contract.

[60] The Strata's view is that the relevant contract here is the Strata by-laws, which bind the Strata and the individual owners. The Complainant has not disputed this, and we accept that the Strata by-laws is a contract for the purposes of this legal basis.

[61] The Strata identified six categories of data subjects whose data may be captured by the CCTV system:

- Owners at the Strata
- Their guests
- Employees of the Strata
- Agents of the Strata
- Contractors of the Strata
- Trespassers

[62] The Strata also gave its view that only two of these six categories of data subjects are parties to the contract: the owners at the Strata and their guests.

[63] Depending on how the Strata is defining the term 'guests', it is possible to foresee other categories of individuals whose data might be captured due to them legitimately being on site, such as tenants and other visitors (delivery drivers, contractors of the owners, or emergency services employees).

[64] From a reading of the by-laws, it is not clear how guests are parties to the contract, which only appears to bind the Strata and the proprietors.

[65] Tenants are made subject to the by-laws via a lease or tenancy that they enter into with the proprietor, but they are parties to the lease or tenancy with the proprietor, not to the by-laws with the Strata direct.

[66] In addition to this, as the Strata pointed out to us in an email dated 19 August 2024, the Complainant's units are owned by a company. It would be this company that is the Proprietor, and therefore party to the contract, not the Complainant as an individual data subject. As it is not uncommon for people to hold properties in the Cayman Islands through a company, it is likely that this also applies to a number of other owners at the Strata.

[67] **Most of the categories of data subjects captured by the CCTV system, including the Complainant, are not parties to the contract. In addition to this, a number of the purposes do not meet the necessity test, and therefore are not necessary for the performance of the contract. This would not appear to be the most appropriate legal basis on which to rely for the processing of personal data via the CCTV system in general, and it cannot be relied upon for the processing of the Complainant's data, as the processing is not necessary for the performance of a contract to which the Complainant is a party.**

Legal basis – legitimate interests

[68] For this legal basis to apply, there must be a legitimate interest being pursued, and the processing of personal data via CCTV must be necessary to achieve that legitimate interest. Then, there must be a consideration of the data subjects' rights, freedoms and legitimate interests. The data controller must balance their own needs against the intrusiveness of the processing and the impact it may have on individuals' rights to privacy.

[69] In its response to us, the Strata simply stated that it was relying on this legal basis without specifying the legitimate interests being pursued. We are working on the assumption that the legitimate interest being pursued is the Strata meeting its obligation under the by-laws, as detailed above.

[70] As detailed in our consideration of necessity above, we are not convinced that the CCTV system is the appropriate method for achieving a number of the purposes listed in the policy. It therefore follows that for those purposes, we do not agree that the processing is necessary to achieve the legitimate interests of the Strata.

[71] In addition to this, the Strata has failed to demonstrate to us that they have balanced their own interests against those of the data subjects. We find that the intrusive nature of the processing for a number of those purposes would be prejudicial to the rights, freedoms and legitimate interests of the data subjects, and would therefore not be justifiable.

[72] **The Strata has justifiable legitimate interests in protecting property and people from crime, and for the defense of legal claims. However, many of the purposes listed in the Policy do not meet the necessity test and could impact the rights and freedoms of data subjects.**

[73] **We find that the Strata's reliance on the legal basis in Schedule 2 Paragraph 6 of the DPA can not be used to justify all of the purposes listed in the Policy. There is no valid legal basis for the use of CCTV for purposes other than crime prevention and legal issues. The processing of personal data to meet the other listed purposes would breach the First data protection principle. Where the use of the footage does not involve the processing of personal data in order to achieve the purpose, this would not be covered by the DPA and would therefore be allowable.**

Third data protection principle – data minimization

[74] One of the key concerns raised by the Complainant was around the wide and excessive purposes for which the Policy allows the CCTV system to be used. The considerations above on necessity and the legal basis for processing have identified a number of purposes which fail to meet the necessity test and therefore have no legal basis. It follows that the processing of personal data for these purposes would also breach the third principle as it would be excessive to use CCTV footage to meet them.

[75] Another concern of the Complainant was around the locations of some of the cameras, which appear to cover areas where individuals would not necessarily expect to be under surveillance, notably the lounge, gym and pool area. The lounge and gym cameras are described as indoor cameras, so it appears that they will capture footage of people making use of these facilities.

[76] One reason given by the Strata for capturing footage in these areas was that there are health and safety issues in these areas, and it cannot afford to employ full time gym staff or lifeguards. Firstly, this argument must be evidence-based. If there is no history of serious health and safety issues occurring in these areas, then there is no pressing need to justify the use of CCTV. It cannot be based on speculative risks that have not been formally assessed.

[77] Even with that said, if there are frequent, serious health and safety issues in these areas, or notable risks have been identified, the Strata should consider other options rather than employing intrusive surveillance. A CCTV system cannot be an adequate replacement for a lifeguard when, by the Strata's own admission, there is little to no active monitoring of the footage.

[78] Another reason given was that the Strata wishes to uphold its rules of appropriate use of these facilities, such as hours of use and prohibitions on access. These purposes fail the necessity test, so it follows that any processing of personal data for these purposes is likely to be excessive and in breach of the Third principle. We have been made aware that the Strata already has other controls in place in any case, such as an electronic access keypad for the gym.

[79] The Strata also wishes to capture evidence from these areas in the event of claims against it should an injury occur in these areas. Speculative recording on the off chance of a legal claim does not meet the necessity test and is not a sufficient justification for siting the cameras in these areas. The Strata may use footage if it is necessary for legal purposes, but this should only be where an incident happens to be captured by cameras that have been installed for crime prevention purposes. It would be excessive to install cameras for the express purpose of capturing evidence for the defense of legal claims.

[80] Recording communal areas like this, where people are far more likely to have an expectation that they are not being monitored or recorded, is, by its very nature, intrusive, and, in the absence of necessity, excessive.

[81] The locations and fields of vision of the cameras should focus on those areas where they are most likely to achieve the stated purposes of crime prevention, such as main points of ingress and egress to the property, and perhaps corridors throughout the site. This may include outdoor cameras covering the entrances to the lounge and gym, if there is a genuine risk of crime in those areas, but indoor cameras in those locations are excessive. The cameras across the whole system should not capture any images inside individual apartments, across the land of neighboring properties, or across public areas such as Seven Mile Beach or West Bay Road.

[82] The Complainant also raised the issue of covert monitoring, which is monitoring of individuals without their knowledge. The Policy mentions circumstances under which covert monitoring may take place, and the controls that would be put in place in the event of such monitoring being undertaken. In response to our questions, the Strata stated that no covert monitoring had taken place, but was merely anticipated in the policy should it be required, "particularly upon request by the RCIPS".

[83] The use of covert monitoring is to be authorized by the CCTV Manager, although in line with our previous findings, this should ultimately be the Strata, as data controller. The Policy limits its use to "occasions when criminal acts have taken place, or staff safety has been identified as being at risk". It also goes on to state that it will only take place where "there are reasonable grounds for believing that illegal or unauthorised activity is taking place".

[84] We asked the Strata to elaborate on the phrase "unauthorised activity", to explain the kinds of activity this would be expected to cover. However, its response failed to give any further detail, nor did it explain the circumstances in which covert monitoring is the most appropriate method to deal with staff safety issues.

[85] In the event that criminal acts have taken place, or are suspected, we would expect the Strata to involve the RCIPS, who can then use the investigative tools at their disposal, which may include covert monitoring. We cannot see any circumstances in which it would be appropriate for the Strata to conduct its own investigation into criminal acts using covert surveillance. The way the Policy is currently written does appear to allow for this.

[86] The Policy also appears to allow for audio recording when undertaking covert surveillance. The Strata has assured us that the cameras currently in place have no audio recording capabilities, although the network video recorder (NVR) does have an audio option that is currently not being used. Given that, even for covert surveillance, the use of audio recording can only be justifiable in exceptional circumstances, we would advise the Strata to remove reference to audio recording from the Policy.

[87] A final purpose mentioned in the Policy is the use of the CCTV system for the monitoring of staff activities. The Policy acknowledges that should this monitoring be considered there must be a data protection impact assessment carried out to judge whether it is a proportionate response to the problem it is seeking to address, and to look at less intrusive alternatives. Again, the use of CCTV for monitoring of staff would only be justifiable in exceptional circumstances, such as where there is suspected criminal activity or gross misconduct. An intrusive surveillance system should not be used for minor conduct issues.

[88] **Consequently, the Strata is in breach of the third principle as it has been processing excessive personal data in relation to the purposes which fail to meet the necessity test. It is also a breach of the third principle to capture footage from locations which are unnecessarily intrusive and not required for crime prevention.**

[89] **The cameras must be located in positions where they are necessary to meet the primary purpose of the CCTV system, which is crime prevention. Other uses of the footage captured by these cameras may be permissible, such as for the defense of legal claims, or where no personal data is being processed, but the location of the cameras should not be dictated by these other uses.**

[90] **The locations and fields of vision of all cameras must be reviewed to ensure compliance with this principle. Cameras covering communal areas such as the gym, pool and lounge, if they are not necessary for crime prevention, must be removed.**

[91] **No covert monitoring has taken place, but the Policy must be much clearer about the circumstances in which it could be used, and the controls that will be in place to ensure it is carried out in compliance with the DPA.**

[92] **Similarly, it does not appear that any monitoring of staff has taken place, but this must only be done in exceptional circumstances, when absolutely necessary, and with appropriate controls in place. Staff must also be made aware of the monitoring in line with the requirements of the First data protection principle, unless an exemption applies.**

Fifth data protection principle – storage limitation

[93] There are two areas for consideration when looking at how long the data recorded by the CCTV system should be stored: (i) regular day-to-day retention of the footage that is recorded on an ongoing basis (what we will call 'standard footage'); (ii) extended storage of that footage which has been flagged as potentially important for investigations or legal cases.

[94] The Policy explains that the video recorder used to store the footage from the CCTV system automatically overwrites the data on a rolling basis, leaving footage from approximately the previous 15-16 days stored.

[95] The DPA does not define specific retention periods for particular processing activities. It states that personal data cannot be kept for longer than it is needed for the purposes for which it is being used. Therefore it is the purpose of the processing that will help a data controller to determine how long they need to retain personal data.

[96] The ICO guidance on video surveillance[5] states that:

> *You should also not determine your retention period simply by the storage capacity of any surveillance system, or just in case you think the data may be useful in the future.*

[97] The Strata was asked to explain the reasoning behind the retention periods that are described in the Policy, but it only answered in relation to footage that was being held for extended periods for evidentiary preservation.

[98] It appears likely that the current standard retention period of 15-16 days is being determined by the settings or storage capacity of the NVR, and we have not been provided with any evidence that the Strata has considered how long it actually needs standard footage to be retained before being overwritten.

[99] The Policy does not provide a great deal of detail to explain the decision-making process for extended retention of footage for investigatory purposes. In fact, it is somewhat confusing, as it states that the CCTV Manager must authorize retention for more than 30 days. It is not clear in what circumstances data would be retained for longer than the standard 16 days but less than 30 days. When asked about this, the Strata confirmed that this was an error in drafting and would be revised to close this gap in timings.

[100] The Policy also does not detail in which circumstances data is able to retained for more than 30 days, and what factors must be considered by the CCTV Manager when being asked to authorize this extended retention.

[101] **The Strata is likely to be retaining personal data for longer than is necessary for the stated purposes, which is in breach of the Fifth data protection principle. It must assess how long it actually needs standard footage to be stored by assessing its use for the approved purposes.**

[102] **The Strata must also detail the circumstances in which data is to be retained for longer than the standard retention period, and the factors which must be considered by the CCTV Manager when they are being asked to authorize that extended retention. It must also be made clear that the**

---

[5] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/how-can-we-comply-with-the-data-protection-principles-when-using-surveillance-systems/#retention

ultimate decision is for the Strata to make, as data controller, even if it is asking the CCTV Manager to do so on its behalf.

Sixth data protection principle – data subject rights

[103] On 1 November 2023, the Complainant issued a notice to the Strata under Section 10 of the DPA requiring the Strata to "cease collecting and processing video footage" of the Complainant via the CCTV system.

[104] The Strata responded on 21 November 2023, refusing to comply with the Section 10 notice, claiming that the processing is necessary for the performance of a contract to which the Complainant as a data subject is a party.

[105] The DPA requires a data controller to respond to a Section 10 request within 21 days of receiving it. The Strata did respond within this timescale.

[106] However, as has been previously established, the legal basis relied upon in the refusal is not valid, and therefore the refusal to comply with the notice is equally invalid.

[107] The legitimate interests legal basis does not provide an exclusion from the duty to comply with a Section 10 notice, so that cannot be relied upon by the Strata.

[108] Part 4 of the DPA contains a number of exemptions, some of which exclude data controllers from the obligation to comply with Section 10 notices. The only two which appear relevant to the Strata's use of a CCTV system are contained in Section 19 (crime, government fees and duties) and Section 25 (disclosures required by law or made in connection with legal proceedings).

[109] It follows that the Complainant's Section 10 notice must be valid insofar as it relates to any purposes that would not be covered by those two exemptions. This accords with our earlier conclusions in relation to the purposes which have a valid legal basis for processing and which meet the test of necessity. The system should only be used to process personal data, where necessary, for the crime purposes defined in Section 19, and in relation to legal proceedings, advice and rights, as detailed in Section 25.

[110] The Complainant also raised two points in their list of reasonable controls that relate to the Sixth principle: the data subject's right to review software access logs; and the use of masking techniques

when responding to subject access requests. The Complainant has not made a request that would involve these matters, so they have not formed part of our investigation. We will not take a view at this time on the right to review software access logs, but we would note that the use of masking techniques to allow the release of footage to data subjects is best practice when handling subject access requests, and the Strata should consider its use if it is not already in place.

[111] **The Strata must reconsider its response to the Complainant's Section 10 request, and only process personal data via the CCTV system for the valid purposes detailed previously.**

Seventh data protection principle – data security

[112] The Complainant raised concerns about the security measures that are in place to protect the data that is being recorded and stored by the CCTV system. In particular, they were concerned that there were inadequate controls on who can access the data and insufficient technical measures in place.

[113] The Seventh principle covers both the technical and organizational measures that are in place to ensure that any sharing of personal data is necessary and secure. It also sets out the contractual relationships that the Strata must have with its suppliers and subcontractors.

[114] Access control functions are delegated to the CCTV Manager and the CCTV System Manager, although the Strata confirmed in its responses to us that ultimate responsibility for determining who has access to the CCTV data lies with the Strata, through the Executive Committee. This seems to be an acceptable arrangement and suitably limits those who have access to the data.

[115] The property manager, working for the CCTV Manager, has access to the CCTV system via a feed to a mobile device. The application is password protected, as is the device. The only storage location for the data is on the NVR device. We are told that no element is cloud-based, not even the communication between the NVR and the mobile device. It is possible to download a copy of video images onto removable media via a USB connection to the NVR, however, this is only possible in the office, which is locked and alarmed if empty.

[116] In the absence of any actual breaches caused by a lack of technical security, or any particularly obvious security holes, it is out of the scope of this investigation to carry out a full assessment of the technical security controls that are in place. They appear to be appropriate given the information available to us.

[117] Paragraph 9.8.5 of the Policy states that images and data may be shared with "those who require assistance with the identification of someone (for example, the victim of crime, or a witness or perpetrator in relation to a criminal incident) and then only in exceptional circumstances". When asked to clarify what is meant by this, the Strata said that "exceptional circumstances simply means that the circumstances are such that the Strata feels compelled to act given the consequences of compliance or non-compliance with the request for the parties involved".

[118] The Strata has clarified that the only sharing of data with third parties has been with the RCIPS, where there had been two incidents of criminal activity on site.

[119] We are concerned that the Strata contemplates sharing of the data in the ways described in paragraph 9.8.5 and gives no detail as to what the 'exceptional circumstances' may involve. It should be clear that crimes should be investigated by the RCIPS and footage in relation to those crimes can be shared with them where necessary and appropriate. Allowing other third parties to access data relating to crimes would not appear to be appropriate and it is difficult to contemplate that being done in compliance with the DPA.

[120] The Strata shared with us a redacted version of its contract with the CCTV Manager. On review, we have found that this does not meet the standards required under Paragraph 3, Part 2 of Schedule 1. It does not state that the data processor is to act only on instructions from the data controller, and it does not require the data processor to comply with obligations equivalent to those imposed on a data controller by the Seventh principle.

[121] The Policy also states that the operators of the CCTV system "will be trained to ensure that they maintain and respect the privacy of neighbours, relevant personnel, strata lot owners within their strata lots, and of their lawfully permitted invitees within their strata lots…".

[122] We asked the Strata to confirm if this training had taken place and to explain the nature of the training. It explained that the new property manager had been given "brief" training by the CCTV System Manager that covered a walkthrough of the CCTV system features, operations, and the application on the mobile device. This appears to be more focused on the technical operation of the system rather than training that is designed to maintain and respect privacy. This does not suggest to us that the Strata has appointed data processors with the appropriate training to ensure compliance with their obligations under the DPA.

[123] There is no contract in place with the CCTV System Manager, although the Strata has told us that it is working with them to close out this issue.

[124] **The Strata has breached the Seventh principle by failing to have appropriate contracts in place with its data processors. It must rectify this in line with the deadline set by this enforcement order. It must also ensure that it has appointed data processors who are appropriately trained or qualified to allow it to meet its obligations under the DPA. The Strata should review our guidance on contracts between data controllers and data processors[6] for details of additional requirements to consider including in its contracts.**

[125] **The access control measures appear in general to be appropriate, and the only sharing of footage with external third parties has been with the RCIPS for the investigation of crimes. However, the Policy does appear to allow what could be excessive sharing of footage with other third parties for crime-related purposes, and it does not provide any detail around the circumstances of such sharing. If the Strata wishes to cover this potential sharing in the Policy, it must provide more detail on the circumstances in which the sharing will take place, the controls it will put in place, and how the sharing will comply with the DPA.**

C. FINDINGS AND DECISIONS

[126] Under Section 45(1) of the Data Protection Act (2021 Revision), for the reasons explained above, I make the following findings and decisions:

a) As part of its response to our questions, the Strata stated that "the system was installed prior to the DPA and none of the persons involved in the installation advised specifically on the need for appropriate policies and as we are sure you appreciate, compliance generally on island with the stringent codes and guidelines as adopted in other larger jurisdictions is a work in progress". The DPA has been in force since September 2019, so there is no excuse for compliance to still be a 'work in progress'. I believe that an enforcement order is a proportionate outcome to this investigation as there are multiple contraventions of the data protection principles that must be corrected.

[6] https://ombudsman.ky/data-protection-organisation/contracts-between-data-controllers-and-data-processors

b) The Strata has also referred, on a number of occasions, to the fact that other Strata complexes also have CCTV systems, which are perhaps being operated in a similar manner. We do not know whether that is the case. The fact is that the Ombudsman received a complaint about the system at the Pinnacle, and given the multiple issues raised, this office was bound to investigate. This order will be publicized, and will therefore inform other users of CCTV systems in Strata complexes and elsewhere of the requirements of the DPA and the rights of data subjects under it.

c) The Policy and contract documentation do not currently make it sufficiently clear who the data controller for the CCTV system is.

d) The Strata has breached the First data protection principle by failing to have an appropriate legal basis for all of the purposes listed in the Policy. In most, if not all, cases, the processing is not necessary for the performance of a contract. A number of the purposes do not meet the necessity test, although the Strata does have justifiable legitimate interests in protecting property and people from crime, and for the defense of legal claims. Where the use of the footage does not involve the processing of personal data in order to achieve the purpose, this would not be covered by the DPA and would therefore be allowable.

e) The Strata has breached the Third data protection principle as it has been processing excessive personal data in relation to those purposes which fail to meet the necessity test. It is also a breach of the third principle to capture footage from locations which are unnecessarily intrusive and not required for crime prevention.

f) The Strata is likely to be retaining personal data for longer than is necessary for the stated purposes, which is in breach of the Fifth data protection principle.

g) The Strata has breached the Sixth data protection principle, as its response to the Complainant's Section 10 notice was not valid.

h) The Strata has breached the Seventh principle by failing to have appropriate contracts in place with its data processors.

i) The access control measures appear in general to be appropriate, and the only sharing of footage with external third parties has been with the RCIPS for the investigation of crimes. However, the Policy does appear to allow what could be excessive sharing of footage with

other third parties for crime-related purposes, and it does not provide any detail around the circumstances of such sharing.

[127] Under Section 45(1) of the DPA, for the reasons explained above, I require the Strata to take the following steps as soon as practicable, but in any event no later than 30 days after the date of this Order:

a) The Policy and the contract must be reviewed to ensure that they are unambiguous as to when the CCTV Manager is acting under the instructions of the data controller. In areas where the CCTV Manager is given responsibility for carrying out certain tasks and taking decisions on behalf of the Strata, it must be made clear that ultimate authority for those decisions rests with the Strata, as data controller. Controls must be put in place to ensure that the Strata does exercise that authority, even though it is relying on the expertise of its processors. It must also be made clear that the CCTV Manager cannot use any of the images or data that are captured by the CCTV system for its own purposes.

b) The Strata must ensure that suitably detailed signage is in place at all points of entry to the property, if it is not already, and that it is reviewed regularly to ensure accuracy.

c) The Strata must review the purposes for which the footage is used and ensure that it has a legal basis for each of them. Any purposes which do not have a legal basis must be removed from the Policy. Any purposes which are retained as they do not involve the processing of personal data to meet them must be flagged as such in the Policy.

d) The cameras must be located in positions where they are necessary to meet the primary purpose of the CCTV system, which is crime prevention. Other uses of the footage captured by these cameras may be permissible, such as for the defense of legal claims, or where no personal data is being processed, but the location of the cameras should not be dictated by these other uses.

e) The locations and fields of vision of all cameras must be reviewed to ensure compliance with the Third data protection principle. Cameras covering communal areas such as the gym, pool and lounge, if they are not necessary for crime prevention, must be removed.

f) No covert monitoring has taken place, but the Policy must be made clearer about the circumstances in which it could be used, and the controls that will be in place to ensure it is carried out in compliance with the DPA.

g) Similarly, it does not appear that any monitoring of staff has taken place, but this must only be done in exceptional circumstances, when absolutely necessary, and with appropriate controls in place. The Policy must reflect this. Staff must also be made aware of any monitoring in line with the requirements of the First data protection principle, unless an exemption applies.

h) The Strata must assess how long it actually needs standard footage to be stored by assessing its use for the approved purposes. The Strata must also detail the circumstances in which data is to be retained for longer than the standard retention period, and the factors which must be considered by the CCTV Manager when they are being asked to authorize that extended retention. It must also be made clear that the ultimate decision is for the Strata to make, as data controller, even if it is asking the CCTV Manager to do so on its behalf.

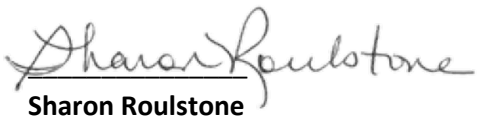
i) The Strata must review its response to the Complainant's Section 10 notice.

j) The Strata must put in place contracts with its data processors that meet, at a minimum, the requirements of Paragraph 3, Part 2 of Schedule 1 of the DPA. It must also ensure that it has appointed data processors who are appropriately trained or qualified to allow it to meet its obligations under the DPA. The Strata should review our guidance on contracts between data controllers and data processors for details of additional requirements to consider including in its contracts.

k) If the Strata wishes to cover the potential sharing of footage with other third parties for crime-related purposes in the Policy, it must provide more detail on the circumstances in which the sharing will take place, the controls it will put in place, and how the sharing will comply with the DPA.

l) The revised Policy must be submitted to this office for review once the required amendments have been made.

[128] Under Section 47, a person who receives an enforcement order under the DPA may, within 45 days of receipt and upon notice to the Ombudsman, seek a judicial review of the Order to the Grand Court.



Sharon Roulstone
Ombudsman