Client Alert: Using CCTV on Business Premises – Zooming in on Data Protection

Date : June 17, 2020

We first prepared these notes in April 2020 and we've updated them to reflect some recent developments and cases.

Closed circuit TV ("**CCTV**") and other types of surveillance systems are widely used in many organisations but also come with inherent privacy risks due to their potential to be intrusive to individuals' rights. Using CCTV in the EU is subject to the General Data Protection Regulation ("**GDPR**"). Other in-country laws may also apply - for example the Data Protection Act 2018 ("**DPA 2018**") in the UK.

Organisations that do not comply can face high fines and other enforcement action such as stop-processing orders. Individuals can also bring civil claims or class actions for losses suffered as a result of infringements of data protection laws.

Organisations are having to navigate a more complex legal landscape as surveillance is becoming more high-tech, with innovations such as automatic number plate recognition ("**ANPR**"), body worn video ("**BWV**"), drones and live video streaming services. This article focuses on use of CCTV in a corporate context. We've also written about some special considerations in automotive here https://bit.ly/gdprauto.

The remit of the data protection regulator, the UK Information Commissioner's Office ("**ICO**"), includes CCTV use to the extent that this involves processing personal data. The ICO has published In the picture: A data protection code of practice for surveillance cameras and personal information ("**ICO Surveillance Code**") to provide good practice advice on the legal obligations in relation to personal data that are applicable to operators of CCTV and other surveillance camera devices that view or record individuals.

The ICO works with the Surveillance Camera Commissioner ("**SCC**"). The SCC's role is to encourage compliance with the Surveillance Camera Code of Practice ("**SCC Code**"), which provides advice and guidance on issues such as operational requirements, technical standards and the effectiveness of available systems.

The Code and the Guidelines have not been updated since the DPA 2018 came into force but still remain useful reference resources.

We have outlined below the key legal requirements and practical considerations when setting up and running a CCTV or other camera surveillance system.

Setting up the CCTV system

When setting up a CCTV system, organisations will need to:

- Carry out a data protection impact assessment ("**DPIA**").

"Large-scale public monitoring" is one of the types of processing activities for which a DPIA is mandatory, as this is considered 'likely to result in a high risk' to the rights and freedoms of individuals. A DPIA will help you to identify and minimise risks that result from data processing activities.

As part of this process you should consider:

1. the nature of the problem you are seeking to address;
2. whether a surveillance system would be a justified and an effective solution, and the existence of any better solutions;
3. the effect that use of the system may have on individuals, and

4. whether, in view of this, its use is a proportionate response to the problem.

We've seen in the Taksi Helsinki Oy case in Finland (see below) that a DPIA could also be required when CCTV is upgraded.

- If there's a UK dimension, register on the ICO's register of fee payers and pay the data protection fee. There's more information on this system here https://www.corderycompliance.com/solutions/privacy-registration-and-renewal/.
- Establish a valid legal basis (under GDPR Article 6) for use of the system.

Where CCTV is used for security reasons or for staff monitoring, the legal basis relied on will typically be "legitimate interests are balanced". If this is the case, a "legitimate interests assessment" (LIA) should also be carried out where the organisation's (or a third party's) legitimate interests is balanced against the privacy rights of the individual.It might be possible to combine a LIA and DPIA.

Depending on the purpose of the surveillance, alternative legal bases available may be where this is necessary to comply with the data controller's legal obligations or, in very limited cases, to protect the data subject's vital interests. If special categories of personal data or criminal offence data is processed, additional conditions must be met (under GDPR Articles 9 and 10 and Schedule 1, DPA 2018).

When CCTV footage is disclosed to the police, it will be processed for a law enforcement process as defined by Part 3 of the DPA 2018, and is taken outside the scope of the GDPR.

- Build adequate privacy controls into the system using data protection by design and by default, in particular by ensuring compliance with the data protection principles, including:
    - Data minimisation – e.g. setting up the system so that it doesn't capture a wider area than is necessary;
    - Purpose limitation – e.g. controls to ensure that CCTV footage collected for security purposes are not used for other incompatible purposes;
    - Accuracy – e.g. CCTV images should be clear and high quality;
    - Retention – e.g. automatic deletion of CCTV images after a reasonable (and generally, short) period; and
    - Confidentiality and integrity – e.g. having monitors in a secure locked room.

As a matter of good practice, organisations should also:

- Implement a clear CCTV policy and / or procedure and to monitor that this is being followed;
- Appoint a nominated individual who is responsible for the operation of the CCTV system; and
- Train staff on CCTV usage.

How should you let people know that CCTV is in operation?

Assuming the system is justified, once you are ready to get it up and running, you will need to:

- Use signs to provide some mandatory information to people who will be captured on CCTV about use of their personal data (GDPR Articles 12 to 14).
- At least disclose the controller's identity and contact details – consider if relevant organisations that operate CCTV systems are joint or co-controllers, e.g. if a building management or security company manages security on behalf of a building owner.

The ICO Surveillance Code says:

"You can meet the GDPR's requirements for privacy notices via prominently displayed signs that provide brief and comprehensible information explaining that CCTV is being used, and stating who manages the surveillance system and how to contact them, as was acceptable under the DPA 1998.

It's advisable to include the URL of a website on which you can publish the full set of information listed above, although you can also provide this information by other means."

Covert surveillance activities of public authorities are governed by the Regulation of Investigatory Powers Act (RIPA) 2000 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.

Do I need to keep CCTV footage secure?

Organisations are required to implement technical and organisational measures (TOMs) to ensure a level of security that is appropriate to the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

In the context of CCTV systems, this might include ensuring that:

- Access to CCTV images is restricted to a limited number of authorised individuals. You'll need to choose those individuals with care – for example one earlier case suggests choosing people further away from the location under surveillance might be better from a data protection point of view. Following the Morrisons case (see https://bit.ly/checkoutmorrisons) you will also need to make sure that the employees who can see the images are reliable and can be trusted;
- Access to online systems is controlled by some form of authentication (eg, a username and secure password);
- Where wireless communication links are utilised (e.g. to transmit images between cameras and a receiver) or images are transmitted over the internet (e.g. for remote viewing), signals are encrypted to prevent interception; and
- Measures are in place to protect devices used to store CCTV images from theft, unauthorised access or physical damage (e.g. keeping storage devices in a locked room, or storing digital recordings in an encrypted format).

Who should see CCTV footage?

Restrictions should be imposed on who is allowed to view CCTV footage, including:

- Restricting external disclosure of CCTV images to law enforcement bodies and identity-verified data subjects.
- For data subject requests, consider:
    - The capability of the device or system to securely export data to third parties (at the procurement stage);
    - What would be an appropriate format of the data to be disclosed in response to subject access requests, and appropriate security controls (e.g. encryption); and
    - Pixelating the faces of others captured in CCTV footage before giving access – you generally cannot give individuals access to personal data if doing so means sharing the personal data of third parties.

How long should you keep CCTV footage for?

Set a retention period that reflects the purpose for which the information is collected and how long it is needed to achieve this purpose. In particular:

- CCTV images should only be retained long enough to fulfil the purpose for which the system has been implemented (eg for a theft to be noticed) and the incident to be investigated; and
- Implement a retention policy and monitor that this is being followed.

Are there any other legal obligations?

Yes. Other laws could also apply. For example, the UK has a separate regulatory system governing security operatives. The Private Security Industry Act 2001 set up a statutory regulatory scheme for private security companies. It may be necessary for individuals viewing CCTV footage to be licensed under the Security Industry Authority regime in addition to complying with data protection laws.

Has there been any recent enforcement action?

Since the introduction of the GDPR, there have been a number of fines for improper use of surveillance technology. These include:

Jurisdiction / Regulator	Date	Respondent	Nature of infringement	Enforcement action
France (CNIL)	June 2019	Uniontrad Company, a small nine person company	Following complaints from staff, the company was fined for continuously filming employees on CCTV without a valid legal basis and not providing adequate privacy information. In setting the fine, the CNIL took into account previous warnings from the regulator, the size of the company and the fact that it was in financial difficulties	€20,000 fine
Spain (AEPD)	February 2020	Casa Gracio Operation	The company used CCTV cameras in a hotel which also captured the public roads outside the hotel. This infringed the data minimisation principle	€6,000 fine
Finland (Tietosuojavaltuutetun Toimisto)	May 2020	Casa Gracio Operation		