GIBRALTAR REGULATORY AUTHORITY

Data Protection Impact Assessment – case study guidance

Guidance on the EU General Data Protection Regulation 2016/679 and Data Protection Act 2004

28 May 2020 (v2)

Case study guidance in relation to Guidance Note IR04/17

FOREWORD

The EU General Data Protection Regulation 2016/679 (the "GDPR") came into force on 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive 95/46/EC.

Her Majesty's Government of Gibraltar amended the Data Protection Act 2004 (the "DPA") on 25th May 2018, in accordance with the introduction of the GDPR. The DPA complements the GDPR and also implements the Law Enforcement Directive 2016/680. Therefore, both the DPA and the GDPR must be read side by side.

It is important to note that the GDPR does not generally require transposition (EU regulations have 'direct effect') and automatically became law in Gibraltar. Therefore, organisations involved in the processing of personal data need to be aware of the obligations that the GDPR and/or the DPA will impose on them. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

The Gibraltar Regulatory Authority, as the Information Commissioner, is aware of the increased obligations that the GDPR and DPA place on organisations. The Information Commissioner's aim is to alleviate some of the concerns for businesses, public-sector and third-sector organisations and assist them ensure data protection compliance.

NOTE

A Data Protection Impact Assessment ("DPIA") is a procedure designed to assist organisations identify and minimise the privacy risks of new projects or policies.

Conducting a DPIA is not mandatory for all data processing. However, it is required where the data processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" as per Article 35(1) of the EU General Data Protection Regulation 2016/679 (the "GDPR") and section 73(1) of the Data Protection Act 2004 (the "DPA"). Although undertaking a DPIA is not always compulsory, organisations may find it useful to conduct one as it will ensure processing is GDPR/DPA compliant.

Note that the GDPR/DPA set out specific features that must be included in a DPIA (see Article 35(7) of the GDPR or section 73(3) of the DPA). Although these features are mandatory, the list is non-exhaustive and flexible, in that organisations may include additional features and adapt the DPIA as appropriate for the type of data used and processing intended.

Please read the Information Commissioner's (the "Commissioner") Guidance Note IR04/17 "GDPR Guidance (4) Data Protection Impact Assessment" before attempting to complete this template. [1]

Acknowledgements

Where appropriate Gibraltar's Information Commissioner will seek to ensure that locally published guidance documents are consistent with others made available by fellow Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the UK's Information Commissioner's office.

[1] Guidance Note IR04/17 "GDPR Guidance (4) Data Protection Impact Assessment" (https://www.gra.gi/dataprotection/guidance-on-the-general-data-protection-regulation/gdpr4).

SUMMARY

Using an example relating to the use of CCTV within a residential estate, this document outlines a how a DPIA process and outcome can be recorded. The document is based on the process detailed in the Commissioner's Guidance Note IR04/17 "GDPR Guidance (4) Data Protection Impact Assessment" that aims to supplement the European Data Protection Board's guidelines on Data Protection Impact Assessments. [2]

Organisations can use the approach used in this case study as guidance of the information that needs to be included in a DPIA, making adaptations where necessary depending on the circumstances of the case. The approach for the completion of the DPIA follows seven steps -

(1) identifying the need for a DPIA;
(2) describing the processing;
(3) consultation process;
(4) assessing necessity and proportionality;
(5) identifying and assessing the risks;
(6) identifying measures to reduce risks; and
(7) sign off and recorded outcomes.

The main body of the document contains a 'DPIA screening checklist' that organisations can use to identify when a DPIA is required. A further set of screening questions at Annex A may also be helpful to identify a proposal's potential impact on privacy, and thereby useful for step 1.

Further, at Annex B, a matrix is provided, which organisations may find useful to identify and assess the risks to the rights and freedoms of individuals, as required in step 5.

A DPIA should be completed at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

[2] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" (as last Revised and Adopted on 4 October 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236> Accessed 02 September 2019.

GENERAL DETAILS

Controller details	
Data controller	Sunset Estate Management Limited
Data controller contact details (name, title, telephone number and email)	Robert King (Director) RobKing--@1234.com +350 200 XXXXX
Data controller DPO or equivalent advisor[3] contact details (name, title, telephone number, email)	Matthew Lees (DPO) MatLees--@1234.com +350 200 XXXXX

Controller details (if joint controllers)	
Data controller	N/A
Data controller contact details (name, title, telephone number and email)	N/A
Data controller DPO or equivalent advisor contact details (name, title, telephone number, email)	N/A

[3] Article 37(1) of the EU General Data Protection Regulation 2016/679 ("GDPR") introduces a requirement for organisations to appoint a data protection officer ("DPO") in certain circumstances. For further assistance, see Guidance Note IR03/17 "GDPR Guidance (3) Data Protection Officer" (https://www.gra.gi/dataprotection/guidance-on-the-general-data-protection-regulation/gdpr3).

CONTENTS

1. IDENTIFY THE NEED FOR A DPIA

Identify the need for a DPIA in relation to the envisaged processing operations and purposes.[4]
Describe and record the reasons for undertaking the project i.e. explain broadly what the project aims to achieve and what type of processing of personal data it involves. ***You should also summarise why you identified the need for a DPIA. You can draw on your answers to the screening checklist in step 1 (see page 2 of this document), your answers to the screening questions at Annex A, or your own screening questions developed to suit the proposed processing.*** ***You may find it helpful to refer or link to other documents, such as a project proposal.***
Sunset Estate Management Limited (the "Data Controller"), who manage Sunset Estate (the "Estate"), is considering the installation of a CCTV system within the Estate, for the purposes of acting as a deterrent for crime, vandalism, graffiti and littering whilst improving the health and safety and security of residents and visitors. The Data Controller is looking to outsource security services, including the running of the CCTV system to Secure Watch (the "Data Processor"). The estate is comprised of one block of flats with 200 residential homes on a total of 20 floors. In the past year, communal areas of the Estate have been damaged on various occasions, for example: • The door of the lift was broken, leading to the lift being out of order for a week. • The lift was defaced with graffiti and the lift buttons were damaged. • A wall inside the garage of the estate was also defaced with graffiti. Records of all incidents have been kept, which detail the dates they occurred, the Estate's attempts to investigate the incidents and pursue any legal action where applicable and the financial impact on the Estate and subsequently the residents. The data that will be captured by the CCTV system includes images of residents and individuals visiting the Estate. In this regard, it is noted that the project will involve systematic monitoring through the CCTV system, which may capture data (i.e. visual images/video) pertaining to children and may capture incidents which involve criminal activity (although not expected/intended).

[4] Seek the DPO's advice when deciding whether a type of data processing meets the requirements for a Data Protection Impact Assessment ("DPIA"). If you already intend to do a DPIA, go straight to step 2. Following completion of the 'screening checklist' and screening questions in Annex A, if it is decided that a DPIA is not

DPIA screening checklist
(See section 3 of Guidance Note IR04/17)

Does your project involve:	Yes	No
Evaluation or scoring of personal data (including profiling and predicting)		X
Automated decision-making with legal or similar significant effects		X
Systematic monitoring (including through a publicly accessible place on a large scale[5])	X	
Sensitive data or data of a highly personal nature (including special categories of data and criminal data)		X
Data processed on a large scale	X	
Matching or combining data sets		X
Data concerning vulnerable people (including children)	X	
Innovative use or applying technological or organisational solutions		X
Processing preventing data subjects from exercising a right or using a service or contract		X
As a general rule, if you have answered **yes** to at least two of the above questions, you must carry out a DPIA.		

Note

In some cases, a data controller may have to carry out a DPIA if answering 'yes' to only one question. In this regard, please see the 'list of processing operations for which a DPIA is required' at Annex B of Guidance Note IR04/17 "GDPR Guidance (4) Data Protection Impact Assessment".

If a data controller is unsure whether a DPIA is required, the Commissioner recommends that a DPIA is carried out, as a DPIA is a useful tool that will help data controllers comply with data protection laws. In such instances, an organisation may want to consider a further set of screening questions at **Annex A** to identify a proposal's potential impact on privacy.

needed, this decision should be documented, along with the reasons for the decision, including the DPO's advice. The aim is to demonstrate that the organisation has properly considered and complied with DPIA obligations. If in doubt, the Information Commissioner (the "Commissioner") strongly recommends that a DPIA is conducted.

[5] Whilst Recital 91 of the GDPR provides some guidance in relation to large scale processing operations, the GDPR does not define what constitutes "large-scale". Therefore, the Commissioner interprets this to mean a relatively significant data processing activity, taking account of the following factors: the number of data subjects concerned (either as a specific number or as a proportion of the relevant population); the volume of data and/or the range of different data items being processed; the duration or permanence of the data processing activity; and the geographical extent of the processing activity.

2. DESCRIBE THE PROCESSING

Step 2: Describe the processing[6]

- ***How will you collect, use, store and delete data?***

Data (i.e. images of individuals) will be captured by the cameras of the CCTV System.
The Data Controller proposes to install fixed CCTV cameras -

- inside the lift (1 camera);
- on every floor opposite the lift entrance (20 cameras), therefore, this may capture hallways and some residents' entrances; and
- in the garage (capturing the entrance and the exit) and the lift area (3 cameras).

The CCTV cameras will be used for the purposes of safety, security and crime prevention.
The images will be transmitted to a digital video recorder ("DVR") and stored on its hard drive. The transmitted images can be viewed from a computer, both the computer and the DVR will be located in a locked cabinet within the Estate, which will only be accessed by authorised individuals for the purposes of accessing, viewing and extracting CCTV footage.
Subject to any incidents, CCTV footage will be recorded over after 30 days.

- ***What is the source of the data?***

Further to the information detailed under "how will you collect, use and delete data?", the personal data is collected directly from data subjects as and when they enter the CCTV System's field of view.

- ***Will you be using data processors? Will you be sharing data with anyone?[7]***

Yes, a Data Processor will be used. The authorised individuals working for the Data Controller and the Data Processor will have access to the CCTV footage. CCTV Footage will ONLY be disclosed to third parties where necessary and in connection with incidents to pursue said incidents. For example, recordings may be disclosed to the police and/or in legal proceedings. Data will not be otherwise shared.

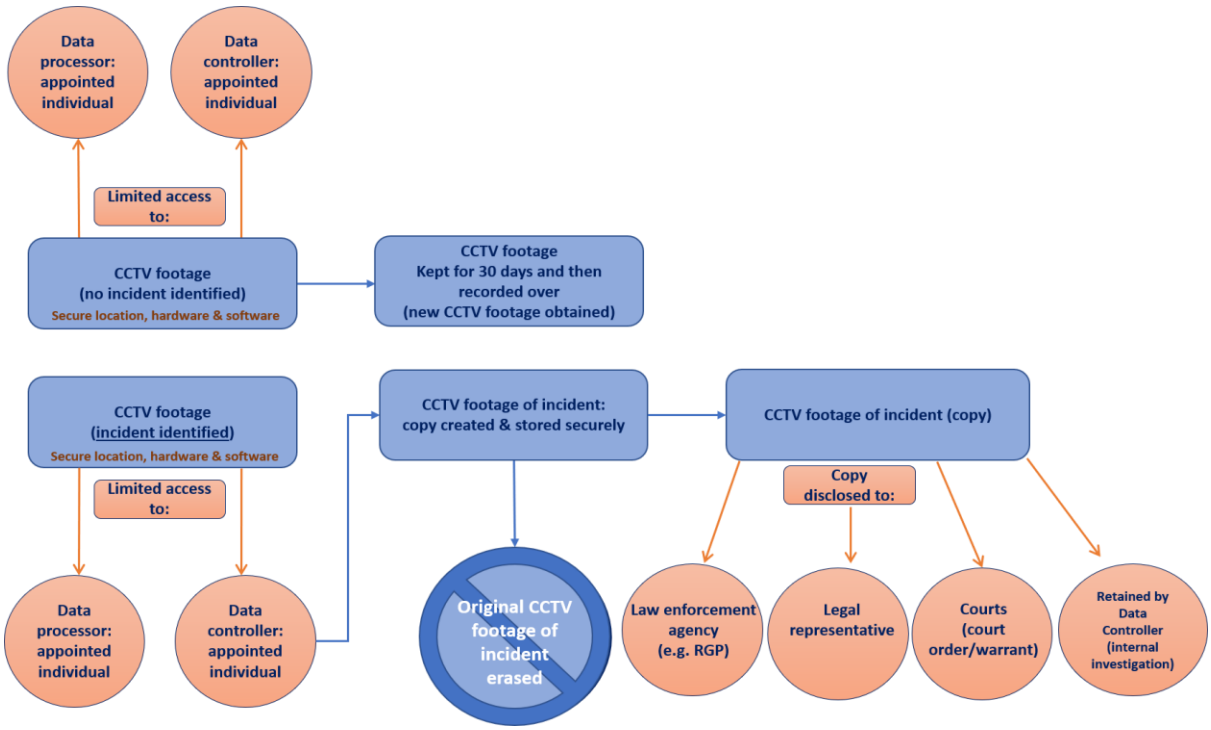
- ***What types of processing (screening criteria) identified as likely high risk are involved?***

- Systematic monitoring of individuals when in the Estate;
- data processed on a large scale; and
- data concerning vulnerable groups of people (e.g. children).

[6] Describe how and why the personal data is intended to be used. This description must include "the nature, scope, context and purposes of the processing".

[7] If the data controller is considering whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, the data controller must take into account the requirements at Article 6(4) of the GDPR.

Input information flow below:[8]



[8] Another important aspect of a DPIA is describing information flows in a project. This process can help organisations identify unforeseen or unintended uses of data, for example data sharing. Therefore, please explain and document how information will be processed, this may take the form of an information map, diagram, etc.

Describe the scope of the processing

- ***What is the nature of the data, and does it include special category or criminal offence data?***

The CCTV data includes video recordings (still images can also be taken from the video recordings). No audio data will be recorded.

No collection of special category or criminal offence data is envisaged.

- ***How much data will you be collecting and using? How often? (i.e. volume and variety of the personal data and the extent and frequency of the processing)***

The CCTV system will be capturing visual images of individuals, 24 hours a day 7 days a week.

- ***How long will you keep it? (i.e. the duration of the processing)***

The CCTV system will be in operation as stated above. Data will be retained for 30 days and then recorded over. If an incident is identified, a copy of the CCTV footage will be created and stored securely until released to the appropriate law enforcement body or requested by a legal representative and/or the Courts. The original CCTV footage of the incident will be erased. Further, the Estate, as Data Controller of the CCTV system, may retain the data in the event of an internal investigation carried out by the Data Controller in relation to the purposes of the CCTV System. A copy of the CCTV footage will be created and stored securely for the duration of the internal investigation and then erased upon conclusion. The original CCTV footage of the incident will be erased (recorded over).

- ***How many individuals are affected? (i.e. number of data subjects involved)***

The residents of the Estate (i.e. over 200 individuals) in addition to any visitors.

- ***What geographical area does it cover?***

Lifts of the Estate, floors of the Estate and garage entrance and exit, as well as lift entrance in the garage.

Describe the context of the processing

- ***What is the nature of your relationship with the individuals?***

The Data Controller looks after and maintains the common areas of the Estate building. Any issues in this regard are reported by the residents to the Data Controller.

- ***How much control will they have over their data?***

By default, individuals cannot prevent the processing if they come within the CCTV's field of view. However, the Data Controller will issue letters (the "Information Letters") to the residents prior to the installation of the CCTV system. These will detail the purpose of the CCTV system and intended processing of their personal data. This will also inform the residents of their rights under the GDPR and how these can be exercised. The Data Controller will also place appropriate CCTV signage around the Estate, with links to a privacy notice (the "Privacy Notice") that will be published online and will include additional information regarding the location of the CCTV cameras so that data subjects can more easily identify and specify the video sources related to the exercise of their rights. A paper copy of the Privacy Notice and corresponding additional information will also be available at the Data Controller's office located within the Estate.

- ***Would they expect you to use their data in this way?***

Prior to the proposal for the installation of a CCTV system, the Estate attempted to address the issues of vandalism and damage to property as well as other minor criminal activity by using less privacy intrusive methods. In first instance, the Data Controller increased the patrols of security personnel. Further, the Data Controller issued three warning letters (the "Warning Letters") to residents, detailing the implementation of penalty notices and involvement of local law enforcement authorities. The Warning Letters were issued over a period of one year, however, incidents have continued to occur at an increasing rate and reparations are resulting in an increase in service charges. An Annual General Meeting (the "AGM") was held where the introduction of a CCTV system was discussed and agreed with a significant majority. The Estate thereby considers that data subjects would expect their data to be used as proposed.

- ***Do they include children or other vulnerable groups?***

Yes, the CCTV system will capture images of children and/or other vulnerable groups visiting and/or that reside in the estate.

- ***Are there prior concerns over this type of processing or security flaws?***

The processing could be considered intrusive and/or excessive as the daily routine of individuals (e.g. entering and leaving the Estate everyday) may be recorded. Further, CCTV footage could record images of the inside of the residents' homes as some of the cameras may be capturing images of the residents' front doors and windows.

Other concerns relate to the secure processing of CCTV footage to avoid leaks of footage, which in general is increasingly being seen on social media.

- ***Is it novel in any way? (e.g. use of new technologies etc.)***

The project does not implement particularly new technology.

- ***What is the current state of technology in this area?***

This is the first time a CCTV system will be used in the Estate, however, this type of technology is widely used and proven.

- ***Are you signed up to any approved code of conduct or certification scheme?***

No relevant codes of conduct have been identified.

Describe the purposes of the processing

- ***What do you want to achieve by the processing activity?***

As stated above, the purpose is to enhance safety, security and to act as a deterrent for vandalism and crime. In particular, report incidents to the relevant authorities.

- ***What is the intended effect on individuals?***

See above and below.

- ***What are the benefits of the processing both for you and more broadly?***

The benefits include:

- Demonstrates a duty of care to both residents and non-residents.
- Enhances security within the Estate.
- Budgets/reparation costs can be reduced/deferred to other more beneficial projects.
- Provides assistance in the detection and prevention of vandalism/crime.

3. CONSULTATION PROCESS

Step 3: Consultation process
Consider how to consult with relevant stakeholders[9]
• ***Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.[10]*** Residents were invited to attend the AGM in which the Data Controller discussed the proposed installation of a CCTV system. Residents approved the implementation of the CCTV system in a vote, records of this have been retained.
• ***Who else do you need to involve within your organisation?*** Advice has been sought and the DPO will monitor the performance of the DPIA in consultation with the Data Controller.
• ***Do you need to ask your processors to assist?[11]*** The Estate sought the views/suggestions of the Data Processor regarding the installation of a privacy friendly CCTV system. The advice will be incorporated into the procedures and policies detailed in step 6.
• ***Do you plan to consult information security experts, or any other experts?*** Currently, advice will not need to be sought from any other experts.

[9] All relevant internal stakeholders should be consulted, in particular anyone with responsibility for information security. It is also recommended that the organisation consider seeking legal advice or advice from other independent experts such as IT experts, sociologists or ethicists where appropriate. However, there are no specific requirements to do so.

[10] As part of the DPIA process, an organisation must seek and document the views of individuals (or their representatives) unless there is a good reason not to. In most cases it should be possible to consult individuals in some form. However, if it is decided that this is not appropriate, the organisation should record this decision as part of the DPIA, with a clear explanation. For example, the organisation may be able to demonstrate that consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable. If the DPIA covers the processing of personal data of existing contacts (for example, existing customers or employees), the organisation should design a consultation process to seek the views of those particular individuals, or their representatives. If the DPIA covers a plan to collect the personal data of individuals that have not yet been identified, there may be a need to carry out a more general public consultation process, or targeted research. This could take the form of market research with a certain demographic or contacting relevant campaign or consumer groups for their views. If the DPIA decision differs from the views of individuals, the organisation would need to document the reasons for disregarding their views.

[11] If a data processor is used, the organisation may need to ask them for information and assistance. Contracts with data processors should require them to assist.

4. ASSESS NECESITY AND PROPORTIONALITY

Step 4: Assess necessity and proportionality[12]
• ***What is the lawful basis for processing?***[13] The processing of personal data in this case relies on 'legitimate interests' of the data controller' under Article 6(1)(f) of the GDPR.
• ***If you are relying on Article 6(1)(f) of the GDPR (i.e. legitimate interests as a lawful basis), have you considered, and can you demonstrate that:*** Yes ○ ***you are pursuing a legitimate interest, i.e. no other lawful basis applies (the purpose test);*** Purpose test conducted and details recorded. ○ ***the processing is necessary to achieve the purpose, i.e. you cannot reasonably achieve the same result in another less intrusive way (the necessity test); and*** Necessity test conducted, details of less intrusive (but ineffective) methods previously implemented recorded. Result cannot be achieved through other methods. ○ ***the individuals' interests, rights and freedoms do not override the organisation's interests (the balancing test).***[14] Balance test conducted and details recorded.

[12] To complete this part of the DPIA, an organisation should consider how their plans help achieve their purpose and if there are any other reasonable ways to achieve the same result. To evaluate whether the impact on privacy is proportionate to the outcomes which will be achieved, organisations should consider, amongst other requirements, Article 6 (and 9) of the GDPR, Article 5(1)(b), 5(1)(c) and 5(1)(e) of the GDPR.

[13] For further assistance, see Guidance Note IR01/18 "GDPR Guidance (6) Identifying the 'Lawful Basis'" (https://www.gra.gi/gdpr-6-identifying-the-lawful-basis).

[14] Note that if you are a public authority you cannot use legitimate interests as your lawful basis if the processing is in the performance of your tasks as a public authority. Further, in practice, legitimate interests is unlikely to be appropriate for any processing purpose where another basis objectively applies. It is likely to be most appropriate where individuals' data is used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing. If individuals would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the organisation's legitimate interests. Once an organisation has demonstrated that they can rely on legitimates interest (i.e. by completing the three-part test) a record of the legitimate interests assessment should be kept to help demonstrate compliance, and details of the legitimate interests must be included in the organisation's privacy notice.

- ***If you are relying on Article 6(1)(a) of the GDPR (i.e. consent as a lawful basis) can you demonstrate that:***

N/A

  - ***it is freely given, specific, informed, unambiguous and withdrawn at any time;***

  - ***details of consent have been recorded and consent is refreshed if anything changes.***[15]

- ***How does the processing actually achieve your purpose?***

The cameras are located in areas that have been vandalised repeatedly. These will act not only as a deterrent for future incidents but will also allow individuals to be identified should there be future incidents.

- ***Is there another way to achieve the same outcome?***

Other options have been explored i.e. the increase in security personnel patrols and the Warning Letters issued over the course of a year. Installing a CCTV system is the next step in order to attempt to further prevent the said incidents.

- ***How will you prevent function creep? (the gradual widening of the use of technology or system beyond the purpose for which it was originally intended especially when this leads to potential invasion of privacy)***

It shall not be technically possible to amend the Cameras' field of view without the approval of the Data Controller and the involvement of the Data Processor. Access to the CCTV footage will be strictly controlled. Only three senior ranking and designated individuals at the Data Controller shall have access to the CCTV footage on the designated computer. Any requests for further use will automatically be rejected.

- ***How will you ensure data quality and data minimisation?***

In regard to data quality, periodic reviews (every 6 months) of the data captured as well as the equipment used will be carried out to ensure appropriate quality and accuracy.

In regard to data minimisation, the personal data will only be processed for the purposes of:

  - Security of the property i.e. to protect the property from vandalism/damage/crime;
  - CCTV footage will only be accessed when an incident that relates to the purposes identified is reported. Requests to use the footage for other purposes will be rejected.
  - The Data Controller will ensure that the field of view of each CCTV camera is limited to what is absolutely necessary (see step 6).

- ***What information will you give individuals?***

[15] The GDPR sets a high standard for consent, an organisation must ensure that their consent mechanisms are compliant, please see Guidance Note IR01/19 "GDPR Guidance (13) Guidance on Consent" (https://www.gra.gi/gdpr-13-guidance-on-consent).

Residents and visitors will be provided information required under Article 13 of the GDPR through the CCTV signage. Further, information about data protection rights will be included in the Privacy Notice, which is available online and in a non-digital format as described in step 2 above (also see step 6).

- ***Please include how data protection compliance will be ensured and in particular, please include relevant details of:***

  - ***how data quality will be achieved/ensured;***
    The Data Controller will review the CCTV system every 6 months to ensure that:
    - images are clear and accurate for evidential purposes;
    - features on the hardware and software are accurate;
    - any damaged or deteriorating hardware or software is either repaired or replaced to maintain the integrity of the images;
    - and the appropriate type of hardware (suitable for the physical area which the camera is recording) is used. See step 6.

  - ***how information rights will be implemented and supported;***
    The Privacy Notice will include information detailing how data subjects may exercise their rights, as well as the additional information regarding the location of the CCTV cameras as referred to in step 2 above. A Data Protection Policy will detail the internal procedures in place to deal with requests (see step 6).

  - ***measures to ensure that data processors (where relevant) are compliant with data protection obligations;***
    The Data Controller will ensure that contracts with the Data Processor include, as a minimum, the information detailed in Article 28(3) of the GDPR. For example:
    - the subject matter and duration of the processing;
    - the nature and purpose of the processing;
    - the type of personal data and categories of data subject;
    - the obligations and respective responsibilities of the controller and processor; and
    - information regarding the organisational and technical security measures in place that will protect the personal data.

  - ***safeguards for international transfers (where relevant).***
    N/A

5. IDENTIFY AND ASSESS RISKS

Step 5: Identify and assess risks[16]

Consider the potential impact on individuals and any harm or damage your processing may cause – whether physical impacts (e.g. health and safety), moral /emotional impacts (e.g. distress) or material impacts (e.g. financial loss). In particular, look at whether the processing could contribute to –

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data).

To assess whether the risk is a high risk, you need to consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm may still count as high risk.

You must make an objective assessment of the risks. It is helpful to use a structured matrix to think about likelihood and severity of risks, an example is provided in **Annex B**.[17]

[16] Assess the potential privacy issues associated with a project. Risks to individuals can be categorised in different ways and it is important that all types of risks are considered, ranging from physical safety, material impacts or moral impacts. This part of the DPIA must also specifically include an evaluation of the risks posed to the rights of data subjects (Articles 12 to 22 of the GDPR) in relation to the proposed processing.

[17] The matrix in Annex B is an example of how risk may be assessed in a structured way. However, organisations may use a different method that can be adapted for this purpose. Organisations may also want to consider their own corporate risks, such as the impact of regulatory action, reputational damage or loss of public trust.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood or harm** (*remote, possible or probable*)	**Severity of harm** (*minimal, significant or severe*)	**Overall risk** (*low, medium or high*)
The intended processing has been assessed in relation to the relevant principles relating to the processing of personal data (Article 5 of the GDPR) and the rights of the data subject (Articles 12 to 22 of the GDPR). Potential breaches of the GDPR have been identified and evaluated in terms of the potential impact this can have on an individual.			
<u>Principles</u>			
• <u>Lawfulness, fairness & transparency:</u> ➢ There is a risk that individuals might be unaware of the CCTV recording taking place. If individuals are not appropriately notified, the Data Controller may not be processing personal data fairly and transparently. ➢ Risk identifier: transparency. ➢ Potential impact: loss of confidentiality (moral impact).	Possible	Minimal	**Low**
• <u>Collected for a specified, explicit and legitimate purpose (purpose Limitation):</u> ➢ Accessing and/or using CCTV footage for purposes other than safety, security and crime prevention. ➢ Risk identifier: improper use. ➢ Potential impact: loss of control over the use of personal data (moral impact).	Possible	Significant	**Medium**
• <u>Adequate, relevant and limited to what is necessary (data minimisation):</u> ➢ Issue raised above, in relation to whether residents' entrances will be captured by the CCTV cameras installed on each floor. This could be intrusive as residents may not expect a CCTV system to capture images of their doorways and potentially inside their house. ➢ Risk identifier: excessive recording. ➢ Potential impact: loss of confidentiality (moral impact).	Possible	Significant	**Medium**

• Accurate and kept up to date (accuracy) ➢ Risk that the CCTV footage captured may not be clear and accurate. For example, the resolution could be too low, this may not be appropriate to identify incidents in the communal areas, also it is possible to have incorrect time and date stamps. ➢ Risk identifier: accuracy. ➢ Potential impact: inability to exercise privacy rights and may affect the ability to report incidents (moral/physical impact).	Possible	Minimal	**Low**
Retention of personal data (storage limitation): ➢ If polices are not in place in regard to the retention of personal data, then the processing purposes may not be met. ➢ Risk identifier: inadequate retention. ➢ Potential impact: loss of control of the use of personal data (moral impact).	Possible	Minimal	**Low**
Security of personal data Appropriate technical and organisational security measures (integrity and confidentiality): ➢ Using inadequate hardware and software, including for example inadequate antivirus software and firewalls, and/or the user's lack of training or guidance may lead to unauthorised or unlawful processing, and accidental loss, destruction or damage. E.g. a lack of security measures when responding to requests for CCTV footage from a law enforcement body, a legal representative and/or the courts could lead to unlawful disclosure of personal data. ➢ Risk identifier: technical & organisational security measures. ➢ Potential impacts: inability to exercise rights, loss of control over the use of personal data, discrimination, reputational damage, loss of confidentiality, etc. (moral impact).	Possible	Significant	**Medium**
Rights			

• <u>The right to be informed (Articles 13 and/or 14 of the GDPR):</u> ➢ Individuals need to be made aware of the CCTV system and will need to be provided with the information in Article 13 of the GDPR. However, it is not always feasible/possible to include the information specified in Article 13 of the GDPR in a CCTV sign. ➢ Risk identifier: providing notice. ➢ Potential impact: loss of confidentiality (moral impact) inability to exercise rights (moral/physical impact).	Possible	Minimal	**Low**
• <u>The right of access (Article 15 of the GDPR and responding in accordance with Article 12 of the GDPR):</u> ➢ By default, this right is the most likely to be invoked by individuals captured on the CCTV systems. If there are no documented policies in place or processes that facilitate access, allowing the Data Controller and Data Processer to extract and provide the said data, the Data Controller may breach the GDPR. Additionally, mistakes can be made when providing the personal data to the individual i.e. leaking third party data. ➢ Risk identifier: access. ➢ Potential impact: inability to exercise privacy rights, could affect ability to report an incident, loss of confidentiality of third parties (moral/physical impact).	Probable	Minimal	**Low**
• <u>The right to rectification (Article 16 of the GDPR), the right to erasure (Article 17 of the GDPR), the right to restrict processing (Article 18 of the GDPR) the right to object (Article 21 of the GDPR)</u>: ➢ These rights are less likely to be invoked. However, lack of recorded policies and procedures to deal with such requests may result in the Data Controller breaching the GDPR. ➢ Risk identifier: rectification, erasure, restrict-processing, objection. Potential impact: inability to exercise privacy rights (moral/physical impact).	Possible	Significant	**Medium**

• The right to data portability (Article 20 of the GDPR) and rights in regard to automated individual decision making, including profiling (Article 22): ➢ Not applicable to the intended processing.	N/A	N/A	**N/A**
• Other risks that can impact individuals: ➢ Breakdowns of the CCTV equipment, due to system failure or general damage. ➢ Risk identifier: equipment breakdown. ➢ Potential impact: inability to exercise rights and loss of personal data (moral/physical impact).	Possible	Significant	**Medium**

6. IDENTIFY MEASURES TO REDUCE RISKS

Step 6: Identify measures to reduce risk				
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.				
Risk Identifier	**Options to reduce or eliminate risk**	**Effect on risk** (eliminated, reduced, accepted)	**Residual risk** (low, medium, high)	**Measure approved** (yes/no)
Transparency	Prior to CCTV System installation: AGM with records of the vote (referred to above), and the Information Letters that will be issued (referred to above). This was also provided in writing within the Information Letters. CCTV signage to be placed in prominent positions within the Estate and prior to entering an area in which the CCTV cameras are in operation. The signs will include the following information - • the identity of the data controller; • the purposes of the processing and the lawful basis for the processing; • categories of personal data processed; and • the DPO'S contact details; and a link to the Privacy Notice (which is available on the Estate's website and in a non-digital format at the Data Controller's office) where all the information referred to in Article 13 of the GDPR will be included.	**Reduced**	**Low**	**Yes**

Improper Use	Requests to use the footage for other purposes other than those defined in the Data Controller's Privacy Notice (or in relation to a data subject's rights), will be rejected. Further, see the options detailed under 'technical and organisational security measures' below.	**Reduced**	**Low**	**Yes**
Excessive recording	Field of view of the CCTV cameras only to capture communal areas of the Estate, i.e. residents' door entrances, windows, etc. will not be captured. Further, areas used for leisure such as the children's park and other seating areas will not be captured. Where the field of view cannot be adjusted, technology will be used to blur out any areas that the CCTV would otherwise capture. The Data Controller will review the camera's field of view on an annual basis. It shall not be technically possible to amend the Cameras' field of view without the approval of the Data Controller and the involvement of the Data Processor. Access to the CCTV footage will be strictly controlled. Only three senior ranking and designated individuals at the Data Controller shall have access to the CCTV footage on the designated computer.	**Reduced**	**Low**	**Yes**
Accuracy	The Data Controller will review the CCTV system every 6 months to ensure that: • images are clear and accurate for evidential purposes; • features on the hardware and software are accurate;	**Reduced**	**Low**	**Yes**

	• any damaged or deteriorating hardware or software is either repaired or replaced to maintain the integrity of the images; and • the appropriate type of hardware (suitable for the physical area which the camera is recording) is used.			
Inadequate retention	Documented retention policy (detailed within the Data Protection Policy) states that: • After 30 days the CCTV footage is automatically recorded over with newly obtained footage. • If an incident is identified, a copy of the CCTV footage will be created and stored securely until the Data Controller's investigation into an incident (relating to the purposes of the CCTV system) has concluded or until this is released to the appropriate law enforcement body, legal representative or the Courts. • The original CCTV footage of the incident will be erased. See step 2 'describe the nature of the processing'.	**Reduced**	**Low**	**Yes**
Technical and organisational security measures	The Data Controller will implement the below to comply with this principle: • Ensure that the contracted Data Processor requires their employees to undertake data protection training. • A contract with the Data Processor (see step 4 'describe compliance and proportionality measures' for specific details). • Ensure that that the CCTV hardware and viewing location is secure. • Have physical and electronic access controls in place (i.e. password protection and	**Reduced**	**Low**	**Yes**

	identity verification, physical locks, access logs, etc.) which will ensure that only designated individuals have access to the personal data. • A written Data Protection Policy will also detail the procedures in place to ensure that the above mentioned physical and electronic access controls are implemented effectively (e.g. procedures relating to the granting, changing and revoking of access, procedures regarding password complexity and change frequency, as well as procedures for the reviewing of access logs). • A written Data Protection Policy is to be made available to employees/members of the Data Controller. • All individuals at the Data Controller with access to the CCTV Footage shall be given data protection and privacy awareness training (annually). • No single person shall have access to the CCTV footage. A two-man access control system shall be implemented: o One designated individual at the Data Controller shall be in possession of the password used to access the only computer which has the software required to access the CCTV footage recorded. o Another designated individual at the Data Controller shall have the password to login to the aforementioned software to view the footage.			

	• A detailed log will be kept of every time CCTV footage is accessed, disclosed and/or otherwise used. • Procedure (recorded in the Data Protection Policy) for the disclosure of CCTV footage to appropriate law enforcement bodies, legal representatives and/ or the Court. Such requests should be made in writing to the Data Controller and be authorised by at least two individuals of senior ranking within that body/organisation. • A separate CCTV camera that monitors access to the room where the abovementioned computer is located will be used to further protect against unauthorised access. This will only be accessible by a separate individual at the Data Controller.			
Providing notice	See options outlined under 'transparency' above, i.e. appropriate CCTV signage.	**Reduced**	**Low**	**Yes**
Access	Information about how to submit a subject access request will be included in the Privacy Notice, with directions to the procedures for requests. In addition, the additional information regarding the location of the CCTV cameras can be used by data subjects to help make their requests. In regard to the internal procedure, this is documented within the Data Protection Policy. Any access to the CCTV footage or extraction of data must be done in compliance with the measures detailed in the Data Protection Policy, as outlined above under 'technical and organisational security measures' (e.g. register logs should include	**Reduced**	**Low**	**Yes**

	how/when/to whom data is disclosed in response to a subject access request). Further, two of the three senior ranking and designated individuals at the Data Controller shall review and approve the release of CCTV footage in response to a subject access request.			
Rectification, erasure, restrict-processing, objection.	Information about other data protection rights will be included in the Privacy Notice, with directions to any respective procedures in place for individuals to exercise their rights. The additional information regarding the location of the CCTV cameras can also be used to assist with such requests. Further, internal procedures to deal with each of these requests will be documented within the Data Protection Policy.	**Reduced**	**Low**	**Yes**
Equipment breakdown	Apart from the contract between the Data Controller and Data Processor (detailed in step 4 'describe compliance and proportionality measures') there will be a service contract that will cover maintenance procedures/obligations.	**Reduced**	**Low**	**Yes**

7. SIGN OFF AND RECORD OUTCOMES

Step 7: Sign off and record outcomes[18]		
Item	**Name/ position/ date**	**Notes**
Measures approved by:	Robert King Director 12/08/2019	
Residual risks approved by:	Robert King Director 12/08/2019	
DPO advice provided:	Matthew Lees DPO 12/08/2019 DPO	
Summary of DPO advice: Clear signage must be put up showing that a CCTV system is in operation with all relevant details of the Data Controller to ensure full transparency. Ensure there are strict procedures in place for the disclosures to occur in limited and controlled circumstances. In such cases, requests should be made in writing to the Data Controller and be authorised by an individual of senior ranking within that body/organisation. Ensure there are strict procedures in place for the disclosure of CCTV footage in response to subject access requests from individuals.		
DPO advice accepted or overruled by:	Accepted by Robert King	*If overruled, you must explain your reasons*
Formal validation of the DPIA: The Director of the company, Sunset Estate Management Limited validates this DPIA for the processing of personal data through the use of the CCTV system which will be installed throughout Sunset Estate. The controls planned for complying with data protection and for addressing the risks to privacy of data subjects have been deemed acceptable. This DPIA will be kept under review and the process will be repeated if there is a substantial change to the nature, scope, context or purposes of the said processing. **Validated by**: Robert King		

[18] As part of the sign-off process, an organisation should seek and document DPO advice on whether the processing is compliant and can go ahead. If their advice is not followed, an organisation must record the reason why. Reasons for going against the views of individuals or other consultees should also be recorded.

Step 3 Consultation responses reviewed by:	Robert King	*If your decision departs from individuals' views, you must explain your reasons*
Comments: Residents approved the installation of the CCTV system as recorded in AGM vote.		
Is prior consultation with the GRA necessary?[19]	No	*The Commissioner must be consulted if residual risks are high and you are unable to mitigate risks when conducting the DPIA. Record decision below.*
Comments: Residual risks are not high. The controls planned for complying with the fundamental principles underpinning privacy protection and for addressing the risks to privacy of data subjects have been deemed acceptable.		
This DPIA will be kept under review by:[20]	Robert King & Mathew Lees	*The DPO should also review ongoing compliance with DPIA*
Comments:		

Document history			
Version number	**Summary of change**	**Reviewer** (name and role)	**Date**
V1	N/A	Robert King Director	13/09/2019

[19] If the results of step 6 still indicate that there will be a high risk to the rights and freedoms of individuals, the organisation will need to consult the Commissioner's office before they can proceed with the processing. When consulting the Commissioner's office, the data controller should provide the information detailed under Article 36(3) of the GDPR.

[20] Article 35(11) of the GDPR requires the data controller to carry out a review to assess if processing is performed in accordance with the DPIA, at least when there is a change of the risk represented by processing operations.

ANNEX A

Screening questions to identify a proposal's potential impact on privacy

1. Will the project involve the collection of new information about individuals?
   Answer: Yes, CCTV recordings of individuals within the Estate have not been captured before.

2. Will the project compel individuals to provide information about themselves?
   Answer: Individuals do not have a choice to provide the information.

3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
   Answer: In certain circumstances, yes. Information could be provided to law enforcement bodies, legal representatives or the Courts.

4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
   Answer: Yes.

5. Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
   Answer: No. However, a CCTV system has not been previously installed.

6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
   Answer: Yes, see answer to question 3.

7. Is the information about individuals particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
   Answer: Potentially, see answer to question 3.

8. Will the project require you to contact individuals in ways which they may find intrusive?
   Answer: Not really.

9. Has a retention period or policy been determined? Is it necessary to keep this personal data for the specified time period? For example, individuals might expect such personal data to be available for a short period of time, after which it would be erased.
   Answer: It is in the process of being determined.

10. Have you identified the assets on which the personal data will rely?
    Answer: Yes.

ANNEX B

Matrix

Severity of impact				
	Severe	**Low risk**	**High risk**	**High risk**
	Significant	**Low risk**	**Medium risk**	**High risk**
	Minimal	**Low risk**	**Low risk**	**Low risk**
		Remote	Possible	Probable
		Likelihood of harm		

IMPORTANT NOTE

This document is purely for guidance. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi