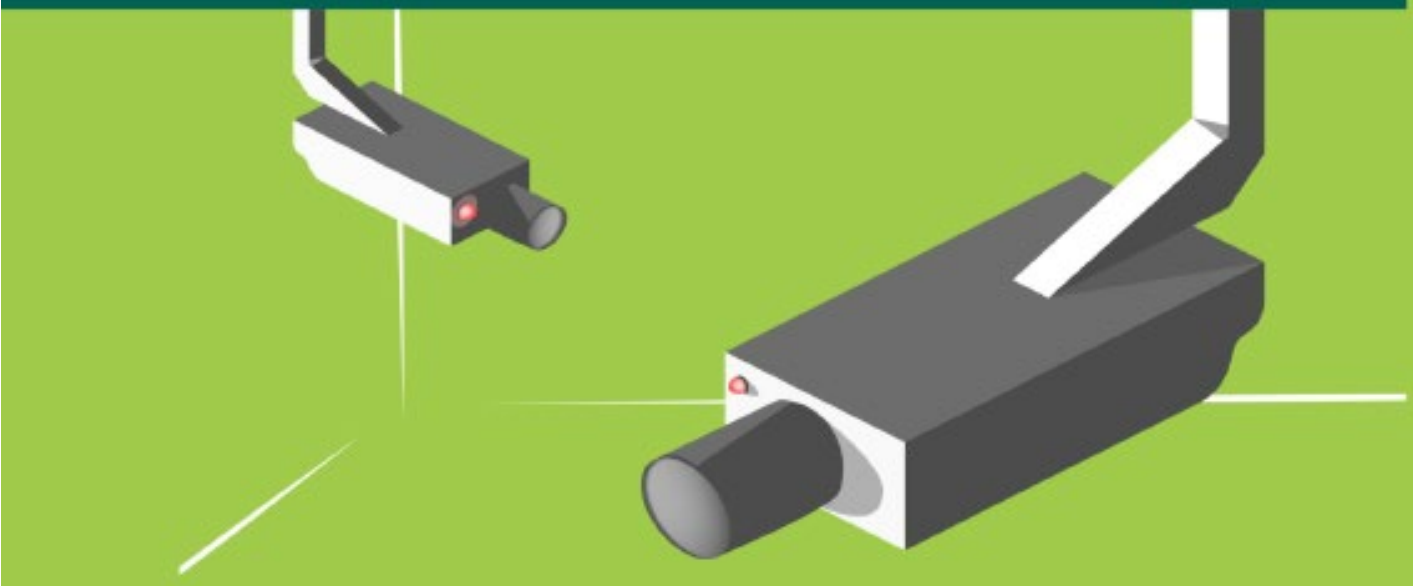
CCTV



Guidance for Data Controllers

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Guidance on the Use of CCTV – For Data Controllers

Contents

Introduction

This guidance is intended to assist owners and occupiers of premises, in particular those that are workplaces or are otherwise accessible to the public, to understand their responsibilities and obligations regarding data protection when using CCTV.

Any person or organisation that collects and processes the personal data of individuals is considered a 'data controller'.[1] For this reason, any usage of a CCTV system must be considered in light of the obligations imposed by data protection legislation on data controllers, and implemented in accordance with the principles of data protection.

The use of CCTV systems has expanded significantly in recent years, due to the increased sophistication of the technology and its affordability. CCTV systems have legitimate uses in securing premises, supporting workplace safety management, and

[1] See Article 4(7) GDPR

aiding in the prevention and detection of crime. However, unless CCTV is used proportionately, it can give rise to legitimate concerns of unreasonable and unlawful intrusion into the data protection and privacy rights of individuals and that excessive monitoring or surveillance may be taking place.

Data controllers should be aware that footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law. Where processes are used to obscure or de-identify individuals from CCTV footage, the footage or images are still considered personal data if it is possible to re-identify the individuals. Further, if footage or images are initially captured in an identifiable form and then irreversibly de-identified, data protection law will still cover the processing up to the point of anonymisation.

Before installing a CCTV system, potential data controllers should consider the following questions. These issues, and others, are expanded upon in more detail in these guidelines.

CCTV Checklist

- ✓ **Purpose**: Do you have a clearly defined purpose for installing CCTV? What are you trying to observe taking place? Is the CCTV system to be used for security purposes only? If not, can you justify the other purposes? Will the use of the personal data collected by the CCTV be limited to that original purpose?
- ✓ **Lawfulness**: What is the legal basis for your use of CCTV? Is the legal basis you are relying on the most appropriate one?
- ✓ **Necessity**: Can you demonstrate that CCTV is necessary to achieve your goal? Have you considered other solutions that do not collect individuals' personal data by recording individuals' movements and actions on a continuous basis?
- ✓ **Proportionality**: If your CCTV system is to be used for purposes other than security, are you able to demonstrate that those other uses are proportionate? For example, staff monitoring in the workplace is highly intrusive and would need to be justified by reference to special circumstances. Monitoring for health and safety reasons would require evidence that the installation of a CCTV system was proportionate in light of health and safety issues that had arisen prior to the installation of the CCTV system. Will your CCTV recording be measured and reasonable in its impact on the people you record? Will you be recording customers, staff members, or the public? Can you justify your use of CCTV in comparison to the effect it will have on other people? Are you able to demonstrate that the serious step involved in installing a CCTV system that collects personal data on a continuous basis is justified? You may need to carry

out a Data Protection Impact Assessment to adequately make these assessments.

- ✓ **Security**: What measures will you put in place to ensure that CCTV recordings are safe and secure, both technically and organisationally? Who will have access to CCTV recordings in your organisation and how will this be managed and recorded?
- ✓ **Retention**: How long will you retain recordings for, taking into account that they should be kept for no longer than is necessary for your original purpose?
- ✓ **Transparency**: How will you inform people that you are recording their images and provide them with other information required under transparency obligations? Have you considered how they can contact you for more information, or to request a copy of a recording?

Recommended Data Protection Policy

Best practice is to set out your position on the issues surrounding the use of CCTV in the form of a CCTV Data Protection Policy. The implementation of appropriate policies can be a key measure, where necessary proportionate in relation the data processing activity taking place.[2] A good policy will set out the reasons why you have decided to implement the use of CCTV and how you will manage it. The scale of the CCTV system and its impact on individuals whose images may be captured will help determine the level of detail that should be included in the CCTV policy and the manner in which the policy may be brought to the attention/made available to individuals.

Any CCTV policy that relates to a place of work should be brought to the attention of employees so that they are fully informed about the processing of their personal data by this means. A policy can be published on an official website to inform members of the public who may attend the premises and answer their questions about how you use CCTV. It will also assist the Data Protection Commission (DPC) in understanding how you have applied the principles relating to processing of personal data to your use of CCTV in the event of an investigation or audit.

Any policies should also be reviewed on a regular basis to ensure that they are being applied as intended and are adapted in light of any relevant changes in circumstances. The situation that originally necessitated the installation of CCTV may have changed, requiring a reassessment of the necessity and extent of its ongoing use.

[2] See Article 24(2) GDPR

Purpose of Utilising CCTV

The principles of data protection require that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*".[3] Personal data should not be collected on a 'just-in-case' basis, but only where there is a clearly identified purpose. This clarity of purpose ensures that data controllers, and their employees, understand why personal data are being collected and processed. It can also serve to address the concerns of individuals when they understand the purpose for which their personal data are being processed.

The first step to implementing the use of CCTV is to identify clearly the purpose or purposes for doing so. The purposes for installing CCTV can be varied, such as ensuring the security of premises, aiding in the prevention and detection of theft and other crimes, and supporting the maintenance of health and safety standards in the workplace. It will often be the case that more than one purpose applies to a situation, but it is important that these be identified at the outset.

Lawfulness of Processing

As with any processing of personal data, the recording of identifiable images of persons must have a legal basis under the data protection legislative frameworks. Having identified a purpose, or purposes, for installing CCTV, the owner/occupier of a premises which installs a CCTV system must also identify an appropriate legal basis for the processing of personal data that will take place.

The consent of an individual to the processing of his or her personal data can provide a legal basis to process data;[4] however, this is unlikely to apply to most uses of CCTV as it will be very difficult to obtain the freely given consent of everyone likely to be recorded.

For public authorities, the use of CCTV may have a legal basis where it is necessary to carry out a task in the public interest, or in the exercise of official authority.[5] Law enforcement agencies may have a legal basis to use CCTV for the prevention, investigation, detection or prosecution of criminal offences under the Law Enforcement Directive.[6] This type of usage is addressed in more detail in the guidance on the DPC website on processing for law enforcement purposes.

[3] See Article 5(1)(b) GDPR
[4] See Article 6(1)(a) GDPR
[5] See Article 6(1)(e) GDPR
[6] See Directive (EU) 2016/680, the 'Law Enforcement Directive' or 'LED', as transposed into Irish law by the Data Protection Act 2018, in particular Part 5 of that Act

Often, CCTV processing may be carried out by the owners and occupiers of premises in pursuit of their legitimate interests in protecting their property and goods and maintaining the safety of persons using their buildings and environs. Such legitimate interests (either of the data controller itself or of a third party) may provide a legal basis for the processing of personal data, provided that the interests of the data controller or third party are balanced with and not overridden by those of the individuals whose personal data are being processed.[7] When relying on legitimate interests as a legal basis to utilise CCTV, the data controller should be able to demonstrate that it is genuinely in their interests to do so, that it is necessary to achieve their identified purpose(s), and that it does not have a disproportionate impact on the individuals whose personal data will be processed. These concepts are expanded upon in the next section.

Necessity and Proportionality

A data controller must be able to justify the use of a CCTV system as both necessary to achieve their given purposes and proportionate in its impact upon those who will be recorded. Necessary processing using a CCTV system means more than the CCTV system being merely helpful to achieve a purpose. The data controller must be able to demonstrate why the use of a CCTV system is necessary for the purpose concerned. An assessment of the situation leading to the decision to install CCTV and of the practical implications of its use will assist in determining whether it is justified.

Assessing the necessity of CCTV should take into account the principle of 'data minimisation', which requires that the least amount of personal data should be processed to achieve a purpose, and that if possible the processing of personal data should be avoided. If other actions such as supervision or the deployment of security staff, which do not involve the processing of personal data, have proven ineffective, this may indicate that the installation of CCTV is a proportionate response.

Proportionality means that any processing of personal data must be measured and reasonable in terms of its objectives. The assessment of the proportionality of the use of CCTV should take into account factors such as the size of the area to be covered and, consequently, the number of cameras that will be employed. Bearing in mind the highly intrusive nature of CCTV cameras, and that staff monitoring using a CCTV system should only occur in special circumstances, employers should consider the number of employees who may be affected by the deployment of CCTV cameras for other purposes in the workplace environment and the extent to which they will be monitored during the course of their work. The extent to which public areas may be under surveillance and monitoring of the public will take place should be assessed, including

[7] See Article 6(1)(f) GDPR

whether young or vulnerable people may be affected. In all cases the impact of CCTV recording on the expectation of privacy that people may have when they are on the premises needs to be taken into account.

Dependent upon these factors, the assessment can be scaled appropriately; to adequately assess the use of a large-scale CCTV system will likely require a data protection impact assessment (DPIA), particularly if the system provides, "systematic monitoring of a publicly accessible area on a large scale".[8] Carrying out a successful DPIA involves engaging with stakeholders. In the employment context, this could include trade union or safety representatives. In a publicly accessible area that may be used by children, it may be of benefit to canvass the opinion of parents before implementing a CCTV programme. The extent to which children or young people are present at a premises such as a school or youth club, should also have a bearing on any consideration of the use of CCTV. Further guidance on conducting data protection impact assessments can be found on the DPC's website.

The assessment process also provides an opportunity to consider mitigating factors than can reduce the impact of processing on the individuals concerned. For example, if cameras are only switched on to protect a premises outside of business hours, this will reduce the scale of data processing taking place. Avoiding the placement of cameras in areas where people have greater expectations of privacy, such as restrooms, will further reduce the intrusive impact of the system.[9]

If an organisation has appointed a Data Protection Officer (DPO), they should be consulted in relation to the carrying out of any data protection impact assessments.

Necessity and Proportionality Assessment - Examples

These example scenarios are intended to indicate the level of assessment that would be appropriate when considering the implementation of CCTV in different situations. In all cases, it is the responsibility of the CCTV user to justify its implementation on the basis of necessity and proportionality. The assessment of whether the implementation of a CCTV system is justified, should be undertaken in a balanced manner, giving full consideration to all alternative options that would assist in achieving the same purpose.

[8] See Article 35(3)(c) GDPR

[9] See section in these guidelines on the use of CCTV in areas of an increased expectation of privacy

Example 1: The owner of a convenience shop intends to install a CCTV system to aid in the prevention and detection of thefts and to protect the security of the premises at night. The shop, along with others in the area, has been subject to robberies and shoplifting in the recent past. The shopkeeper identifies the prevention and detection of crime, and the safety of staff members as the purposes for installing CCTV. The necessity of using CCTV is justified by the shopkeeper based on the ongoing threat of crime and the lack of viable alternative solutions.

The shopkeeper decides that internal cameras will cover the publicly accessible area of the shop where shoplifting has taken place in the past, and the till area where staff are at risk of robbery. An external camera will be focussed on the door of the premises. When deciding on the positioning of the cameras, the shopkeeper avoids recording in areas that employees may use for their breaks, and ensures that the external camera is focused on the entrance to the shop and is aimed away from the public street.

Given the limited processing that occurs it is likely that this processing does not present a high risk to individuals' rights and freedoms. As a result, this type of installation will not require an in-depth analysis of its data protection impact. The purpose for the system and the shopkeeper's legitimate interest in protecting the property are clear. The shopkeeper should take into account other measures, such as the employment of additional staff or security personnel, in their assessment process.

Should the shopkeeper proceed with a CCTV system, the reasons and decision for the installation of the system, including details of the data collected, how it is secured, for how long it is retained and for what purposes it is used should however be recorded. It will also be necessary to provide transparent information to affected individuals.

Example 2: The owner of a large warehouse facility intends to install a CCTV system following a series of break-ins, out of hours and at weekends. There have also been a number of manual handling accidents onsite, where the circumstances have not been fully established.

The identified purposes for using CCTV are to aid in the prevention of break-ins, and in improving the health and safety of staff members. The owner justifies the necessity of the use of CCTV based on the need to monitor the security of the facility out of hours and to assist in the management of health and safety.

Even though the facility is large and requires the use of several external cameras to provide coverage, it is not accessible to the public at any time. For this reason, the owner determines that there is no large scale monitoring of a public space taking place. The owner further determines that internal cameras are required only in the areas of the facility where goods are stored, and where accidents are likely to occur, to monitor health and safety. Cameras will not be placed in the office area, staff recreational areas, or bathrooms.

In this case, the assessment of the impact of the CCTV system will be relatively straightforward due to the lack of a public presence onsite, and the focus of the internal cameras on relevant work areas. The owner of the property will need to address the legitimate privacy expectations of employees by means of assessment, and ensure that adequate information is provided to them about the processing of their data, ideally by means of a data protection policy.

The property owner should also consider alternative measures, or a combination of alternative measures, to CCTV that would assist in achieving the same purposes. For example, improving perimeter fencing and the installation of alarm systems would aid in securing the facility out of hours. With regard to health and safety, monitoring via CCTV should not be considered an alternative to employee training and the provision of personal protective equipment.

Example 3: The Facilities Manager of a university intends to install a campus-wide CCTV system, including cameras in all buildings and external cameras covering the grounds to assist with security and safety. The buildings on the campus include academic facilities, administrative centres, student residences, and sports and social amenities. The grounds of the campus are open to the public and local residents, including children, make frequent use of them for recreational purposes. The campus is accessed on a daily basis by thousands of students, employees, contractors and visiting members of the public.

In this case, the scale of the system across diverse locations, as well as the large number of affected individuals across a broad spectrum of categories, indicate that there may be high risks with the intended processing and an in-depth assessment of the potential impact of the processing of personal data will be necessary. A CCTV system of this scale would likely qualify as "systematic monitoring of a publicly accessible area on a large scale", and would require a full Data Protection Impact Assessment (DPIA). The DPIA process will test the necessity of placing cameras in buildings and external areas. As an employer, the university must also consider the impact of CCTV upon the legitimate expectations of privacy of employees and avoid excessive monitoring in work locations.

As part of a comprehensive stakeholder engagement in the course of conducting a DPIA, the university should take on board the views of employees, the student body, and neighbouring families who may use the campus for recreational purposes. This is part of ensuring that due consideration is given to the privacy rights of each of these groups.

In a large scale project like this example, the DPIA process may indicate that CCTV is not a justifiable measure in every suggested use case due to the suitability of alternative measures or the disproportionate impact it will have on affected individuals. The conduct of a DPIA is an ongoing process. Any decision to implement a measure such as CCTV should be reviewed after installation to ensure that it is being used as intended and that its use continues to be justifiable.

The transparency requirements in this case will reflect the scale of the usage of CCTV. It will be for the university to determine how best to provide information on processing to the diverse categories of data subjects. The university's Data Protection Officer (DPO) should be consulted at all stages of the process.

Transparency and Accountability

The principle of transparency means that individuals have a right to be informed about the processing of their personal data.[10] Notification of CCTV usage can usually be achieved by placing easily-read and well-lit signs in prominent positions. A sign at all entrances will normally suffice indicating the purpose of the CCTV system and the identity and contact details of the data controller. A person whose images are recorded by a CCTV system must be provided with, either directly or in a way the individual can easily access, at least the following information:

- The identity and contact details of the data controller
- The contact details for the data protection officer, if one has been appointed
- The purposes for which data are processed
- The purpose and legal basis for the processing
- Any third parties to whom data may be disclosed
- The security arrangements for the CCTV footage
- The retention period for CCTV footage
- The existence of data subject rights and the right to lodge a complaint with the DPC

It is the responsibility of each data controller to determine the most appropriate way to transmit the required information, taking into account the audience which is intended to receive it. The European Data Protection Board, (EDPB), has adopted 'Guidelines on Transparency under the GDPR', advising on the transmission of information to individuals to meet the transparency requirements of the GDPR.

In terms of the principle of accountability, the GDPR requires data controllers to be responsible for compliance with the principles relating to the processing of personal data, but also be able to demonstrate that they are compliant. Most data controllers, particularly larger organisations, are required to maintain a record of all of their data processing activities and this record should include any use of CCTV systems and any data protection risks involved. It is important that where an assessment of the installation of CCTV has been carried out, that this is included in data controller's record keeping. This should be done in a manner that clearly sets out the necessity, proportionality, reasoning and the assessment criteria and process justifying the decision.

[10] See Articles 5, 12, 13, and 14 GDPR in particular regarding transparency obligations

Security of Personal Data

When the owner/occupier of a premises installs a CCTV system, having justified it as a necessary and proportionate measure, they will be a data controller for the purposes of data protection law. Due consideration must be given by data controllers to the safe storage of personal data and the implementation of appropriate security measures.

Data controllers are obliged to implement technical and organisational measures to ensure that personal data are kept secure from any unauthorised or unlawful processing and accidental loss, destruction or damage. For CCTV systems, this can include restricting access to footage and the use of encryption and password protection for devices storing CCTV footage. Generic or shared passwords should be avoided in order to reduce the risk of inappropriate use of the system occurring and going undetected. The storage medium should be maintained in a secure environment and the use and regular review of an access log can provide assurance that only authorised personnel have access to and may view the footage.

Some CCTV systems allow footage to be accessed remotely, via mobile phone for example. Remote access to CCTV cameras, by whatever means, is becoming more frequent with advances in technology. Such technology is helpful in terms of providing security monitoring of an empty building at night time or at weekends. However, controllers utilising remote access must consider any additional risk of unauthorised disclosure which may arise from such functionality, and further potential concerns from a data protection perspective arise where the remote access takes place in relation to areas such as manned workplaces and where workers perceive that their work performance is being monitored on a live basis. Employers may be tempted to use such technologies as a substitute for on-the-ground supervision by supervisory or managerial staff; this type of monitoring or surveillance is unlikely to justifiable.

The implementation of both technical and organisational security measures should be accompanied by robust policies and protocols to ensure their ongoing effectiveness. Access controls should be frequently reviewed and tested, and security measures should be enhanced or upgraded where necessary.

Data Protection by Design and by Default

Data controllers are obliged to adhere to the principles of data protection by design and by default. Data protection by design requires that appropriate measures to implement data protection principles are integrated at the planning stage of any data processing operation, and maintained at all stages. This means that where the implementation of CCTV is being considered, data protection concerns are addressed at the earliest stage of the project.

Data protection by default requires that technical and organisational measures be put in place to ensure that only personal data which are necessary for a specific purpose are processed. In the rollout of a CCTV system, this will have a bearing, for example, on the placement of cameras, the focus of the cameras, the capability of the cameras, the functionality of the cameras (have they pan, tilt or zoom functionality?) and privacy masking features as well as the determination of an appropriate retention period. Users of CCTV systems should be aware that the use of particular features, such as zoom capability, can increase the potential intrusion on individuals' privacy.

Data Processors

CCTV systems are often managed and maintained by third party contractors on behalf of the owners of premises. Security companies that place and operate cameras on behalf of clients may be considered "data processors", where they process personal data under the instruction of data controllers (their clients), subject to contract.

Data protection law places a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all unlawful forms of processing. This obligation can be met by measures such as having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted. Staff of the security company must be made aware of their obligations relating to the security of data.

Clients of the security company should have a contract in place, which details what the security company may do with the data, what security standards should be in place, and for how long the data should be retained. Please note the guidance on data processing contracts available on the DPC website.

Retention of Personal Data

Data protection law requires that personal data should be retained for no longer than is necessary to achieve the identified purpose for which it is processed. The law does not define specific retention periods. A data controller needs to be able to justify a defined retention period, and data may not be kept on a 'just-in-case' basis. A data controller may wish to consider any previous incidents or situations giving rise to the necessity for access to CCTV footage to achieve a purpose that may have a bearing on the appropriate retention period.

As an example, Section 8 of the Civil Liability and Courts Act 2004 requires that where a letter of claim in a personal injuries action is served one month after the accident, the court shall draw such inferences as appear proper. A 30-day retention period may thus be deemed reasonable, proportionate and balanced for CCTV footage for the purpose of defending a potential personal injury action. For a normal security system, it would be difficult to justify retention beyond one month, except where the images identify an issue – such as a break-in or theft – and is retained specifically in the context of the investigation of that issue.

The retention period should be the shortest period necessary to achieve the purpose for which the system was installed and should allow the controller enough time to review any footage as necessary before deleting the data. Where a CCTV recording system or device has a default retention period , this should be reviewed by the data controller, and compared to their own assessment of what is a necessary retention period to avoid the retention of data for longer than is necessary.

Where footage has been identified that relates to a specific incident a longer period may be justifiable for the particular section of footage concerned, such as in the investigation of a workplace accident or where footage may be used as evidence in criminal proceedings. This footage should be isolated from the general recordings and kept securely for the purposes that has arisen.

CCTV in the Workplace

While employers may have legitimate reasons in very exceptional and special circumstances only for installing CCTV, employees also have legitimate expectations that their privacy will not be intruded upon disproportionately. Where possible, cameras should be focused upon areas of particular risk, i.e. at cash points or areas where human observation is difficult. CCTV recording should be avoided in areas where employees have an increased expectation of privacy such as break rooms, changing rooms and toilets.[11] The threshold to justify the use of CCTV in such locations is at the highest level and generally very difficult to meet.

Employees should be given a clear notification that CCTV monitoring is taking place and informed as to where and why it is being carried out. If the use of CCTV has been justified for a specific purpose such as security or health and safety, it should not be used for a further purpose such as monitoring staff attendance or performance.

[11] See section in these guidelines on the use of CCTV in areas of an increased expectation of privacy

The use of CCTV in the workplace can be contentious and it is not generally considered to be an appropriate tool to monitor staff attendance or performance. However, situations can arise where an employer needs to use CCTV footage for a purpose other than one identified at the outset such as to investigate an allegation of gross misconduct or other disciplinary matter. This may be legitimate where it is carried out strictly on a case-by-case basis, and is justified based on necessity and proportionality to achieve the given purpose. The employer must be able to demonstrate why the use of CCTV is necessary to provide evidence in a disciplinary matter, and that their access of CCTV footage is proportionate and limited in scope to the investigation of a particular matter. In such cases, the rights of the employee and their expectation of privacy will not be seen as overriding the interests of the employer, and the employee's data protection rights should not be seen as presenting a barrier to the investigation of serious incidents.

The case study set out below, 'Case Study 2 of the Data Protection Commission's Annual Report 21 May – 31 December 2018', provides an example of processing of this kind by an employer.

Case Study: Provision of CCTV footage by a bar to an employer (Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

The DPC received a complaint against a city-centre bar, alleging that it had disclosed the complainant's personal data, contained in CCTV footage, to his employer without his knowledge or consent and that it did not have proper CCTV signage notifying the public that CCTV recording was taking place.

During our investigation, we established that a workplace social event had been hosted by an employer organisation in the bar on the night in question. The complainant was an employee of that organisation and had attended the workplace social event in the bar. An incident involving the complainant and another employee had taken place in the context of that workplace social event and there was an allegation of a serious assault having occurred. An Garda Síochána had been called to the premises on the night in question and the incident had been reported for a second time by the then manager and headwaiter to the local Garda station the following day. We established that the employer organisation had become aware of the incident and had contacted the bar to verify the reports it had received. Ultimately the bar manager had allowed an HR officer from the employer organisation to view the CCTV footage on the premises. The HR officer, upon viewing the CCTV footage, considered it a serious incident and requested a copy of the footage so that the employer organisation could address the issue with the complainant.

The bar manager allowed the HR officer to take a copy of the footage on their mobile phone as the footage download facility was not working.

The DPC considered whether there was a legal basis, under the grounds of the 'legitimate interests' of the data controller or a third party under Section 2A(1)(d) of the Acts, for the bar to process the complainant's personal data by providing the CCTV footage to the employer organisation. This provision allows for the processing that is 'necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject'.

In its analysis of this case, the DPC had regard to the judgment of the CJEU in the Riga regional security police case in which the CJEU had considered the application of Article 7(f) of the Data Protection Directive (95/46/EC) on which Section 2A(1)(d) of the Acts is based, and identified three conditions that the processing must meet in order to justify the processing as follows:

a) There must be the existence of a legitimate interest justifying the processing;
b) The processing of the personal data must be necessary for the realisation of the legitimate interest; and
c) That interest must prevail over the rights and interests of the data subject.

The DPC established during its investigation that, arising from the incident in question, there was an allegation of a serious assault committed by the complainant against a colleague and the bar had provided a copy of the CCTV footage to the complainant's employer so that the employer could properly investigate that incident and the allegations made. The DPC took into account that as the incident had occurred during the employer organisation's workplace social event, the employer might have been liable for any injuries to any employee that could have occurred during the incident. Accordingly, the CCTV was processed in furtherance of the employer organisation's obligation to protect the health and safety of its employees. As the CJEU has previously held that the protection of health is a legitimate interest, the DPC was satisfied that there was a legitimate interest justifying the processing. The DPC also considered that the disclosure of the CCTV in this instance was necessary for the legitimate interests pursued by the employer organisation so that it could investigate and validate allegations of wrongdoing against the complainant.

The DPC considered, in line with the comments of Advocate General Bobek in the Riga regional security police case, that it was important that data protection is not utilised in an obstructive fashion where a limited amount of personal data is concerned. In these circumstances the DPC considered that it would have been unreasonable to expect the bar to refuse a request by the employer organisation to view and take a copy of the CCTV footage, against a backdrop of allegations of a serious assault on its premises, especially where the personal data had been limited to the incident in question and had not otherwise been disclosed. On the question of balancing the interest of the employer organisation against the complainant's rights and interests, the DPC had primary regard to the context of the processing, where the bar had received a request for the viewing and provision of a serious incident on its premises, which it had deemed grave enough to report to An Garda Síochána. A refusal of the request might have impeded the full investigation of an alleged serious assault, and the employer organisation's ability to protect the health and welfare of its employees. Accordingly the DPC considered that it was reasonable, justifiable and necessary for the bar to process the CCTV footage by providing it to the employer organisation, and that the legitimate interest of the employer organisation took precedence over the rights and freedoms of the complainant, particularly given that the processing did not involve sensitive personal data and there had not been excessive processing.

On the facts, the DPC was also satisfied that the bar currently had adequate signage alerting patrons to the use of CCTV for the purpose of protecting staff and customers and preventing crime, and that in the absence of any evidence to the contrary offered by the complainant, the complainant had been on notice of the use of CCTV at the time in question.

In many of the complaints that the DPC handles, data subjects hold the mistaken belief that because they have not consented to the processing of their personal data, it is de facto unlawful. However, there are a number of legal bases other than consent that justify processing depending on the particular circumstances. With regard to the legitimate interests justification, the DPC will rigorously interrogate whether the circumstances of the processing satisfy the elements that the CJEU has indicated must be present for controllers to rely on this legal basis. Equally, however, the DPC emphasises that where the circumstances genuinely meet the threshold required for this justification, as per the sentiment of Advocate General Bobek of the CJEU, protection of personal data should not disintegrate into obstruction of genuine legitimate interests by personal data.

Disclosure of CCTV to Third Parties

On occasion, a data controller may be asked to disclose CCTV recordings to third parties for a purpose other than that for which they were originally obtained. This may arise, for example, where a request is received from An Garda Síochána or another law enforcement body to provide footage to assist in the investigation of a criminal offence. In these circumstances, it is recommended that requests for copies of CCTV footage should only be acceded to where a formal written request is provided to the controller stating that An Garda Síochána (or other law enforcement body) is investigating a criminal matter. For practical purposes, and to expedite a request speedily in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request should be followed up with a formal written request. For accountability purposes a record of all Garda Síochána requests should be maintained by data controllers and processors detailing any provision of footage.

As noted in the case study in the previous section, a data controller may be requested to provide CCTV footage to a third party to investigate an incident. In such cases, the same assessment procedure as applied for the original purpose should be applied to the new purpose to determine if it can be justified in the pursuit of a genuinely legitimate interest of the data controller or another party. Such eventualities will need to be assessed on a case-by-case basis to ensure that the principles of data protection are adhered to, and the rights of individuals are not prejudiced. It should be noted that the legitimate interests of a third party do not oblige a data controller to disclose CCTV footage, but may permit such disclosure subject to assessment.

Providing Access to CCTV to Data Subjects

Data protection law provides for a right of access to their personal data by individuals. This applies to any individual whose identifiable image has been recorded by a CCTV system. When a data controller receives a request from an individual to access CCTV data, they must normally respond within one month.

To facilitate the processing of the request, the controller may ask the individual to give a reasonable indication of the date and time of the footage they are looking for. If the recording has already been deleted on the date on which the request is received, the defined retention period having expired, the individual should be informed that the footage no longer exists. If an access request has been received, the footage should not be deleted until the request has been fulfilled.

Responding to an access request usually involves providing a copy of the footage in video format, as well as providing detailed information on the legal basis and purpose for the filming, and any disclosures that may have been made. Where the footage is

technically incapable of being copied to another device, or in other exceptional circumstances, it may be acceptable to provide picture stills as an alternative to video footage. Where picture stills are supplied, it would be necessary to supply sufficient stills for the duration of the recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.

Where images of parties other than the requesting data subject appear on the CCTV footage the data controller needs to consider, on a case-by-case basis, whether the release of the unedited footage 'adversely affects' the rights or freedoms of the third parties, such as their data protection rights, trade secrets, or intellectual property rights such as copyright. The controller needs to conduct a balancing test between the right of the data subject (requester) to access his or her personal data as against the identified risk to the third party that may be brought about by the disclosure of the footage. The GDPR notes that these considerations should not result simply in a refusal to provide all relevant information to the data subject. Where necessary, measures may include pixelating or otherwise de-identifying the images of other identifiable parties before supplying a copy of the footage from the footage to the requester. Alternatively, the data controller may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.

Data controllers of CCTV systems should have a procedure in place to respond without undue delay to any requests for access to data. This could include identifying a third party processor to edit footage to retrieve images of the requester and to redact the images of any other persons as necessary. Information can be provided through a public website to facilitate members of the public in making access requests and identifying the location, time and data of any footage they wish to access.

Covert Surveillance

The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert surveillance is normally only permitted on an exceptional case-by-case basis where the data are kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies that a written specific policy be put in place detailing the purpose, justification, procedure, measures and safeguards that will be implemented with the final objective being, an actual involvement of An Garda Síochána or other prosecution authorities for potential criminal investigation or civil legal proceedings being issued, arising as a consequence of an alleged committal of a criminal offence(s).

Covert surveillance must be focused and of short duration. A DPIA should be carried out prior to the installation of any covert systems, to clearly assess whether the measure

can be justified on the basis of necessity and proportionality to achieve the intended purpose. Only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease. If the surveillance is intended to prevent crime, overt cameras may be considered to be a more appropriate measure, and less invasive of individual privacy.

Further, where a data processor is involved in the covert surveillance, controllers must remember that a data processor contract will be required.

Facial Recognition and Biometric Data

Specific technical features of certain CCTV systems, such as the use of facial recognition software, may be a factor in determining the basis on which the data can be lawfully processed. Facial recognition processing involves a matching step where previously seen faces are registered and recorded on the system so that when and if they appear again they are matched and can uniquely identify the individual in question. Facial recognition processing is considered biometric processing and accordingly the data processed is categorised as "special category" of personal data subject to the requirements of the GDPR, which, sets out further conditions to provide for the lawful processing of the data.[12]

Any processing of biometric data should be considered as separate to the regular usage of the CCTV system and a data controller engaging in such processing must take all steps to ensure that it is compliant with the data protection legislative frameworks.

The use of CCTV in areas of an increased expectation of privacy

In general, data controllers should avoid using CCTV in circumstances where a reasonably high expectation of privacy exists.[13] For example, individuals have the highest expectation of privacy when using the changing rooms of a clothes shop or the cubicles in the toilet facilities of a restaurant. Using CCTV to monitor individuals in these specific areas will likely contravene the GDPR in nearly all circumstances, as the level of

[12] See Article 9 GDPR

[13] Determining what is a reasonable expectation of privacy is case specific. It will depend on a person's actual expectation of privacy and, given all the circumstances, whether society would view that expectation as reasonable. The question is not whether a particular individual actually expects the processing, but whether on balance a person should reasonably expect the processing in the overall set of circumstances. See further information in terms of the expectations of users as set out in paragraphs 36 – 39 of the Guidelines 3/2019 on processing of personal data through video devices

intrusiveness and impact on individuals will not be warranted in light of the purposes for its use.

Individuals who attend shopping centres are well aware of and expect that there are multiple CCTV cameras in operation around these complexes for a number of legitimate purposes such as the detection and prevention of crimes. They also expect that specific stores within a shopping centre have CCTV in use for similar purposes. However, it is reasonable to assume that individuals would not expect the use of video surveillance in toilet cubicles in the shopping centre or in changing rooms within shops. Data controllers therefore need to be mindful that in most situations where they wish to deploy CCTV in such areas, it will generally not be fair on patrons. Even if a rationale for deployment in such areas to address a serious and legitimate issue exists, it is likely it will not warrant constant electronic surveillance and a high level of intrusion.

However, there may be circumstances where a controller can demonstrate that CCTV is permissible to monitor areas near or within the vicinity of a changing room or cubicle as the reasonable expectation of privacy of a user may be lower. The threshold required to justify using CCTV in such areas remains very high, and it will be challenging for data controllers to meet, requiring a rigorous examination of all data protection implications to individuals prior to deployment.

In order to demonstrate that the use of CCTV is compliant, a data controller must address and demonstrate the following:

i. Its use meets the principles of data protection and is in pursuit of a legitimate aim;[14]
ii. It is necessary and proportionate taking account of data subjects rights and interests;[15] and
iii. All risks associated with the processing of personal data have been identified, assessed and minimised to an acceptable level.

Data controllers are therefore required to identify and carefully examine all the legitimate issues arising, which are intended on being addressed by the use of CCTV in these areas and to assess and implement appropriate measures which adequately

[14] See section in these guidelines on Lawfulness of the Processing, Transparency and Accountability
[15] See section in these guidelines on Necessity and Proportionality

protect the interests of individuals who will use such facilities. This needs to occur prior to deployment.

Serious Problem

Deploying CCTV in places where there is a reasonable expectation of individual privacy should only occur when there is a particularly serious and documented problem.[16] If data controllers intend on installing CCTV in such areas, they will need to be in a position where they can provide detailed evidence, which clearly justifies their use at any given time.

Therefore, data controllers must establish the following:

1. The problem(s) being addressed is/are sufficiently serious to justify the use of CCTV in such locations;
2. The problem(s) cannot be addressed by less intrusive measures;
3. The use of CCTV addresses the problems identified; and
4. The risks posed to data subjects using the facilities have been fully assessed and mitigated to an acceptable level.

In order to achieve the above, the controller should fully assess, understand and document the scale, scope, nature and extent of the issues presented.

The following checklist of questions is relevant in terms of understanding the nature of the problem to be addressed:

- ✓ What is the nature and seriousness of the problem?
- ✓ Is the problem location specific? Where does the problem occur, or where is it most prevalent?
- ✓ Does the problem occur at particular times or days? For example, 24/7, only on Friday & Saturday nights or perhaps there is no pattern.
- ✓ How long has the problem existed? Is this a relatively new or emerging problem, or has it been a problem for some considerable time?
- ✓ Has the extent of the problem changed over time? Has the problem got worse over time, stayed the same or even improved? If it has changed, over what period has it changed e.g. last month, six months, a year?
- ✓ Does the problem give rise to further problems? Is the presence of the problem actually a catalyst to other problems?
- ✓ What are the causes behind the problem?

[16] The controller would need to provide compelling evidence of the seriousness of the issues it is trying to address. Issues that are not sufficiently serious, such as maintaining the cleanliness of the facility or isolated anti-social behaviour would not justify the use of CCTV in such locations.

- ✓ What are you trying to achieve?
- ✓ What alternative measures, if any, have been considered to eliminate or reduce the problem?[17]
- ✓ Who are the data subjects? What information is to be collected?
- ✓ Do they include children or vulnerable groups?
- ✓ What is the scale and duration of the processing?

Answers to the checklist of questions above will help a data controller identify the context and purposes of the proposed processing as well as assisting in terms of assessing whether the use of CCTV in such locations will have the desired impact to address the problem. For example, if the objective sought is to reduce serious anti-social behaviour in a restaurant's toilet facilities at a particular time, can the controller assess whether or not the intervention has been effective? Can the controller identify, assess and demonstrate that less intrusive measures were not appropriate to address the serious issues? The use of CCTV should be a necessary and proportionate response to the problem data controllers are addressing. Data controllers should, therefore, carefully consider whether to use a surveillance system if other less intrusive options are available and effective. Ultimately, it is a matter for the data controller to be able to justify that the processing is necessary and proportionate in light of the concerns presented.

A data controller decides to use CCTV in its public toilet areas to deter serious anti-social behaviour. The data controller does not have any documented evidence of such behaviour or the times it has allegedly occurred. In addition, the data controller does not consider whether implementing less intrusive measures will achieve its objective. In such circumstances, it will be very difficult for a data controller to demonstrate that its use of CCTV in its toilet areas is warranted.

If the documented evidence of a data controller who runs a family restaurant suggests that serious anti-social behaviour is regularly occurring on weekend evenings after 9pm in its restrooms, deploying CCTV, which is continuously recording all individuals who use the facility outside of this particular time, is likely to be a disproportionate measure to achieve the objective.

[17] For example, could better lighting, improved physical security measures adequately mitigate the risk posed by the problem? Does the camera operation need to be continuous? If dismissing alternative and less intrusive measures, a data controller should be able to provide valid reasons for not relying on them and opting to use CCTV.

It is accepted that a data controller has the right to take steps to protect its staff, customers and its property against issues such as anti-social behaviour, vandalism etc.. However, steps taken to address these issues must be implemented in a transparent and proportionate manner where the data protection rights of individuals are not unfairly infringed.

Transparency and Fairness[18]

Data controllers must ensure that individuals being monitored by CCTV are fully aware they are being recorded. Notices and signs should be more prominent and frequent in these areas. They should be positioned so that it allows individuals to easily recognise the circumstances of the recording before entering the areas being monitored. Even if data controllers can point to a lawful and legitimate basis for using CCTV, they may not be able to satisfy the principle of fairness if an individual is already being captured by CCTV recording in the monitored area whilst reading the warnings about the particularly intrusive surveillance technology for the first time.

Assessing Risk to Individuals

As the intended processing of personal data could have a greater chance of harming individuals, the controller needs to assess the risks before processing takes place.

It is strongly recommended that data controllers conduct appropriate and detailed assessments (such as a Data Protection Impact Assessment (DPIA) and/or a legitimate interest assessment)[19] for all instances where CCTV is to be deployed in these areas. Doing so gives a data controller the best opportunity of demonstrating compliance with the GDPR. In addition, data controllers should consult with all users of these facilities (i.e. workforce, customers etc.) as part of the assessment process.

If CCTV is intended to be used in areas which are frequented by children a DPIA will be required in line with the Children Fundamental Guidelines.[20] Accordingly, if a school were contemplating deploying CCTV in its toilet facilities, it would be imperative that it has conducted a comprehensive DPIA in advance of processing, which demonstrates that the risks envisaged have been mitigated to a permissible level, and that the processing envisaged complies with the GDPR.

[18] See section in these guidelines on Transparency and Accountability
[19] See pages 21 – 24 of the Legitimate Interest Guidelines
[20] See page 62

Mitigation of Risks

There are a number of measures a controller can take to mitigate risks associated with this type of processing:[21]

- Implement measures to ensure the field of vision of the CCTV only captures the intended area (techniques such as masking or screening can be useful to achieve this purpose).
- Ensure CCTV is operational to address the specific serious issue arising and consider the appropriateness of its functionality/design in light of that purpose.[22]
- Document consideration/assessment of other less intrusive measures.
- Provide clear, prominent signage at the entrance to the areas being monitored and under the camera in the facility.[23]
- Ensure adequate security and restrictions on viewing and disclosing images are in place for those using the system:[24]
    - Access is restricted to select supervisors in a secure, locked environment.
    - IT security training is provided to the supervisors who have access.
    - Remote access is restricted to one CCTV project lead and only for a specified and necessary purposes i.e. maintenance purposes.
    - Third-party access is restricted to system engineers for maintenance or requests from AGS.
    - Encrypted CCTV.
    - Regular system logs checks (to prevent unauthorised access) and routine audits for password protection.
- Conduct regular reviews to ensure the use of surveillance camera systems remains justified.

In addition to the above, it is important that a data controller can provide the following:

- Documented retention policy, risk management policy, and CCTV policy.
- Contract and data processing agreements with third-party CCTV providers, if relevant.[25]
- Procedures to manage data subject access requests or other rights requests.
- Documented assessments of the processing undertaken with the full involvement of a DPO or other relevant expert.

[21] This not an exhaustive list of measures which could be taken and demonstration of the use of a combination of these measures may not necessarily mitigate the risks to an acceptable level
[22] See section in these guidelines on Data Protection by Design and by Default
[23] See section in these guidelines on Transparency and Accountability
[24] See section in these guidelines on Security of Personal Data
[25] See section in these guidelines on Data Processors

Engagement with the DPC

The following documentation is likely to be sought from the data controller if the DPC is assessing a complaint or carrying out an inspection of an area:

- A copy of the assessments carried out by the data controller. These documents would need to address the following:
  - Documentary evidence of the serious issue/concern.
  - Documentary evidence of all other less intrusive measures considered/exhausted prior to the placement of CCTV.
  - Documentary evidence of consultations with relevant stakeholders, including staff and customers, prior to the placement of CCTV.
- A copy of the Privacy Policy, in particular as it relates to the use of CCTV.
- A copy of the Data Retention Policy as it relates to use of CCTV.[26]
- A copy of the Risk Management Policy.
- A balanced legitimate interest assessment if the controller is relying on a legitimate business interest as its lawful basis to process its customer's data by CCTV.
- Evidence of clear transparent signage in place prior to entering the areas in question.
- Evidence of a policy for dealing with a customer wishing to enforce their data subject rights under Article 12-22 GDPR.
- Evidence of consultation with a Data Protection Officer (or other relevant individual).

[26] See section in these guidelines on Retention of Personal Data