Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit

IGDC • DHCW

Expectations Guidance Document

4-Video Surveillance

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the Video Surveillance section of the Welsh Information Governance Toolkit (WIGTK).

Please note: this section of the WIGTK does not apply to Third Party Contractors and therefore, will not be visible on the form for this organisation type.

Under the UK GDPR video surveillance use should be carefully managed to ensure it is lawful, fair, transparent and meets the other standards set in data protection law, while still achieving its security and monitoring objectives. Organisations using video surveillance must be able to demonstrate compliance with UK GDPR, including processing for legitimate purposes, secure storage, upholding individual rights, transparency, recording data processing activities and conducting Data Protection Impact Assessments (DPIA) where necessary.

What is covered under Video Surveillance?

Video surveillance can be categorised based on various factors; the main categories include:

- Closed-Circuit Television (CCTV)
- Automatic Number Plate Recognition (ANPR)
- Body Worn Video (BWV)
- Unmanned Aerial Systems (UAS)/Drones
- Facial Recognition technologies and surveillance
- Smart Doorbells (commercial use)
- Surveillance in vehicles
- Action cameras and other portable surveillance

Minimum Expectations

DPIAs

Conducting Data Protection Impact Assessments (DPIA) is a legal requirement and applies in most cases relating to video surveillance, given the inherent privacy risks involved in the use of these systems. This includes systematically monitoring publicly accessible places on a large scale.

Within the DPIA, your organisation should consider and document the data protection implications of using other functions, such as audio recording, live streaming, facial recognition, and cloud storage.

Policies and Procedures

Principle 5 of the Surveillance Camera Code of Practice states:

> "Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them."

Therefore, your organisation will need to implement a policy to help the organisation use video surveillance consistently. The policy or procedure should cover the purposes the organisation is using video surveillance for and how the information will be handled, including guidance on disclosures and recording. Your policy should also state who the appropriate individual to contact about the video surveillance system is.

Your policy should be reviewed regularly to ensure all information remain accurate and up to date.

Nominated Individual
The organisation should have a nominated individual who is responsible for the operation of video surveillance system to ensure it complies with data protection laws and maintains transparency and accountability regarding its surveillance practices.

Principle 4 of the Surveillance Camera Code of Practice states:

> "There must be clear responsibility and accountability for such a system. It is good practice to have a designated individual responsible for the development and operation of a surveillance camera system, for ensuring there is appropriate consultation and transparency over its purpose, deployment and for reviewing how effectively it meets it purpose."

The name and contact details for this nominated individual should be stated in your video surveillance policy/procedure.

Responding to Requests
Your organisation should have an established process to recognise and respond to individuals or organisations making requests for copies of video surveillance footage/images.

All relevant staff within an organisation should know what to do or who to contact if a member of the public makes an enquiry about a surveillance system.

Staff Training
All relevant staff should be aware of the organisations video surveillance policy and procedures and trained to operate video surveillance systems where necessary.

For example:

- All staff who are authorised to access the cameras should be familiar with the system, and with the processes for reviewing footage and extracting it if required.
- All staff should be familiar with procedures for recognising and dealing with requests for personal data.
- All staff should be familiar with the likely disciplinary penalties for misuse of the cameras.
- Where a staff member's role explicitly includes monitoring video surveillance, such as a security guard, the organisation should ensure that the individual meets and records

appropriate training standards (such as Security Industry Authority (SIA) qualifications).

Retention

Your organisation should retain data for the minimum time necessary for its purpose and dispose of it appropriately when no longer required.

The organisations retention period should not be based merely on the storage capacity of the system used, or just in case you think the data may be useful in the future but reflect how long the data is required for the purpose. Data may need to be retained for a longer period, if requested by a law enforcement body for investigative purposes.

Organisation should delete the data when it does not achieve the purpose for which it is collected. The organisation should implement controls including:

- Document your information retention policy for video surveillance information and ensure it is understood by those who operate the system.
- Implement measures to ensure you permanently delete information through secure methods at the end of the retention period.
- Undertake systematic checks to ensure that you are complying with the retention period in practice.

Quality of Images

Organisations should ensure that they select a system which produces high quality, clear images. High quality depends on the purpose, location or device being utilised and is not the same criteria for all types of video surveillance.

Your organisation needs to determine that the surveillance equipment, when in operation, provides images/sound that enables clear identification of data subjects and could be utilised by law enforcement bodies to investigate crime. Therefore, the specification required would depend on the equipment, location, and usage.

Your organisation should ensure that video surveillance systems are placed in the best locations, where possible. Checks should be carried out regularly to ensure that the system is continuing to produce high quality images and that system settings do not compromise quality.

Storage, access, and maintenance of system

Your organisation should store recorded material securely in a way that maintains the confidentiality, integrity and availability of the information. This is to ensure that you protect

the rights of individuals recorded by surveillance systems and can use the information effectively for its intended purpose.

Principle 7 of the Surveillance Camera Code of Practice states:

> "Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes."

When implementing appropriate technical and organisational security measures, you should check:

- Any ability to make copies of information is restricted to appropriate staff.
- There are sufficient controls and safeguards in place if the system is connected to, or made available, across a network.
- where information is disclosed to a third party, you are able to safely deliver it to the intended recipient.
- Control rooms and rooms where information is stored are secure.
- Staff are trained in security procedures, with sanctions against staff who misuse surveillance system information.
- Staff are aware that they could be committing a criminal offence if they misuse surveillance system information.
- There are any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied to your system, or any other devices connected to it, or both.

Signage

In keeping with the principle of fairness and transparency, it is important that organisations inform individuals that their personal data is being processed. The best way to do this is through clear and visible signage explaining that video surveillance is in operation and recording is taking place.

All signage should be the right size and located so that the person is aware that they are being observed and given as much warning as possible.

Principle 3 of the Surveillance Camera Code of Practice states:

> "There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints."

The name of the controller collecting the information should be visible on signage to enable individuals to enquire about their data. Where it is not obvious who is responsible for the system, the organisation should ensure there are contact details displayed on the sign(s).

Exceeded Expectations

There is no expectation exceeded questions within this section of the WIGTK.