

Introduction	2
About this guidance	3
What does this guidance address?	5
What are our responsibilities in terms of accountability?	8
How can we comply with the data protection principles when using surveillance systems?	14
Additional considerations for technologies other than CCTV	29
Governance (post-deployment)	47
Checklist for limited CCTV systems	54

Introduction

The steady growth of the use of video surveillance systems across public and private sectors, has led to both fixed and mobile cameras becoming more accepted in society. As video surveillance technology becomes more mainstream and affordable, it is now more common to see technologies such as smart doorbells and wireless cameras. Traditional closed circuit television (CCTV) also continues to evolve into more complex artificial intelligence (AI) based surveillance systems. These can process more sensitive categories of personal data.

The ways in which the technology is used also continue to develop. This includes connected databases utilising Automatic Number Plate Recognition (ANPR) or the use of Facial Recognition Technology (FRT) in public spaces. Often they process the personal data of large numbers of the general public for security, crime prevention or for other specified purposes such as digital advertising. However, some of these uses can be particularly intrusive, especially if processing takes place without the knowledge of the individual.

Building public trust and confidence is essential to ensuring that the benefits of any new technology can be realised. The public must have confidence that the use of surveillance systems is lawful, fair, transparent and meets the other standards set in data protection law. The rights and freedoms of individuals can be greatly affected where decisions are made about them based on particularly intrusive means of processing personal data. For example, recording in places individuals would not normally expect. In addition, these surveillance techniques can also play an influential role in how people may behave and move around freely in public spaces. It is therefore important that the use of surveillance is not seen as the cure to the problems that organisations may face. But instead, a helpful supporting tool where lawful, necessary and proportionate in the circumstances.

We have developed this guidance to help organisations in the public and private sector, who use video surveillance systems to collect and process personal data. It will help you to stay within the legal requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). This guidance will also be relevant to law enforcement authorities that are using video surveillance separately for any purposes under the UK GDPR.

About this guidance

This guidance provides advice for when you operate video surveillance systems that view or record individuals. It also covers information that relates to individuals, for example vehicle registrations captured by Automatic Number Plate Recognition (ANPR) equipment. It explores emerging capabilities that can assist human decision making, such as the use of Facial Recognition Technology (FRT) and machine learning algorithms.

Information held by organisations that is classed as personal data relating to identifiable living individuals is covered by the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). This guidance will help you comply with these legal frameworks. When processing personal data, it is important you comply with key data protection requirements, such as data protection by design and default, fairness, accountability, transparency, and respect for the rights that individuals have.

The recommendations in this guidance are all based on the [principles of UK data protection law](#), and are set out to follow the lifecycle and practical operation of surveillance systems.

Sections of this guidance also provide checklists that you should address to help you achieve the good practice recommendations.


Following the recommendations in this guidance will:

- help you to process personal data lawfully and comply with the UK GDPR, the DPA 2018 and other relevant statutory obligations;
- contribute to the efficient deployment and operation of a surveillance system;
- mean that the personal data you process is usable and the processing can meet your intended objectives;
- re-assure those whose personal data you are processing;
- help inspire wider public trust and confidence in the use of surveillance systems; and
- reduce reputational risks by staying within the law and avoiding regulatory action and penalties.

This guidance also acknowledges the wider regulatory environment. For example, where public authorities intend to use video surveillance you must comply with data protection law but also a broader framework of legal, procedural and risk based obligations such as:

- obligations under the Freedom of Information Act 2000 (FOIA); Freedom of Information (Scotland) Act 2002 (FOISA);
- the Human Rights Act 1998 (HRA); and
- the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (PoFA).

The Surveillance Camera Code of Practice (PoFA 2012)


The Protection of Freedoms Act 2012 (PoFA) led to the introduction of the [Surveillance Camera code of practice \(SC code\)](#)  in 2013 and the appointment of a Surveillance Camera Commissioner to encourage compliance with the SC code and review its operation and impact. In England and Wales, relevant

authorities deploying overt surveillance systems should pay due regard to the SC code, regardless of whether or not there is any live viewing, or recording of images or information or associated data.

Separate to this guidance, the SC code provides supporting advice and guidance for organisations using surveillance systems on issues such as operational requirements, technical standards and governance arrangements.

The PoFA requires **relevant authorities** to take the 12 guiding principles in the SC code into account. In general terms, the Police, Police and Crime Commissioners and local authorities in England and Wales are designated as relevant authorities, along with the National Crime Agency. All other controllers and operators are encouraged to follow the SC code, templates and toolkits as good practice on a voluntary basis.

Read further details on the [Biometrics and Surveillance Camera Commissioner's website](#) .

The UK GDPR and DPA 2018 apply to all organisations that process personal data across the UK and has the same effect across all sectors. The SC code only applies to relevant authorities across England and Wales. Further, the Scottish government has produced its own separate [CCTV Strategy for Scotland \(2011\)](#) . This strategy provides a common set of principles that operators of public space CCTV systems in Scotland should follow. The principles aim to ensure that these systems are operated fairly and lawfully.

What does this guidance address?

At a glance

This guidance covers the processing of personal data by video surveillance systems by public and private sector organisations. Surveillance systems specifically include, but are not limited to traditional CCTV, Automatic Number Plate Recognition (ANPR), Body Worn Video (BWV), Drones (UAVs), Facial Recognition Technology (FRT), dashcams and smart doorbell cameras.

Organisations using surveillance systems that process the personal data of identifiable individuals need to comply with the UK GDPR and DPA 2018.

This particular guidance does not cover:

- covert surveillance techniques;
- processing for specific criminal law enforcement purposes by competent authorities under Part 3 of the DPA 2018;
- processing by intelligence services under Part 4 of the DPA 2018; and
- processing that is purely in the context of personal or household activities, such as household CCTV within the boundaries of private property.

This guidance also does not cover the use of 'dummy' or non-operational systems. However, it does cover pilots or trials as personal data is still processed.

In detail

- [What do we mean by a surveillance system?](#)
- [Who is this guidance for?](#)
- [What does this guidance address?](#)
- [What does this guidance not address?](#)

What do we mean by a surveillance system?

S29(6) of the [Protection of Freedoms Act 2012](#)  (PoFA) states that "surveillance camera systems" mean:

- (a) closed circuit television or automatic number plate recognition systems,
- (b) any other systems for recording or viewing visual images for surveillance purposes,
- (c) any systems for storing, receiving, transmitting, processing or checking images or information obtained by systems falling within paragraph (a) or (b), or
- (d) any other systems associated with, or otherwise connected with, systems falling within paragraph (a), (b) or (c).

Surveillance systems can be used to monitor and record the activities of individuals, often in high definition

and with ease. As such, these systems can capture information about identifiable individuals and how they behave. This is likely to be personal data under data protection law.

“Personal data” under Article 4(1) UK GDPR means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Biometric data”, in particular, means personal data resulting from specific technical processing relating to the physical, physio-logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR.

Who is this guidance for?

This guidance is aimed at organisations in both the public and private sectors who use surveillance systems and are subject to the UK GDPR and the DPA 2018.

This guidance does not apply to domestic surveillance systems or individuals recording footage in a purely personal or household context. See our separate [guidance on personal or household processing](#) for more information.

It is also not directed at specified “competent authorities” using surveillance systems for criminal law enforcement purposes, who are subject to the separate law enforcement processing regime under Part 3 of the DPA 2018. However, this guidance as a whole still provides advice for competent authorities using surveillance systems for other non-criminal law enforcement uses under the UK GDPR. For more information on which regime applies to you, see our [guidance on which regime](#).

What does this guidance address?

This guidance covers UK GDPR and DPA 2018 requirements. It applies where personal data is being processed by video surveillance systems in the public and private sectors. From the localised small scale use of more traditional CCTV in shops and premises for security purposes, to the deployment of facial recognition technologies and the processing of personal data on a larger scale.

This guidance outlines additional considerations for the use of:

- Automatic Number Plate Recognition (ANPR);
- Body Worn Video (BWV);
- Unmanned Aerial Vehicles (UAVs, also known as drones);
- Facial Recognition Technology (FRT) and surveillance;
- commercial products such as smart doorbells and surveillance in vehicles;
- workplace monitoring, live streaming; and
- other commercially available surveillance systems that have the potential to process personal data.

What does this guidance not address?

This guidance is not intended to address covert surveillance activities by public authorities governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). This type of recording is covert and directed at a specific individual or individuals.

This guidance also does not address:

- processing for specific criminal law enforcement purposes by competent authorities under Part 3 of the DPA 2018;
- processing by intelligence services under Part 4 of the DPA 2018; and
- processing that is purely in the context of personal or household activities, such as household CCTV within the boundaries of private property.

Note: The UK GDPR and DPA 2018 apply to information captured by surveillance systems. This guidance does not cover the use of 'dummy' or non-operational systems as no personal data is likely to be processed. However, it does cover pilots or trials where personal data is processed.

The use of conventional cameras (not CCTV) by the news media or for artistic purposes, such as for film making, are also not addressed by this guidance. This is because an exemption within data protection legislation applies to certain activities relating to journalistic, artistic and literary purposes. However, this guidance does apply to information collected by surveillance systems that is then provided to the media.

Surveillance systems vary substantially, as do the extent and reasons for use, and how personal data is processed. Therefore not all sections of this guidance are relevant in all cases. A checklist within this guidance for limited surveillance systems provides particular assistance in circumstances where privacy risks are small and resources are limited. To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. If you use video surveillance in a limited way but you wish to use your surveillance system for a new purpose, you should read the full guidance.

Further Reading

 [Relevant provisions in the legislation - See UK GDPR Articles 4\(1\), 4\(14\) !\[\]\(fcaee6d397c07452e54229b176f1295d_img.jpg\)](#)

External link

Further reading

[Website for the Biometrics and Surveillance Camera Commissioner !\[\]\(51514032c8ca341817228f39f1307b05_img.jpg\)](#)

What are our responsibilities in terms of accountability?

At a glance

Under the UK GDPR and DPA 2018, you have an obligation to implement appropriate technical and organisational measures. These show that you have considered and integrated the principles of data protection law into your processing activities. It is also important that you identify an appropriate lawful basis, and justify any processing to be necessary and proportionate.

If you are a controller, and your surveillance system is processing the personal data of identifiable individuals, you are required to notify and pay a data protection fee to the Information Commissioner's Office (ICO) unless exempt.

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance. Your accountability obligations are maintained throughout the life of the processing.

Specifically under Article 30 of the UK GDPR, organisations are required to maintain a record of the processing activities taking place. This applies to both controllers and processors that use surveillance systems. The records you keep should cover areas such as the purpose(s) for the lawful use of surveillance, any data sharing agreements you have in place and the retention periods of any personal data.

For surveillance systems, you must take a data protection by design and default approach and perform a Data Protection Impact Assessment (DPIA) for any processing that is **likely to result in a high risk** to individuals. This includes:

- processing special category data;
- monitoring publicly accessible places on a large scale; or
- monitoring individuals at a workplace.

You should assess whether your use of surveillance is appropriate in the circumstances. As part of your assessment, you should also take into account the reasonable expectations of the individuals whose personal data are processed and the potential impact on their rights and freedoms. You should record your considerations and mitigations in a DPIA prior to any deployment of a surveillance system that is likely to result in a high risk to individuals. If high risks cannot be mitigated, prior consultation with the ICO is required.

In detail

- [How do we ensure effective control of our surveillance systems?](#)
- [How do we demonstrate accountability?](#)
- [What is data protection by design and by default?](#)
- [How do we carry out a Data Protection Impact Assessment \(DPIA\)?](#)

- [What about documentation?](#)
- [Do we need to pay a data protection fee?](#)

How do we ensure effective control of our surveillance systems?

Checklist

- ☐ We know who has responsibility for the control of information within our organisation and who makes decisions about how it can be used.
- ☐ We have notified with the ICO if we are a controller, especially for the use of a surveillance system that processes personal data.
- ☐ We have agreed responsibilities if more than one controller is jointly involved in the processing, and each know their responsibilities in a transparent manner.
- ☐ We have written contracts in place that clearly define the responsibilities of organisations that provide processing services for us.
- ☐ We make sure that information is only processed by others in accordance with our instructions, with guarantees about security, storage and the use of properly trained staff.

It is important that you establish who exercises **overall control** of the personal data being processed. For example, who decides what is to be recorded, how it should be used and to whom it may be disclosed if needed. If you are the organisation that makes these decisions determining the purpose and means of processing, then you are the controller and you are legally responsible for compliance with data protection law.

If you make joint decisions with another organisation about the purposes for, and operation of, the surveillance system then you are joint controllers for this processing. All joint controllers remain responsible for compliance with the controller obligations under the UK GDPR and DPA 2018. For further information see our [guidance on joint controllers](#).

Organisations may share information from a surveillance system in order to assist with joint running costs. This includes situations where the surveillance system is managed by a third-party on behalf of, or in conjunction with, another organisation. For example, this could be a CCTV server hosted by a council, and a feed could be linked into a local law enforcement control room.

The agreement to share services must have strict guidelines and procedures in place to ensure that the control and use of these systems is appropriate. In a shared service situation you should also make clear who is legally in control of what information at any given time.

As a controller, you need clear procedures to determine how you use the system in practice. You should therefore consider the following questions:

- Have you clearly defined the specific purposes for the processing of personal data and use of information? Have you communicated these to those who operate the system?

- Are there clearly documented procedures for how information should be handled in practice? This could include policies and procedures for disclosures and how to keep a record of any data sharing. Are these accessible to the appropriate people?
- Has responsibility for ensuring that procedures are followed been allocated to a data protection officer (DPO) or to an appropriate named individual? They should ensure that standards are set, procedures are put in place to meet these standards, and that the system complies with this guidance and other legal obligations.
- Are proactive checks or audits carried out on a regular basis to ensure that procedures are being complied with? This can be done either by you, as the system operator, or a third party.

How do we demonstrate accountability?

The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to **demonstrate** your compliance. Your accountability obligations are maintained throughout the life of the processing.

Article 24(1) of the UK GDPR says that:

- you must implement technical and organisational measures to ensure, and demonstrate, compliance with the UK GDPR;
- the measures should be risk-based and proportionate; and
- you need to review and update the measures as necessary.

The below headings expand on broader accountability obligations you must adhere to under data protection law.

What is data protection by design and by default?

Data protection by design and default is about considering data protection and privacy issues upfront, from the earliest stages of project planning. You must consider this in a consistent manner, in everything you do, where you are processing personal data. It can help you comply with the UK GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Under data protection law, you have an obligation to implement appropriate technical and organisational measures to show that you have considered and integrated the principles of data protection into your processing activities. [Data protection by design](#) has broad application. Examples include physical design, or developing organisational policies, processes, business practices or strategies that have privacy implications. This requirement is particularly important for the new or novel use of more intrusive surveillance systems such as ANPR, BWV and Facial Recognition Technology (FRT).

Prior to purchasing any surveillance system, you should make decisions based on its ability to provide a data protection compliant solution to a problem. You should not purchase a system because it is new, available, affordable or in the belief that it will gain public approval. You should also establish criteria for procuring systems and the decisions you make about deployment and configuration.


The [Biometrics and Surveillance Camera Commissioner's Buyers' Toolkit](#)  will also help you when planning and installing surveillance camera systems.

You should also ensure that the design of your surveillance system allows you to easily locate and extract personal data in response to individuals exercising their rights. For example, in response to subject access requests or for disclosures to authorised third parties such as law enforcement.

Example

An ambulance service wishes for staff to use a BWV system, so that staff can capture any abusive behaviour towards them when they are on duty. Prior to using the technology, the service should conduct a DPIA to assess whether the use of this technology is a necessary and proportionate response to a problem. The service should not purchase the system just because it is new or useful technology, but because the use of the system is justifiable in the circumstances.

It is also important that there is sufficient focus on the governance of the information that is collected, rather than the technical capability of the cameras. For example, how the information is safely stored, retained or edited if needed. Again, the service should have appropriate policies and procedures for the use of the technology and information collected, with appropriate training for staff who actually wear the cameras or subsequently process the information.

You may also wish to refer to the [Biometrics and Surveillance Camera Commissioner's secure by design, secure by default scheme](#)  which outlines requirements for manufacturers of surveillance camera systems and components.

How do we carry out a Data Protection Impact Assessment (DPIA)?

To identify and help mitigate risks at an early stage you should perform a DPIA prior to any processing. This 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.

For surveillance systems in particular, you **must** perform a DPIA with balanced consideration for any type of processing that is **likely to result in a high risk** to individuals. To assess the level of risk, you should consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. For example this could involve unexpected or unfair monitoring, or particular decision making against an individual. We have further [guidance about the types of risks that DPIAs address](#).

Your DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

If you decide to not do a DPIA you need to document your reasons and be prepared to justify why the processing is not of a type likely to result in high risk. You can use our [screening checklists](#) to help you

decide.

- You need to consider the privacy issues involved with using new surveillance systems, such as lawfulness and transparency. You should assess whether the use is necessary and proportionate and appropriately solves a problem. You should always consider less privacy intrusive methods of achieving this need where possible, or explain why these alternatives are not suitable or sustainable.
- You should also look at the problem the surveillance system is supposed to address, and show whether or not the system will meet this need. You should base your assessment on reliable evidence and show whether the proposed surveillance system can be justified as proportionate to the problem identified.

The Biometrics and Surveillance Camera Commissioner's predecessor and the ICO jointly published the [SCC DPIA template and associated guidance notes for surveillance systems](#). The ICO has also produced [detailed guidance for conducting DPIAs](#).

For the purposes of using surveillance systems, you may encounter data protection problems if you fail to take a data protection by design and default approach and do not conduct a DPIA where required. You could avoid these problems by acting at an early stage.

There are also wider benefits in terms of identifying problems early and avoiding unnecessary costs and reputational damage. Further, a failure to carry out a DPIA when required in itself infringes the UK GDPR and may leave you open to enforcement action.

If you have carried out a DPIA that identifies a high residual risk after mitigation measures, you are required to consult with the ICO under data protection law. You cannot go ahead with the processing until you have consulted us. If you have established methods to reduce or mitigate the risk so it is no longer high, you do not need to consult us.

What about documentation?

Checklist

- ☐ If we are a controller for the personal data we process using surveillance systems, we document all the applicable information under Article 30(1) of the UK GDPR.
- ☐ If we are a processor for the personal data we process using surveillance systems, we document all the applicable information under Article 30(2) of the UK GDPR.
- ☐ We conduct regular reviews of the personal data we process and update our documentation accordingly.
- ☐ Our documentation is readily available if it is requested by the ICO, or another regulatory authority.

Documenting your processing activities is a legal requirement under data protection law. It can support good data governance and help you demonstrate your compliance with the UK GDPR and DPA 2018. Knowing what information you have, where it is and what you do with it makes it much easier for you to comply with other aspects of the law. For example, making sure that the information you hold about people

is accurate, relevant and secure.

Under Article 30 of the UK GDPR, most organisations are required to maintain a record of their processing activities. This also applies to controllers and processors that use surveillance systems. The records you keep should cover areas such as the purpose(s) for the use of surveillance, data sharing and retention.

[Further guidance and templates about documentation](#) are on our webpages.

The UK GDPR and DPA 2018 also outline the legal requirement for an appropriate policy document to be in place when processing [special category](#) and criminal offence data under certain specified conditions.

This document should demonstrate that the processing of any special category and criminal offence data is compliant with the requirements of the UK GDPR Article 5 principles.

Read [further guidance about appropriate policy documents and special category and criminal offence data](#).

Do we need to pay a data protection fee?

If you are acting as a controller, and your surveillance system is processing the personal data of identifiable individuals, you are required to notify and pay a data protection fee to the ICO, unless exempt.

The Data Protection (Charges and Information) Regulations 2018 outline the different tiers of fee controllers are expected to pay. The fees are set by Parliament to reflect what it believes is appropriate based on the risks posed by the processing of personal data by controllers.

In the context of video surveillance, if you are processing images of identifiable individuals outside of purely personal, family or household use, then you may be required to pay a data protection fee and notify with the ICO as a controller.

Read further guidance about the [data protection fee](#).

How can we comply with the data protection principles when using surveillance systems?

At a glance

Article 5 of the UK GDPR sets out seven key principles. These principles should lie at the heart of your approach to processing personal data. When using surveillance systems, you can encounter data protection problems if your focus is on technical capability over the transparency of the processing or the governance of information. Therefore, you need to consider each aspect equally.

For any use of surveillance systems, you need to identify and document a lawful basis under Article 6 of the UK GDPR. In practice, it is often difficult to obtain genuine consent from individuals for processing their personal data in public spaces. Therefore, it is likely the appropriate lawful basis will be either legitimate interests, or a reliance on public task (if you are carrying out your tasks as a public authority in the public interest or under official authority). A [legitimate interests assessment](#) (LIA) can help you demonstrate lawfulness of the processing, and can naturally feed into a DPIA.

You need to identify an Article 9 UK GDPR condition, if you are actively processing [special category data](#), such as biometric data (for example when using facial recognition systems to **uniquely identify** individuals). If you process criminal conviction data, you need to comply with Article 10 UK GDPR.

The type of surveillance system you choose and the location it operates within must achieve the specific purpose(s) for which you are using it.

The information your surveillance system processes must be of good quality and be adequate, relevant and limited to what is necessary. You should identify the minimum amount of personal data you need to fulfil your purpose(s).

The UK GDPR and the DPA 2018 do not prescribe any specific minimum or maximum retention periods which apply to surveillance systems or the information you may process. Rather, it is the purpose of your processing that should determine your necessary retention period.

You should store recorded information securely in a way that maintains its confidentiality, integrity and availability. This is to ensure that you protect the rights of individuals you record by surveillance systems and use the information effectively for your intended purpose.

In detail

- [What should we generally consider when using surveillance systems?](#)
- [How do we demonstrate lawfulness, fairness and transparency?](#)
- [How do we comply with the purpose limitation principle?](#)
- [How should we minimise the information we process, and ensure its quality?](#)
- [What about the retention of information?](#)
- [How should we securely store and view the information our surveillance system processes?](#)

What should we generally consider when using surveillance systems?

Modern surveillance systems can offer:

- greater clarity of images with high definition picture;
- improved capability due to the size and positioning of lenses; and
- additional functions to post footage online or share information with others in real time.

As such, surveillance systems can be particularly intrusive. Especially if they impact on the private lives of individuals and process personal data beyond their reasonable expectations.

Some systems are also capable of placing large numbers of people under surveillance as they go about their day-to-day activities. For example, this may include the use of ANPR or facial recognition technology in public spaces.

Regardless of the size of the system, you should initially consider achieving your outcome using alternative, less privacy intrusive methods. You may consider that new technology is an attractive or affordable solution. However, the use of surveillance systems should be a necessary and proportionate response to the problem you are addressing. You should therefore carefully consider whether or not to use a surveillance system, if other options are available.

Example

A disused public space is subject to vandalism and antisocial behaviour, and a local authority installs a surveillance system to try and monitor the area.

In order to reduce the amount of CCTV in the area, the local authority may wish to first consider less intrusive alternatives to surveillance systems. For example, improved lighting, fences and improvements to the area to encourage regeneration. This may also discourage antisocial behaviour if the space is used more often by the wider community.

Both fixed and mobile cameras should be focussed on a relevant space, and where wider surveillance is possible but unnecessary, this should be restricted. This ensures that surveillance does not occur in areas which are not of interest and individuals are not unintentionally made the subject of surveillance.

Example

A café installs a surveillance system which captures the entrance of the premises to improve its security, as there have been reports of break-ins in the local area.

When reviewing the system, the café owner realises that the camera's field of vision also captures footage of a nearby flat, and can see into the property.

The café owner adjusts the field of vision so that the focus of the recording is restricted only on the

café entrance to avoid any unnecessary privacy intrusion to nearby residents.

[Article 5 of the UK GDPR](#) sets out seven key principles that should lie at the heart of your approach to processing personal data.

You should carefully consider whether it is appropriate to use a surveillance system, and assess any potential impact this may have on the rights and freedoms individuals have under data protection law.

It is also important that you identify an appropriate lawful basis under the UK GDPR and DPA 2018. You should clearly document and justify your reliance on a particular lawful basis in conjunction with the principles of data protection law prior to any deployments.

As previously mentioned, for the use of surveillance systems you must perform a DPIA for any type of processing that is **likely to result in a high risk** to individuals. This is a legal requirement and applies in most cases, due to the inherent privacy risks involved in the use of surveillance systems as a type of processing. [See section on DPIAs](#).

How do we demonstrate lawfulness, fairness and transparency?

Lawfulness

Checklist

- ☐ We have identified an Article 6 lawful basis for the processing of personal data under UK GDPR.
- ☐ We have also identified an Article 9 UK GDPR condition for the processing of any special category data, especially where the unique identification of individuals occurs.
- ☐ We have identified an appropriate DPA 2018 Schedule 1 condition where specifically required for the processing of special categories of personal data or criminal conviction data.
- ☐ Where relevant, we have identified our authority for any processing of criminal offence data under Article 10 UK GDPR.
- ☐ Where required, we have a readily available appropriate policy document (APD) that demonstrates the above.

For any use of surveillance systems you need to identify and document a lawful basis for processing under Article 6 of the UK GDPR. In practice, it is difficult to obtain genuine consent from individuals that are subject to video surveillance in public spaces. Therefore, it is likely the appropriate lawful basis will be either legitimate interests, or a reliance on public task (if you are carrying out your tasks as a public authority in the public interest or under official authority). A [legitimate interests assessment](#) (LIA) can help you demonstrate lawfulness of the processing, especially if you are not carrying out a DPIA. You must however independently identify an appropriate lawful basis that best suits your organisation or method of processing.

You need an Article 9 UK GDPR condition, if you are actively processing [special category data](#), such as biometric data (for example when using facial recognition systems to **uniquely identify** individuals). There are 10 conditions for processing special category data in Article 9 of the UK GDPR. Five of these require you to meet additional conditions and safeguards set out in UK law, at Section 10 and in Schedule 1 of the DPA 2018. If you record footage involving criminal offence data, you also need to comply with Article 10 of the UK GDPR, Section 10(5) of the DPA 2018 and identify an appropriate condition under Schedule 1 of the DPA 2018. For more information see our [guidance on criminal offence data](#).

Example

A shop manager suspects an employee of stealing money from the till. The manager compiles a report showing the shifts of the individual and collects CCTV footage of them at the till during those shifts.

This personal data is criminal offence data as it relates to the alleged commission of an offence which is unproven and requires compliance with Article 10 UK GDPR.

In some circumstances, the UK GDPR and DPA 2018 also require you to have supporting documentation that explains how you demonstrate lawfulness, in the form of an 'appropriate policy document'. Read further [guidance about documentation](#).

Fairness

Processing of personal data must always be fair as well as lawful. If any aspect of your surveillance is unfair you will be in breach of this principle – even if you can show that you have a lawful basis for the processing.

In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.

Naturally, there are places where individuals have a heightened expectation of privacy, such as private property. But also in public toilets and changing rooms, where the use of visual or audio recording would not be expected and often difficult to justify. If you are considering surveillance systems in these environments, you should only use them in the most exceptional circumstances, where it is necessary to deal with very serious concerns.

Example

An individual walks down a public shopping precinct and expects to be captured on CCTV that is installed for the prevention or detection of crime. When entering a shop, the shop also has a CCTV system installed for similar reasons. But the individual may not expect there to be a camera in the changing rooms where there is often a heightened expectation of personal privacy.

You always need to ensure that those under surveillance are clearly aware that they are being recorded. You should provide individuals with appropriate information about how they can exercise their rights, and that appropriate restrictions on viewing and disclosing images are in place for those using the system.

You need to assess whether the individual can reasonably expect the processing. In particular, you need to take into account when and how you collect the information. This is an objective test. 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.

In terms of the use of surveillance systems, you need to recognise whether you are using a new technology or processing data in a new way that an individual may not reasonably anticipate. Or conversely, whether there are any developments in technology or updates to services that individuals have come to expect. Again, you should reflect this risk assessment in a DPIA prior to any deployment of a surveillance system.

By installing surveillance systems in areas where people have greater expectations of privacy, you may inadvertently increase the intrusion on their private life, especially where their behaviour is not modified. The use of surveillance systems in public spaces may also have a chilling effect on the way in which people behave, interact with each other, or the places that they choose to move freely. It is important that you also consider these issues when planning to use new or existing systems and whether they can be justifiable set against the purpose(s) for the processing.

Example

A business responsible for managing a public multi-storey car park wishes to use CCTV cameras around the premises and in the elevators, to ensure the safety and security of individuals using them. Those using the car park are likely to expect CCTV cameras for general safety reasons, but also in areas where a crime could possibly occur.

The owners of the car park should ensure that there is appropriate signage that people can read within, and prior to entering, the premises. It should include details of the organisation operating the system, the purpose for using it and who to directly contact in the event of a query.

Example

A school wishes to install CCTV cameras in the toilets in order to prevent vandalism.

The school would have to make a rigorous assessment based on necessity and proportionality in order to justify the processing. This is because the cameras would be recording children, particularly in an environment where there would be a natural and heightened expectation of privacy by both students and parents. Given the potential level of intrusion, this use is unlikely to be proportionate in most circumstances. The school should seek less privacy intrusive measures in order to solve a particular

problem.

Transparency

Checklist

- ☐ We have signs that accompany our surveillance system that are clearly visible and readable, explaining that its use is in operation.
- ☐ We include details of the organisation operating the system, the purpose for using the system and who to directly contact about its use.
- ☐ We include as a minimum basic contact details such as a website, telephone number or email address.
- ☐ We have signs that are an appropriate size depending on the context of the systems use. For example, whether the signs are viewed easily by pedestrians or drivers.

The need for transparency is a fundamental aspect of data protection law. You must tell people when you are capturing their personal data, where appropriate. However, it is recognised that the use of surveillance systems often presents challenges for providing individuals with privacy information. For example, it could prove difficult to ensure that an individual is fully informed of recording taking place if:

- you are using a drone at altitude;
- the surveillance system is attached to a person's uniform; or
- the system is fixed in a location that individuals would not reasonably expect.

If you operate a surveillance system you are likely to collect personal data directly from the individuals you monitor. As a result you need to comply with data protection law, in particular Article 13 of the UK GDPR. This means you need to find a way to provide them with information about the surveillance. In any case, you must let people know when they are in an area where a surveillance system is in operation. You can also back up messages with an audio announcement, if public announcements are already used, such as in a train station or onboard public transport.

An effective way to provide transparent information is to place signs prominently before the entrance to the system's field of vision and reinforce this with further signs inside the area. You should position information at a reasonable distance from the places monitored, and in such a way that individuals can easily recognise the circumstances of the surveillance before entering the monitored area. For example, it is not considered fair for an individual to read a sign that warns them about particularly intrusive surveillance technology in the area, if the system has already captured them whilst reading it.

Example

It may be useful to use websites or social media to inform individuals that certain types of surveillance systems are in operation at a specific time and in a specific area. It is important to note however that publishing information on a website, by itself, is not enough to comply. You have to draw the individuals' attention to the information. Therefore, you could use physical signage with linked information, so that individuals can find out more if they are interested. This would essentially function as a layered privacy notice.

As a general rule, signs should be more prominent and frequent in areas where people are less likely to expect that they will be monitored by a surveillance system. For example, this is particularly important when you are using a system to cover a large public area and capture a large amount of personal data.

Example

A construction company uses traditional CCTV alongside security guards within the perimeters of a building site. This is to protect the site operatives, and nearby members of the public from any harm. The CCTV system provides extensive monitoring across the site, and the footage records the activity of the members of staff stationed there.

The site includes large, prominent notices to inform individuals:

- about the CCTV system;
- that the cameras are there for the purposes of safety and security; and
- who to contact directly in the event of a query.

Signs do not need to say who is operating the system if this is obvious. If a surveillance system is installed within a shop, for example, it may be obvious that the shop is responsible. 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.

Example

Where processing is not obvious to an individual, a sign could read "Images are being monitored and recorded for the purposes of crime prevention and public safety. This system is controlled by XXXXX. For more information, visit our website at (web address) or call 01234 567890."

How do we comply with the purpose limitation principle?

Checklist

- ☐ We have initially considered achieving our outcome using alternative, less privacy intrusive methods without the need for surveillance systems.
- ☐ If we need to use a surveillance system, we only use it in locations where it achieves our specific purpose(s).
- ☐ We have assessed any potential impact the use of surveillance may have on the rights and freedoms individuals have under data protection law.
- ☐ We only use audio recording where there is an evidenced and justified need.
- ☐ Any audio capabilities in our system are switched off by default.
- ☐ We take additional steps to make it clear to individuals that audio recording is taking place, over and above any visual recording which is already occurring.

You must be clear about what your purposes for processing personal data are from the start under the UK GDPR and DPA 2018. You need to record your purposes as part of your documentation obligations and specify them in your privacy information for individuals.

When using surveillance systems, you can only use the personal data for a new purpose if:

- this is compatible with your original purpose;
- you get consent from individuals; or
- you have a clear obligation or function set out in law.

Audio recording

You should not normally use surveillance systems to directly record conversations between members of the public. This is highly intrusive and unlikely to be justifiable in most circumstances. In most situations, the use of audio recording, particularly where it is continuous, is considered more privacy intrusive than purely visual recording. Its use will therefore require a much greater justification and you should switch **off** by default any capability to record audio. You should only use it in exceptional circumstances, for example by a trigger switch.

If your system comes equipped with an independent sound recording facility, then you should turn this off or disable it in some other way, unless you can clearly justify and evidence its use. If you cannot control sound recording separately you need to consider how privacy intrusive the system is as a whole, including the recording of sound.

You should **only** use audio recordings when you have:

- identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- considered other less privacy intrusive methods of achieving this need;

- reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is through the use of audio recording.

You should take additional steps to make it clear to individuals that audio recording is taking place, over and above any visual recording which is already occurring.

Surveillance in the workplace

If you are an employer, there may be cause for you to consider using overt surveillance systems to monitor staff, for reasons of health and safety, public health or security.

This could involve installing traditional CCTV cameras that record staff performing a particular task, or installing systems to record employees entering or exiting a secure premises. However, it is likely that employees would not always reasonably expect to be monitored by video or audio surveillance systems in their day-to-day roles. In the case of audio monitoring, this guidance focuses on the recording of face-to-face or private conversations, rather than business telephone calls commonly used for monitoring or training purposes.

It is therefore important if you are using surveillance systems in the workplace, especially any use of audio recording, that you use them in **rare** circumstances. In addition, you must:

- consult with your workforce (eg staff and/or trade unions), especially during the DPIA process;
- ensure that there are adequate notices, or other means, to clearly inform employees about the nature and extent of surveillance and its purpose(s);
- ensure that you make people other than workers, such as visitors or customers, who may inadvertently be caught by monitoring, aware of its operation and why you are carrying it out;
- target any video or audio monitoring at areas of particular risk and confine it to areas where expectations of privacy are low;
- consider that continuous video or audio monitoring of particular individuals is only likely to be justified in the rarest of circumstances, and may involve other legal requirements outside data protection law for targeted monitoring;
- respect the individual rights staff have about their personal data, and provide a mechanism for them to raise complaints or concerns directly with you as their employer.

Example

An employer records incoming calls taken by employees in a call centre for training purposes, and this is known and accepted by staff. However, the employer also wishes to install video recording in a separate rest area, where staff can take breaks from work and interact.

This use of surveillance would not generally be expected by staff, and would be difficult to justify as a necessary or appropriate use by the employer. Such surveillance may also prevent staff from using the rest area, and may affect the way in which people behave and interact with each other. The employer should rethink the purposes of the recording, and should not install the system if there is no compelling justification for its use. Conducting a DPIA prior to any installation would also be a useful exercise to help identify a genuine need for monitoring and any associated risks.

Further reading – ICO guidance

[Employment practices code](#)

This legacy guidance is based on the DPA 1998 and may not include all the requirements of the UK GDPR.

Live streaming

You may choose to install a surveillance system, such as a webcam or even use a mobile phone app that provides access to live streaming functions. This does not necessarily record any footage or save any data to a storage device or the cloud. Instead, it streams the footage over the internet to be viewed in real-time.

The definition of processing is broad and means that it isn't limited to simply holding the data under the UK GDPR and DPA 2018. Collecting or viewing data in real time on a screen also qualifies as processing. This means that even though you are not storing the images captured on a live stream camera, it still constitutes the processing of personal data if you can identify individuals directly or indirectly.

Your processing may involve broadcasting a video stream (eg online) to an indefinite number of people. This live streaming of images of identifiable individuals is still subject to the requirements of the UK GDPR and DPA 2018.

Example

A property developer provides maintenance services for a block of flats. As part of the service, the controller decides to install a surveillance system that live streams footage of the corridors and entrances back to themselves without the knowledge of the residents.

The surveillance is likely to be unnecessarily intrusive and capture individuals visiting and leaving their

private apartments. Therefore, the streaming of this footage would not be justified, nor within the reasonable expectations of the residents.

Can we record and share an online meeting, event or a lesson that we host?

As technology helps organisations to stay more connected with staff, colleagues and students, it is important that the use of any video conferencing technology by organisations is fair and transparent. Attendees of an online meeting or students in a virtual lesson need to know how you are processing their data, as well as having appropriate choice and control over it.

If you are acting as a controller for the processing of personal data, even by a live stream, you are responsible for protecting the rights attendees have about their personal information. It is important that you are able to make a clear justification for its use based on necessity and proportionality. For example, if you are using video conferencing as a way to communicate with staff or to host a virtual lesson with students, or make a physical record of a specific interaction.

You should consider whether it is truly necessary in the circumstances to use video conferencing to live stream or record interactions. You should always consider if you could achieve the purpose by less privacy intrusive methods, such as audio only calls. If you feel that the use of video conferencing is necessary and helpful, such as for online schooling, then you must be able to justify and document your reasons for this type of processing.

In the interest of transparency, you must also tell individuals, or in some circumstances the parents of young students, what you are doing. This is so that they can raise any safeguarding concerns or objections should they wish.

Generally, it is not appropriate for you to post recordings online or make personal data available to an indefinite audience without the express permission of those recorded. If formal recording and publication of an interaction is required, you must clearly explain to the individual(s) what the purpose of the recording is. You must also ensure that you do not use the recording for any other incompatible purpose or disclose it to unauthorised third parties unless there is a justifiable reason.

You should also consider providing a secure link to a live stream or recording, that only attendees can view by a strong password, rather than placing it on an unsecured open website or social media platform for others to view.

How should we minimise the information we process, and ensure its quality?

Checklist

- ☐ We have checked that the personal data our surveillance system processes is adequate, relevant and is limited only to what is necessary in the circumstances.
- ☐ We have identified the minimum amount of personal data we need to fulfil our purpose.
- ☐ We have a surveillance system that can produce good, clear, quality images. The quality of the information collected is also maintained throughout the recording process.

- ☐ We have set up the system in such a way that information cannot be inadvertently corrupted.
- ☐ We have regular checks in place to ensure that the date and time stamp recorded on images is accurate (eg, when the UK switches between summer and winter time).
- ☐ We have procedures in place to ensure the accuracy of systems we use that match personal data, such as ANPR and Facial Recognition Technology (FRT).
- ☐ We have fully documented our use of any algorithms, AI or machine learning in our automated systems to assist with accountability requirements.
- ☐ We have considered the data protection implications of using other functions, such as audio recording, live streaming and cloud storage and we have further documented their use in our DPIA.

Under the UK GDPR and DPA 2018, you must ensure that the personal data you are processing is:

- adequate – sufficient to properly fulfil your stated purpose;
- relevant – has a rational link to that purpose; and
- limited to what is necessary – you do not hold more than you need for that purpose.

You should therefore identify the minimum amount of personal data you need to fulfil your purpose. You should hold that much information, but no more. For example, this could involve recording for a defined time period, or restricting the recording to a particular location.

It is also important that a surveillance system produces information that is of a suitable quality to meet the purpose(s) you installed it for. If the identification of individuals is a necessary part of the processing, then poor quality information that does not assist this purpose may undermine the reason for installing the system.

The decisions you make, and the reasons for selecting a particular surveillance system should not be based solely on technical capabilities. For example, the quality of the images it can produce, the field of vision it offers or the amount of data it can record. It is important that you also consider the governance capabilities that complement the system, such as software that enables footage to be uploaded, stored and audited. In addition, personal data should be easily retrievable in response to a subject access request and other individual rights. You should ensure that your systems have the capability to redact footage if third parties need to be blurred or obscured. See the section in this guidance on redaction for further information.

You can encounter challenges to compliance with data protection law if your focus is on technical capability over the transparency of the processing or the governance of information. You need to consider each area equally. You may feel constrained by what is available on the market in terms of surveillance systems, however this does not stop you from specifying the features you require and asking system providers to respond to these demands. This is supported by the UK GDPR (Recital 78), which explains that manufacturers of products and services that are based on the processing of personal data, should be encouraged to take into account the right to data protection when in development. This is an aspect of data protection by design and default.

Example

A controller chooses a Body Worn Video (BWV) system that allows video and audio recording to be switched on and off easily, to ensure that excessive information is not recorded continuously. In addition, the controller is able to efficiently upload necessary footage at the end of use in a secure manner, and retain it for a defined period.

In response to a subject access request, the controller is able to efficiently locate relevant footage and apply redaction techniques to protect the rights of third parties if required, within the statutory response times.

What about the retention of information?

Checklist

- ☐ We have decided on the shortest period that we need to retain the information for, based on our purpose(s) for recording.
- ☐ We have documented our information retention policy and it is readily available and understood by those who operate the system.
- ☐ We have measures in place to ensure the permanent deletion of information through secure methods.
- ☐ We undertake systematic checks to ensure that the retention period is being adhered to.

The UK GDPR and the DPA 2018 do not prescribe any specific minimum or maximum retention periods which apply to surveillance systems or the personal data you may process. Rather, it is the purpose of your processing that should determine your retention period. You should therefore be able to determine what your purpose for using a surveillance system is, and then how long you need to retain the data for. Personal data held for too long will, by definition, be unnecessary. You are therefore unlikely to have a lawful basis for such retention. It is key that you do not retain data for longer than is needed. Therefore your retention period should be the shortest period for that purpose. Where information is no longer needed, then you should delete it.

You should also not determine your retention period simply by the storage capacity of any surveillance system, or just in case you think the data may be useful in the future. For example, footage from a surveillance system shouldn't be kept for six months merely because the manufacturer's settings on the surveillance system allow retention for this length of time.

On occasion, you may need to retain information for a longer period for a specific purpose. For example, where a law enforcement agency is investigating a crime and asks for you to preserve it to give them an

opportunity to view it as part of an active investigation.

How should we securely store and view the information our surveillance system processes?

Checklist

- ☐ We can demonstrate that appropriate technical and organisational measures are in place that maintains the confidentiality, integrity and availability of the information captured from our surveillance systems.
- ☐ We ensure that access to footage is restricted only to authorised individuals.
- ☐ We can obtain copies of footage from our system in a timely manner, in a suitable format without losing image quality or time and date information.
- ☐ We are able to retrieve footage from our systems efficiently if it is requested for disclosures or for further examination, within relevant statutory timescales.
- ☐ We can demonstrate that the information we collect complies with designated technical standards.

You 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.

To do this, you need to carefully choose how you hold and record the information, and ensure that access is restricted only to authorised individuals. You also need to ensure that the information is secure and where necessary, encrypted. Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. However, there are circumstances where it is not always possible to apply encryption.

Where encryption is not achievable, then you should employ other appropriate technical methods to ensure the safety and security of information.

If you are going to collect and retain a large amount of information, (eg extended video footage), then you may consider storing the data in a cloud computing system. You need to ensure that this system is secure. If you have contracted a cloud provider to provide data storage, you need to ensure that the provider can offer sufficient security, and explore whether the sharing of personal data might amount to an international transfer (if the cloud provider is based abroad). The ICO has published [guidance on international data transfers](#) that covers this issue in more detail.

For accountability reasons, you may also wish to keep a record or audit trail showing how you handle information, if it is likely to be used as evidence for law enforcement purposes.

You should restrict the viewing of live surveillance on monitors to the operator and any other authorised person, unless the monitor displays a scene which is also in plain sight from the monitor location. You should also view recorded surveillance footage in a restricted area, such as a designated secure office.

Example

A CCTV system is installed in a hotel for the purposes of security, with monitors at the hotel reception area showing guests in the corridors and lifts, (i.e. out of sight of the reception area).

The monitors should be positioned so that they are only visible to relevant staff. Members of the public should not be allowed access to the area where staff can view them.

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.

Where possible you should aim to document procedures and ensure you review them regularly. This is to ensure you maintain the standards you established during the setup of your system.

Similarly, you should build in a periodic review of your system's effectiveness to ensure that it is still doing what it was intended to do. If it does not achieve its purpose, you should stop the processing until you modify the system accordingly. The timescale for such a review depends on your organisation's circumstances, but could include a regular monthly review or a much longer timescale if appropriate.

Further reading

- [ICO encryption guidance](#)
- There is further information in the [ICO's guidance on the use of cloud computing](#).

Additional considerations for technologies other than CCTV

Advances in technology and software mean that surveillance systems can pose an increased risk to people's privacy in both the public and private sectors. This section covers developing and pre-existing technologies, and also highlights additional considerations when using surveillance systems to process personal data, with good practice recommendations you should follow in order to comply with the UK GDPR and DPA 2018.

Surveillance technologies can be interconnected, which means that information can be shared or linked easily. If you are intending to match data together from different systems, you need to be careful that the information you are collecting is:

- accurate;
- not excessive;
- used only for defined purposes; and
- the use is still necessary and proportionate throughout the lifecycle of the processing.

Some systems also allow for data to be integrated into broader 'big data' processing systems that your organisation may operate. This has implications in terms of profiling, what you can learn about individuals and how you make decisions about them. The ICO published a [report on the data protection implications of big data](#) that covers this issue in further detail.

In detail

This guidance specifically covers:

- [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](#)

Automatic Number Plate Recognition (ANPR)

Checklist

- ☐ We have identified a genuine need to read Vehicle Registration Marks (VRMs) from vehicles using public or private roads and car parks, in a way that is fair, lawful and transparent.
- ☐ We have conducted a Data Protection Impact Assessment (DPIA) that fully addresses our use of

ANPR, and explores any impact on the rights and freedoms of individuals whose personal data are processed.

- ☐ We keep the number of ANPR cameras we use to a minimum, to ensure that we only use the appropriate amount in a specific area to address a particular need.
- ☐ We ensure that the location(s) of our cameras are fully justifiable, and are placed in such a way that they do not accidentally capture any vehicles that are not of interest.
- ☐ We have clear and prominent signage in place to inform individuals that ANPR is in use, with sufficient detail about who to contact if they have a query.
- ☐ We have appropriate retention and disposal policies in place for any vehicle data we process.
- ☐ We have efficient governance procedures in place to be able to retrieve stored data and process it for subject access requests or onward disclosures where required.
- ☐ Where we process other supplementary data for the purpose of matching data obtained from cameras, we ensure that it is kept up-to-date and relevant to the purpose of the ANPR system.
- ☐ We comply with the [Surveillance Camera code of practice](#) where required.

Automatic Number Plate Recognition (ANPR) systems have the ability to collect and analyse large quantities of personal data in real time. Cameras process personal data when vehicles drive past their field of vision. Despite ANPR being more commonly used by law enforcement, these systems are also used by privately-owned car parks and other businesses. Millions of number plates have the potential to be scanned and cross-referenced with live databases across the UK. Due to the increasing affordability of these systems, its use in both the public and private sectors are popular.

ANPR systems generally capture:

- images of vehicles (an overview image);
- images of the vehicle's number plate (the plate patch); and
- the vehicle registration mark (VRM)

ANPR systems also commonly supplement data collected from their cameras with additional information, such as the date, time and location of the vehicle. It is therefore important that you are aware of your responsibilities around processing personal data.

Is a Vehicle Registration Mark (VRM) personal data?

A VRM is a unique mark linked to a specific vehicle, displayed on its number plate. Surveillance technologies such as CCTV and ANPR can process VRMs for law enforcement purposes or civil matters, such as parking enforcement.

In most circumstances, a VRM is personal data. However, this can depend on the context of the processing. A VRM is personal data at the point where you collect it, if you process it as part of a surveillance system for the purposes of identifying an individual (potentially to take some action, such as to serve them with a parking fine).

This is because while the VRM may not directly identify a living individual, the purpose of the system means that you are likely to find out further information. This will enable you to identify either the driver, registered keeper or both.

How should we use ANPR?

Regardless of the sector you operate in, if you are using or intend to use an ANPR system, it is important that you undertake a DPIA prior to deployment. You should show that the use is necessary and proportionate in the circumstances, and that you have minimised the risks. This is particularly important given the amount of data an ANPR system can collect in a relatively short amount of time. You should also ensure that the information your ANPR system processes is limited to what you need to achieve your purpose, and that you are able to justify your decisions surrounding the data it captures.

When storing the information and cross-referencing it with other databases to identify individuals, you need to keep these databases:

- up-to-date;
- accurate; and
- of sufficient quality to prevent mismatches.

Similarly, both the cameras and any algorithms you use to determine a match must be of sufficient quality to prevent any misidentification of a VRM.

If you intend to share the personal data you process with third parties you need to make sure that doing so is lawful. We also advise you to have a data sharing agreement in place. This agreement should ensure that you have appropriate safeguards in place to keep the information secure, and that the amount of information you share is limited to what is necessary. Read further guidance about data sharing in our [data sharing code](#).

You also need to have appropriate retention periods in place for the personal data you collect and store through your ANPR system. The retention periods should be consistent with the purpose you are collecting the data for. You should only keep the data for the minimum period necessary and should delete it once you no longer need it. For example, this could apply to personal data stored for vehicles that are no longer of interest.

Example

A gym uses an ANPR system that processes VRMs to monitor use of its car park when there is a two-hour parking limit. The system retains the details gathered from the ANPR system for those cars that have exceeded the time limit, but also about those who have not exceeded the parking limit.

It is likely there is no need to retain information for an extended period for vehicles that have adhered to the time limit. It would be unnecessary and excessive to do so, unless there was a justifiable reason. If not, the extended retention of this information is unlikely to comply with the data protection principles.

The gym would need to amend the system to ensure that they delete any information about vehicles

that are not of interest, as soon as appropriate.

Signage

In keeping with the principle of fairness and transparency, it is important that you inform individuals you are processing their personal data. The best way to do this is through clear and visible signage explaining that ANPR recording is taking place and, if possible to do so, the name of the controller collecting the information. While it is a challenge to inform motorists that they are being overtly monitored, there are methods you can use, such as physical signs at entrances, posts on official websites and social media.

You must provide appropriate signs to alert drivers to the use of cameras on the road network or in areas that vehicles have access to, such as car parks. It is important that these signs do not affect the safety of road users. You should consider the amount of time the driver will have to read the information you provide; particularly where the road has a high speed limit.

Signs must make clear that cameras are in use and explain who is operating them. This means that individuals know who holds information about them and therefore have the opportunity to make further enquiries about what is happening with their data.

Further reading

We have further [guidance on 'what is personal data'](#).

Body Worn Video (BWV)

Checklist

- ☐ We have conducted a Data Protection Impact Assessment (DPIA) that fully addresses our use of BWV, and addresses any impact on the rights and freedoms of individuals whose personal data are captured.
- ☐ We provide sufficient privacy information to individuals before we use BWV, such as clear signage, verbal announcements or lights/indicators on the device itself and have readily available privacy policies.
- ☐ We train any staff using BWV to inform individuals that recording may take place if it is not obvious to individuals in the circumstances.
- ☐ We have appropriate retention and disposal policies in place for any footage that we collect.
- ☐ We have efficient governance procedures in place to be able to retrieve stored footage and process it for subject access requests or onward disclosures where required.
- ☐ We have the ability to efficiently and effectively blur or mask footage, if redaction is required to protect the rights and freedoms of any third parties.

Body Worn Video (BWV) involves the use of cameras that are worn by a person, and are often attached onto the front of clothing or a uniform. These devices are capable of recording both visual and audio information. Due to BWV's increasing affordability, many different organisations in the public and private sectors can purchase and use such equipment.

BWV has the ability to capture footage and audio in close proximity to individuals, and can also be used to record in new or novel ways. This type of surveillance therefore has the potential to be more intrusive than conventional CCTV systems. Scenarios could include face-to-face on doorsteps, on public transport or inside buildings such as homes and shops. This versatility therefore increases the risk of privacy intrusion to individuals.

Before you decide to procure and deploy such a system, it is very important that you justify its use and consider whether it is necessary, proportionate and addresses a particular need. If you are going to use audio recording as well as visual recording, the collection of audio and video needs to be justifiable. The use of BWV therefore requires you to undertake a DPIA.

BWV devices have the ability to be switched on or off, but it is important to know when and when not to record. Continuous recording requires strong justification as it is likely to:

- be excessive; and
- capture others going about their daily business, as well as the individual who is the focus of your attention.

Some BWV devices offer the ability to continuously buffer recording, so if you turn it on it may also have recorded the previous few seconds. It is important that you ensure any buffered recording is not excessive, and you only record the amount of footage you intend to.

Remember that the presence of audio recording adds to the privacy intrusion. You will require further justification if you are thinking about recording in more sensitive areas, such as private dwellings, schools and care homes. In such circumstances, the need will have to be far greater in order for the use of BWV systems to be proportionate. The operator will need to provide more evidence to support its use in these situations.

Example

It may be appropriate for a security guard to switch on their BWV camera when they believe an individual is being aggressive towards them. However, it may not be appropriate to switch it on when an individual is merely asking for directions.

If you want to use both video and audio recording, the most privacy-friendly approach is to purchase a system where you can control and turn them on and off independently. You should consider these two types of data processing as separate data streams. Therefore you should consider controlling them separately to

ensure that you do not process irrelevant or excessive data. It is important that you identify a BWV system which has the ability to be controlled in this way at the procurement stage.

If your BWV system cannot record audio and video separately, you should only use it when you can justify the recording of audio and video together in the circumstances.

Providing privacy information

If you use BWV systems, you should be able to provide sufficient privacy information to individuals. As BWV cameras can be quite small or discreet, and could be recording in fast moving situations, individuals may not be aware that they are in fact being recorded.

You should think of ways to provide further information to individuals in order to make them aware of recording. For example, you should:

- inform or verbally announce to individuals that the recording of video or audio or both is about to take place, and the reasons why, prior to turning on the BWV device;
- place visible signage or a warning light on the device or uniform, to indicate that the device is switched on and recording; or
- if more appropriate in the circumstances, direct individuals to the privacy notice on your website, if you have one.

Security and governance

Due to the versatility of the technology and the specific circumstances where they can be used, BWV cameras can also process special category data that could be more sensitive. Processing special category data can increase the risks to individuals. This means you are more likely to need to do a DPIA for the processing. Due to the nature of this data, it is important that you have appropriately assessed the level of risk involved and implemented robust technical and organisational measures, including physical security, to mitigate them. Read further [guidance about special category data](#).

For example, you should consider the use of [encryption](#), whether this involves the device itself or the storage medium. (Where this is not appropriate, you should have other ways of preventing unauthorised access to information.) In addition, you should consider designs that have robust technical security measures, for example BWV that do not have removable memory cards, to further reduce the risk of loss or compromise of data if a device is stolen or misplaced.

The **governance** of the information that you collect is particularly important, as BWV cameras can process information in isolation, or as part of a larger workflow. You therefore need to make appropriate decisions about the retention and disposal of information, alongside retrieval of information and staff training. For example, staff training can be tailored for individuals who use the cameras. This could include knowing when to record, processing recorded information safely and securely, and responding to queries and requests from the general public.

You need to ensure that you can securely store all of the data you capture and have appropriate policies in place for the storage. The policy must set out:

- how long you should keep the information for (this should be the shortest time necessary for your purpose); and

- when you no longer require it, when to appropriately dispose of it

You should store the information so that you can easily identify, locate and retrieve recordings relating to a specific individual or event. You should also store it in a way that remains under your control, retains the quality of the original recording and is adequate for the purpose you originally collected it for.

If you will be regularly sharing recorded information with a third party, then we advise you to have a data sharing agreement in place. For further guidance, see our [data sharing code](#).

You also need to consider any steps you must take when individuals exercise their rights, particularly when doing so could affect the rights of others. For example, responding to a subject access request for footage that involves individuals other than the one making the request. This may require you to apply video and audio **redaction** techniques in some circumstances. Some techniques may include blurring, masking, or using a solid fill to completely obscure parts of the footage. For further information see the dedicated sections in this guidance on redaction and responding to subject access requests.

Unmanned Aerial Systems (UAS) / Drones

Checklist

- ☐ We have considered whether there is a genuine need for us to use a drone, if alternative systems or methods of surveillance are not suitable to solve a particular problem.
- ☐ We have conducted a Data Protection Impact Assessment (DPIA) which includes the risks associated with recording at altitude, and capturing footage of individuals that are not intended to be the focus of our surveillance.
- ☐ We have registered our drone if the system falls within the specific criteria set by the Civil Aviation Authority (CAA). See the [CAA website](#) for further details about registration.
- ☐ We have robust policies and procedures in place for the use of drones, and our operators are appropriately trained, with documented credentials.
- ☐ We inform individuals that we are using a drone where possible, and we have an accessible privacy notice that individuals can read to learn more about our use.
- ☐ We comply with the [Surveillance Camera code of practice](#) [↗](#) where required.

What are Unmanned Aerial Systems (UAS) / Drones?

Drones are otherwise known as Unmanned Aerial Systems (UAS), Unmanned Aerial Vehicles (UAVs) and Remotely-Piloted Aircraft Systems (RPAS). They are lightweight unmanned aircraft commonly controlled by operators or onboard computers, which can also be controlled by operators. Drones can be used in many innovative ways, for example for photography, the geographical mapping of an area or searching for missing people. But they have raised privacy concerns due to their manoeuvrability and enhanced capabilities of taking photos, videos and sensing the environment. Using drones can result in the collection, use, or sharing of personal data, including information about individuals who are not the intended focus of

the recordings.

Smaller models in particular, can be easily purchased online or on the high street by businesses and members of the public. There is a distinction between those individuals who can be considered as 'hobbyists' and are therefore generally using their device for purely personal activities, and those individuals or organisations who use the device for professional or commercial purposes.

In contrast, organisations using drones are clearly controllers for any personal data that the drone captures, and therefore are required to comply with data protection law.

Providing privacy information

A key issue with using drones is that, on many occasions, individuals are unlikely to realise they are being recorded or be able to identify who is in control. If you are a controller, you must address the challenge of providing [privacy information](#) if you decide to purchase and use such surveillance systems.

You need to come up with innovative ways of providing this information to individuals whose information is recorded, and be able to justify your approach. Or, if doing that is very difficult or would involve disproportionate effort, document this information in a way that is readily available. Some examples could involve:

- formally registering your drone with the Civil Aviation Authority (CAA);
- placing signage in the area you are operating a drone explaining its use; and
- having a privacy notice on a website that you can direct people to, or some other form of privacy notice, so individuals can access further information.

How do we record information responsibly?

The use of drones has the potential for 'collateral intrusion' by recording images of other individuals unnecessarily. This can therefore be privacy intrusive. For example:

- The likelihood of recording individuals inadvertently is increased, because of the height drones can operate at and the unique vantage point they afford.
- Individuals may not always be directly identifiable from the footage captured by drones, but can still be identified through the context they are captured in or by using the device's ability to zoom in on a specific person.

As such, it is very important that you can provide a strong justification for their use. Performing a robust DPIA will help you decide if using a drone is the most appropriate method to solve a problem that you have identified.

It is important that you can switch on and off any recording or streaming system on a drone, when appropriate. Unless you have a strong justification for doing so, and it is necessary and proportionate, recording should not be continuous. You should look at this as part of your DPIA.

As always, you should consider the wider context you are using the drone in, rather than just the use of the drone itself. For example, does it connect or interface with other systems. You should also ensure that you store any data you have collected securely. For example, by using encryption or another appropriate method of restricting access to the stored information. This is particularly important if the drone is piloted beyond visual line of sight or crashes, and there is potential for the device and the data to be lost or stolen

as a result. You should also ensure that you retain data for the shortest time necessary for its purpose and dispose of it appropriately, when you no longer require it.

You may be able to reduce the risk of intrusion of others by incorporating data protection by design methods. For example, you may be able to procure a device that has restricted field of vision, or only records after the drone has reached a certain altitude. You can incorporate data protection by design and default into your DPIA and it can form part of your procurement process.

Do I have to register my drone?

Subject to certain permissions and exemptions for certain users, there are UK requirements for people who fly or are responsible for small unmanned aircraft, including drones and model aircraft. Further information about drone registration in the UK can be found on the [CAA's Drone Safe website](#).

Example

A local authority wishes to deploy a drone over a seaside resort to monitor public beaches for crowd movement and littering. Naturally, any visitors to the beaches may not reasonably expect to be recorded, especially if they are swimming, sunbathing or there are children present.

The local authority needs to make a strong justification for any recording, based on the sensitivity of the processing. They should take a risk-based approach by carrying out a DPIA before using the technology. This will help assess necessity and proportionality.

If recording does occur in a manner that is compliant with individuals rights and aviation rules, the local authority is required to provide the general public with appropriate information about the recording. They would also need to include information about who is responsible, how to contact them, and how individuals can exercise their rights if needed.

Example

A building surveyor uses a drone in a residential area to inspect damage to a roof. The surveyor wishes to use a drone because the high resolution images allow for a safer and more cost effective way of working.


In keeping with the principles of data protection law, the surveyor makes a risk-based assessment prior to deployment. They assess how to fly the drone in a way that does not affect the rights and freedoms of individuals. In order to prevent the unintended filming of residents, the surveyor only begins recording at altitude, and does not record any other private property, with the focus being on the roof.

The surveyor also ensures that, where possible, they provide individuals with links to their privacy information or website via temporary signage, and that any operators are fully trained and registered in

keeping with Civil Aviation Authority (CAA) requirements.

Facial Recognition Technology (FRT) and surveillance

Checklist

- ☐ We have conducted a Data Protection Impact Assessment (DPIA) that fully addresses our need to use Facial Recognition Technology (FRT), the lawful basis for its use and explores the impacts on the rights and freedoms of individuals whose personal data are captured for every deployment.
- ☐ We fully document our justification for the use of FRT, and the decision-making behind these justifications, and they are available on request.
- ☐ We have ensured that a sufficient volume and variety of training data has been included to assist accurate performance.
- ☐ We have chosen an appropriate resolution for the cameras we use, and we have carried out full testing of the equipment.
- ☐ We have positioned our cameras in areas with sufficient lighting, to ensure good quality images are taken to assist accurate recognition.
- ☐ We are able to clearly identify false matches, and true matches.
- ☐ We are able to record false positive or false negative rates where appropriate.
- ☐ We are able to amend the system to correct false positive or false negative rates that are considered to be too high.
- ☐ We ensure any watchlists we use are constructed in a way that is compliant with data protection law.
- ☐ We have considered whether an Equalities Impact Assessment (EIA) is required to fulfil our obligations under the Equalities Act 2010.
- ☐ We comply with the [Surveillance Camera code of practice](#)  where required.

What is facial recognition technology?

Facial recognition technology identifies or otherwise recognises a person from a digital facial image. Cameras are used to capture these images and facial recognition software measures and analyses facial features to produce a biometric template. This typically enables the user to identify, authenticate or verify, or categorise individuals. Often, the software which incorporates elements of artificial intelligence (AI), algorithms and machine learning processes estimates the degree of similarity between two facial templates to identify a match. For example, to verify someone's identity, or to place a template in a particular category (eg age group).

FRT can be used in variety of contexts from unlocking our mobile phones, to setting up a bank account online, or passing through passport control. It can help make aspects of our lives easier, more efficient and more secure.

The concept may also be referred to using terms such as automatic or automated facial recognition (AFR) or live facial recognition (LFR) which is a type of FRT that is often used in public spaces in real time.

Depending on the use FRT involves processing personal data, biometric data and, in the vast majority of cases seen by the ICO, special category personal data. Biometric data is a particular type of data that has a specific definition in data protection law.

“Biometric data”, in particular, means personal data resulting from specific technical processing relating to the physical, physio-logical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data, as defined at Article 4(14) UK GDPR.

Under the UK GDPR, processing biometric data for the **purpose(s) of uniquely identifying** an individual is prohibited unless a lawful basis under Article 6 and a condition in Article 9 can be satisfied. Five of the conditions for processing are provided solely in Article 9 of the UK GDPR. The other five require authorisation or a basis in UK law. This means you need to meet additional conditions set out in section 10 and Schedule 1 of the DPA 2018, depending on the Article 9 condition relied upon. Read further [guidance about special category data](#).

Further detailed information can be found in the [Information Commissioner’s published Opinion about the use of facial recognition technology in public spaces](#).

How does facial recognition in public spaces work?

Common uses of FRT such as unlocking our mobile phones, typically involve a “one-to-one” process. This means that the individual participates directly and is aware of why and how you are using their data. Live facial recognition in public spaces is different, and is typically deployed in a similar way to traditional CCTV. This means it is directed towards whole spaces rather than specific individuals. In its most simple form, the face of an individual is scanned and cross-referenced with images from a ‘watchlist’ in order for you to determine a match. This is a bespoke gallery of individuals that could include authorised visitors, people banned from a particular premises, or in some cases a wanted criminal.

After a facial match is suggested by the system, human intervention is commonly required to assess whether the match is correct. This enables you to determine the appropriate response. The level of human intervention required can vary based on the use of the system and the risk of harm to individuals. For example, meaningful human intervention could involve deciding whether to stop an individual in a public space. In contrast, for organisations granting physical access into a premises or secure facility, human intervention may only be required to ensure the system works correctly, or allow for a second opinion.

It is likely that most systems will have an element of human decision-making built-in the process. But Article 22 of the UK GDPR establishes stricter conditions about systems that make **solely** automated-decisions (ie those without any human input). Systems that only support or enhance human decision-

making are not subject to these conditions. But you must ensure that any human input to your processing is active, and has a meaningful influence on the outcomes. See our [guidance on automated decision making](#).

Example

A business wishes to trial the use of live facial recognition on a large crowd of people at the entrance to a concert, in order to improve security. The faces of individuals would be scanned at the entrance, and then cross-referenced with a watchlist of persons of interest. A staff member or officer would review and scrutinise the suggested matches from the system, prior to stopping or questioning any individuals.

FRT can also be used **retrospectively**, in order to identify an individual from old footage or photographs. This is in contrast to using FRT in **real-time** in order to locate an individual in a live public setting. It is still very important to take the principles of data protection law into consideration. For example, you should ensure that the images you use for such retrospective processing are:

- obtained lawfully;
- used for defined and limited purposes;
- accurate; and
- not retained for longer than is necessary.

When using FRT and considering your compliance with the data protection principles, it is particularly important that you recognise and understand the potentially intrusive nature of the technology.

In terms of accountability, when using FRT you must be able to provide a clear explanation of:

- the lawful basis you are relying on;
- why you consider the use of FRT necessary in the circumstances or in the public interest;
- why you have ruled out less intrusive options;
- your assessment of the likelihood that the objectives of FRT (and associated processing) will be met; and
- how you have measured its effectiveness.

In all sectors, any processing you undertake as a result of deploying FRT is likely to result in a high risk to individuals' information rights. You should see a DPIA as a living document that you complete, update or review prior to every deployment. This means you are able to demonstrate that you have considered the risks to the rights and freedoms of individuals.

You may also wish to consider whether an Equalities Impact Assessment (EIA) is required to fulfil your obligations under the Equalities Act 2010.

How do we mitigate bias or demographic differentials?

FRT will typically incorporate machine learning and artificial intelligence. These types of systems learn from data, but this does not guarantee that their outputs will be free of discriminatory outcomes. Both developers and controllers should be mindful about the data used to train and test these systems, as well as the way they are designed and used. This is because these factors may cause them to treat certain demographics less favourably, or put them at a relative disadvantage. For example, this may be based on characteristics such as gender, race or ethnicity.

As a controller you should determine and document your approach to bias and demographic differentials from the very beginning of any use of FRT. This means that you can put appropriate safeguards and technical measures in place during the design of the FRT system.

You should also establish clear policies and procedures surrounding the data which you use to train or pilot systems. You should ensure that the data is sufficiently diverse in order to represent the population the FRT system will be used on. In order for an FRT system to be processing personal data accurately, the output of the system should be the best possible match to the facial image in question. However, this can be a significant challenge when we consider:

- the varying quality of images that can be captured;
- as well as the capabilities of the algorithm used; and
- the ways that faces can be obscured or changed.

Your DPIA should explain how you have implemented effective mitigating measures, including matters relating to bias.

Further, before you procure an FRT system, you should engage with manufacturers, vendors and software developers to explore how they have prevented technical bias within their systems. This will help ensure that their products will allow you to comply with the requirements of data protection law.

How do we determine if FRT is necessary and proportionate?

It is not possible to provide an exhaustive list of all scenarios where the processing of personal data by FRT could be regarded as [necessary](#) and proportionate. You need to be able to demonstrate and document each case on its own merits. You are expected to clearly articulate the lawful use of FRT systems as part of a DPIA and “appropriate policy document”, where required by the UK GDPR and DPA 2018. This applies to the use of FRT in both public and private sectors.

Further detailed information, particularly about necessity and proportionality, can be found in the [Information Commissioner’s published Opinion about the use of facial recognition technology in public spaces](#).

The context in which you are using such systems is a key consideration when you determine whether your use of FRT is appropriate. For example in shopping centres, you still need to be able to strongly justify that your use of FRT is lawful and necessary to achieve your outcome, and that you could not do so using less privacy intrusive methods. It may be more difficult for you to justify processing images of large numbers of individuals to only identify a few, where the need to do so or public interest is not justifiable or realistic.

If you are relying on consent to use FRT, for that consent to be valid you must ensure that you give individuals a fully informed and freely given choice whether or not to be subject to such processing. In practice, consent could prove very difficult to obtain especially in circumstances where you are using FRT on

multiple individuals in public spaces. In cases where you cannot obtain appropriate consent, you must identify an alternative lawful basis to use the system on individuals.

You must also ensure that the use of FRT does not lead to individuals suffering detriment. So, for the use of FRT for authentication purposes, one example is to provide an alternative way for individuals to use a service if they do not wish to participate or consent to facial recognition processing. This could involve individuals using a unique key code or an alternative route to enter a premises.

Example

A gym introduces a facial recognition system to allow members access to the facilities. It requires all members to agree to facial recognition as a condition of entry – there is no other way to access the gym. This is not valid consent as the members are not being given a real choice – if they do not consent, they cannot access the gym. Although facial recognition might have some security and convenience benefits, it is not objectively necessary in order to provide access to gym facilities, so consent is not freely given.

However, if the gym provides an alternative, such as a choice between access by facial recognition and access by a membership card, consent could be considered freely given. The gym could rely on explicit consent for processing the biometric facial scans of the members who indicate that they prefer that option.

Smart doorbells (commercial use)

Checklist

- ☐ We have conducted a Data Protection Impact Assessment (DPIA) that fully addresses our need to use smart doorbells, the lawful basis for their use and explores the impacts on the rights and freedoms of individuals whose personal data are captured.
- ☐ We appropriately position our smart doorbell in such a way that the camera does not inadvertently record neighbouring entrances or private property, that are not the intended subject of surveillance.
- ☐ We ensure that any footage that we record, is kept securely and is appropriately governed in terms of retention, security, disclosure and access.
- ☐ We ensure that any smart doorbell apps we use, or associated software, is secure and kept up-to-date with the latest patches by checking communications from the manufacturer or vendor.
- ☐ We place appropriate signage to inform individuals that surveillance is in use where doorbells are located.
- ☐ We limit any continuous recording, and the possible intrusion of others, by only having the camera activate when the doorbell is pressed.

What is a smart doorbell?

Smart doorbells utilise the positioning of traditional doorbells, and incorporate cameras that can capture images and sometimes audio of individuals visiting or leaving your premises. Some designs can offer a high definition field of vision up to 180 degrees, which can also allow you to see individuals at the door from head to foot.

Often, smart doorbells also connect to a mobile app which can allow you to:

- view a live feed from a remote device;
- save and edit any recorded footage; or
- even potentially share recorded footage with others such as insurance companies or law enforcement.

If you are considering using a smart doorbell for business purposes, it is important that you think about the capabilities of the camera prior to its use. For example, the field of vision it offers and the potential privacy intrusion of others.

As with most video surveillance systems, it is important that you carry out a DPIA that fully addresses:

- your need to use smart doorbells;
- the lawful basis for their use; and
- explores the impacts on the rights and freedoms of individuals whose personal data are captured.

Some models of smart doorbells can be also equipped with facial detection and recognition technologies, which give you the capability to automatically identify an individual at your door. For example, the software may assist access through the door itself by verifying the identity of a visitor. Or more commonly, it may alert you to a specific person of interest if they visit the property. This can be done via a mobile app.

If your system is designed to **uniquely identify** individuals through technologies like facial recognition, then you are also likely to be processing special category data. Therefore, you need to have further protection and safeguards in place. See our [guidance on special category data](#).

It is important that you position your smart doorbell in such a way that the camera does not inadvertently record neighbouring entrances or private property, that are not your intended subject of surveillance.

Example

The owners of a private office building wish to install a smart doorbell at their entrance to increase security, so reception staff only let in recognised clients.


The office entrance is located directly opposite another private building, and it is possible for the camera to see into the windows of the other premises.

The business owners ensure that the smart doorbell is positioned side on, in such a way that the field of vision only captures those that stand at the doorway. In addition, the owners ensure that the camera is only activated when the doorbell is pressed, so they are not using continuous recording.

They also place a sign that reminds visitors about the use of a surveillance system at the entrance to the office building.

Surveillance in vehicles

Checklist

- ☐ We have conducted a Data Protection Impact Assessment (DPIA) that fully addresses our use of surveillance in vehicles, and explores the rights and freedoms of both drivers and passengers whose personal data could be captured by the system.
- ☐ We have clear and informative signage in place within vehicles to let drivers and passengers know when video surveillance systems may be used, and who to contact in the event of a query.
- ☐ We only use audio recording in exceptional circumstances, and this is switched **off** by default if the feature forms part of the installed surveillance system.
- ☐ We have efficient governance procedures in place, such as for the retention of information, and we are able to retrieve stored footage and process it for subject access requests or onward disclosures to third parties where appropriate.
- ☐ We comply with the [Surveillance Camera code of practice](#)  where required.

How is surveillance in vehicles used?

Surveillance systems in vehicles, such as inward or outward facing cameras, are often small systems that are designed to be mounted in cars (or on bikes, most often on the rider's helmet). They record footage of the journey and any incidents that might occur.

While other commercially available action cameras allow for mounting in a car and for footage to be recorded, some surveillance systems are specifically designed for in car use. They have features such as GPS technology, and allow footage to be saved automatically to aid an investigation in the event of a crash or sudden stop.

If you are considering using surveillance systems within any of your vehicles, you should consider the data protection issues that may arise in the specific context of its use. For example, an employer may choose to install inward facing cameras in licensed vehicles as a way to prevent crime, and to protect drivers and vulnerable passengers if there is a genuine need to do so. You should read sections in this guidance about the data protection principles and individuals rights for further information.

Surveillance systems can be intrusive, and can impact on the rights and freedoms of individuals where such

systems are used, especially in places that people would not reasonably expect. In terms of outward facing cameras or dashcams, this can apply to other motorists or pedestrians being recorded outside of the vehicle, or for inward facing systems, drivers and passengers within a vehicle.

Employment and licensed vehicles

If you act as an employer, or oversee the use of licensed vehicles for example, then you should pay particular attention to data protection law if you choose to mandate surveillance systems within vehicles. This is so you can identify an appropriate lawful basis for processing, and adequately safeguard the rights and freedoms of both licenced drivers, passengers and other members of the public.

You must provide sufficient privacy information. For example, you should ensure that you have appropriate signage within the vehicle. This should notify drivers and passengers that recording is taking place and under what specific circumstances.

In addition, you must provide clarity over who is the controller for the processing. For example, sufficient contact details of the relevant controller so that individuals can exercise their rights under the UK GDPR, such as the right of access.

Read further information about installing surveillance in the workplace in our [Employment practices code](#).

Can we record audio within vehicles?

You should also apply the same data protection considerations for recording any audio by in-vehicle surveillance systems. Generally, you should switch **off** any capability to record audio by default. You should only use it in exceptional circumstances, for example by a trigger switch, due to its intrusive nature. Continuous activation requires strong justification that you need to document and risk assess thoroughly.

Example

A logistics firm equips their lorries with in-vehicle surveillance systems with audio capability.

Whilst no intentional audio recording is made within the cabin, it is possible that conversations held by the driver can be picked up. The logistics firm, acting as controller, is therefore required to review whether or not the use of audio is necessary and proportionate in the circumstances. Conducting a DPIA prior to installation must be done to identify such risks to privacy.

Any capability to record audio should be switched **off** by default, and only used, for example by a trigger switch, in exceptional circumstances.

Example

A taxi company, acting as a controller, wishes to mandate the use of onboard cameras in taxis and private hire vehicles. These cameras will record video footage for the purposes of preventing crime and protecting drivers and passengers. The company wishes to use a system that records continuously, which is activated when a vehicle is running.

The drivers express concern that where vehicles are also used for private purposes outside of core working hours, that they, their friends and family would be subject to unnecessary continuous recording.

The company must conduct a DPIA, and ensure that the use of such systems are necessary and proportionate. Continuous recording, whilst the vehicle is being used for private purposes outside of working hours, is likely to be considered excessive. Drivers should have the option to deactivate the recording in these circumstances. The company would also need to take a data protection by design approach, and ensure that the systems they install are of a suitable technical standard, and allow compliance with the principles of data protection law.

Action cameras and other portable surveillance technologies

Checklist

- ☐ We ensure that we record footage in areas that individuals would reasonably expect, to prevent any unwanted intrusion of their privacy.
- ☐ We check that the device is secure, and any removeable memory cards where footage is stored, are securely fitted so they are not easily lost or stolen.
- ☐ We inform individuals by signage or announcements where possible, that we will be recording prior to collecting any footage.
- ☐ We edit or crop footage or both to minimise any risk of harm to others.

There may be instances where your organisation wishes to use more commercially available products, other than traditional CCTV cameras. Such products could include mobile phone cameras, web cams or action cameras. Popular branded products and other portable devices, are often used outside and can be attached to the user's clothing or similarly attached to a mode of transport such as a bike.

Portable action cameras can provide a robust and versatile method of filming that traditional CCTV cameras are not suitable for, and present new ways in which you can process personal data. They do, however, have similar capabilities to Body Worn Video (BWV) cameras that are widely adopted in both public and private sectors. The systems you choose should offer the same levels of security and governance that other surveillance technologies provide when processing personal data. Any use of portable surveillance technology should still respect the rights and freedoms of individuals, and this should be explored in a DPIA prior to using the technology.

Governance (post-deployment)

At a glance

You must control any disclosure of information to third parties from your surveillance system and ensure that the disclosure is consistent with the purpose(s) for which you set up the system.

Your staff who operate surveillance systems should be able to recognise a request to access, erase or restrict personal data, and help progress these requests efficiently.

You may need to use specialist software to redact visual and audio data of third parties. Available techniques include blurring, masking, or using a solid fill to completely obscure parts of the footage. The technique most applicable depends on the circumstances of how the footage was created and the quality of the footage.

The design of your surveillance system should allow you to easily locate and extract personal data, specifically in response to subject access requests and FOI requests.

In detail

- [Can we disclose information to third parties from our surveillance system?](#)
- [How do we comply with the rights of individuals?](#)
- [How should we redact information about third parties?](#)
- [What about freedom of information legislation?](#)

Can we disclose information to third parties from our surveillance system?

Checklist

- ☐ We have clear guidance for relevant staff in our organisation who may handle requests for disclosure, that explains the circumstances where it is appropriate to make a disclosure and when it is not.
- ☐ We record the date of the disclosure along with details of who we have provided the information to (the name of the person and the organisation they represent) and why they required it.
- ☐ We ensure that any method of disclosing information is secure, so the footage is only seen by the intended recipient, and not lost in transit.
- ☐ We have data sharing agreements in place where appropriate, if we need to share information on an ad hoc or routine basis.
- ☐ We are aware that some disclosures to third parties may be unlawful and qualify as an offence under data protection law if the disclosure was made knowingly or recklessly without the consent of the controller.

You must ensure that any disclosure of information to third parties from your surveillance system is controlled and that the disclosure itself is consistent with the purpose(s) for which you set up the system. For example, in most cases it is appropriate to disclose video surveillance information to law enforcement when the purpose of the system is to contribute to the prevention and detection of crime. Unless a court order applies, this is not a legal requirement and is often voluntary. But this could be a shopkeeper proactively disclosing CCTV footage of a crime taking place on the premises, to the police.

You should note that even if your surveillance system was not established to prevent and detect crime, it is still acceptable to disclose information to law enforcement agencies, if relevant. Failure to do so could prejudice an ongoing investigation.

Example

An assault takes place in a night club and the event is captured on CCTV, which is installed inside the premises for public safety and crime prevention.

The local police force requests a copy of the footage from the night club owner in order to investigate the incident. When satisfied by the request, the night club owner is able to efficiently review and retrieve the captured footage and provide a specific clip of the incident to the police to assist the ongoing investigation.

You should approach any other requests for information with care, as wider disclosure may be unfair on the individuals concerned. Further, some disclosures to third parties may be unlawful and qualify as an offence under section 170 DPA 2018 if the disclosure was made knowingly or recklessly without the consent of the

controller. In some limited circumstances it may be appropriate to release information to a third party in the public interest, where the needs of the disclosure outweigh those of the individuals whose information is recorded. Further guidance about data sharing can be found in our [data sharing code](#).

In the majority of circumstances it may not be appropriate for you to place footage captured by your organisation on the internet to an indefinite audience (eg by uploading it to a video-sharing platform). Placing such information on the internet incorrectly, for incompatible purposes or without full consideration, may cause the unlawful disclosure of personal data. You should also balance such disclosures against Article 85 UK GDPR, the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

Unauthorised disclosures can cause damage and distress to individuals, and may lead to the ICO taking enforcement action. Other laws that focus on libel, harassment, malicious communications or threatening behaviour may also apply in some circumstances.

As the operator of the surveillance system, any decisions about disclosure are your responsibility. You have discretion to refuse any request unless there is an overriding legal obligation. For example, a court order.

Once you have disclosed information to a third party they become the controller for the copy they hold. It is their responsibility to also comply with the UK GDPR and the DPA 2018 for any further disclosures. It is also important that any method of disclosing information should be secure. This is to ensure the footage is only seen by the intended recipient, and not lost in transit or unintentionally distributed further.

Further reading – ICO guidance

[Data sharing code](#)

How do we comply with the rights of individuals?

Checklist

- ☐ We have staff who operate surveillance systems that can recognise a request to access, erase or restrict personal data, and can help progress such requests efficiently.
- ☐ We have internal procedures for the handling of requests. This includes keeping a log of the requests we receive and how we dealt with them within the statutory timescales.
- ☐ We have procedures in place to help locate the requester's information. This includes using the date, time and location where the footage was captured.
- ☐ We are able to provide footage to individual requesters or law enforcement in a commonly used video file format.

The right of access

You need to ensure that your staff who operate your surveillance system are aware of the rights that individuals have under data protection law, such as the right of access, erasure or restriction. Relevant staff need to be able to recognise these requests from individuals. This means that they can retrieve information in a timely manner, and also help prevent any processing that is likely to cause substantial and unwarranted damage or distress. You also need to be able to provide footage to individual requesters or law enforcement authorities in a commonly used video file format.

Under Article 15 of the UK GDPR, the [right of access](#) gives individuals the right to obtain a copy of their personal data from you, as well as other supplementary information. This is a fundamental right for individuals and helps them understand how and why you are using their data, and check you are doing it lawfully. You should ensure that the design of your surveillance system allows you to easily locate and extract personal data in response to subject access requests.

Before you can respond to a subject access request (SAR), you need to be able to decide whether the information you hold is personal data and, if so, whose personal data it is. Individuals can make a request verbally or in writing where needed, or to follow-up a verbal request with a written one. To ensure you comply with your obligations, we suggest for you to keep a log of any verbal requests to ensure a satisfactory record and audit trail.

If you are unsure whether or not the request is valid, you should check with the individual that you have understood their request. This can help avoid later disputes about how you have interpreted it, and prevents delays. Individuals who request access must provide you with supporting details, such as a photo, date or time, that allows you to identify them as the subject of the information and also to help locate the personal data on your system efficiently.

Under the UK GDPR you are required to provide the data subject with a copy of all the information caught by the request that constitutes their personal data, unless an exemption applies. You must supply them with a copy of the information in a permanent form or, if they agree, allow or arrange for them to view the information. If an individual refuses an offer to view the footage or they insist on a copy of the footage, then you must do whatever is reasonable in the circumstances to provide them with a copy of this information.

Under the UK GDPR, there is no longer a standard fee that you can charge to exercise the right of access. You may however refuse to deal with the request or charge a reasonable fee if you feel the request for footage is manifestly unfounded or excessive. As a controller, you need to be able to demonstrate the excessive or manifestly unfounded character of the request. Read further [guidance about excessive or manifestly unfounded requests](#).

You must provide information promptly and within one month of receiving the request. Under the UK GDPR, you can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. Providing information promptly is important, particularly where you may have set retention periods for surveillance footage. This means that the information may be routinely deleted if you take the full month to respond. In such circumstances it is good practice to prevent the premature deletion of any information that falls within the scope of a request.

Providing an individual with a transcript of either the audio or visual information contained in the footage is **not** enough to comply in most circumstances. This is because a transcript, or even a still photograph for example, is unlikely to fully communicate all of the contextual information within the footage that could be considered the data subject's personal data.

A clearly documented process will also help guide staff and operators of the system through these requests.

The right to erasure

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the [right to be forgotten](#). However, the right is not absolute and only applies in certain circumstances. This could, for example, be a request from an individual to request erasure of unnecessarily retained CCTV footage.

In the context of surveillance, this right can apply if:

- the information is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their information, and there is no overriding legitimate interest to continue this processing;
- you have processed the personal information unlawfully (ie in breach of the lawfulness requirement); or
- you have to erase it to comply with a specific legal obligation.

There are circumstances where the right to erasure cannot be exercised as certain exemptions apply. In the context of surveillance, this may include but is not limited to:

- processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- certain research activities; or
- compliance with a specific legal obligation to process surveillance information.

The right to restriction of processing

Article 18 of the UK GDPR gives individuals the [right to restrict the processing of their personal data](#) in certain circumstances. This means that an individual can limit the way that you use their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. In the context of surveillance footage, this may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

The UK GDPR suggests a number of different methods that you could use to restrict data, such as:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

How should we redact information about third parties?

In the context of video surveillance, responding to the right of access may involve providing information that relates both to the requester and another individual. Your obligations under the UK GDPR are to

provide a copy of the information about the requester rather than a complete version of footage. But also to ensure doing so does not adversely affect the rights and freedoms of others. Therefore, you may have to consider seeking the consent of third parties where reasonable or alternatively removing or redacting particular footage. You should consider the nature and context of the footage to determine the level of harm that may arise from choosing not to redact. In practice, you need to approach each request for information on a **case-by-case** basis, and make a reasonable determination based on the particular circumstances.

For example, from Body Worn Video (BWV) or a more traditional CCTV system, available techniques could include blurring, masking, or using a solid fill to completely obscure parts of the footage. You may also wish to consider removing metadata from footage files where necessary. The technique most applicable will depend on the circumstances of how the footage was created and its quality. To do this, you may need to use specialist software to redact visual and audio data.

This software is sometimes provided with commercially available surveillance systems to support back office functions, or through separate products. While professional software requires training and expertise to operate, redaction tools that compliment systems are designed to be easy to use. You should train relevant members of staff to use this software, for example to respond to requests efficiently within the statutory timescales.

When you procure a surveillance system, as part of your DPIA before any processing you should always consider the capabilities the technology offers in terms of governance. You should not choose a product based solely on its ability to capture footage. You should also seek to use products whose manufacturers have built them in line with data protection by design and default considerations. This ensures that you do not adopt a system that does not allow you to comply with your data protection obligations.

It may be necessary for you to contract out the redaction process to a specialist organisation. In this context, the third party is likely to become a processor, so you would need to have a written contract that specifies exactly how the information is to be used and provides you with explicit guarantees in terms of quality and security. See our [guidance on controllers and processors](#) for more information.

What about freedom of information legislation?

If you are a public authority, then you may receive requests under the [Freedom of Information Act 2000 \(FOIA\)](#) for information captured by surveillance systems. You should have a member of staff who is responsible for responding to freedom of information requests, and understands your responsibilities. You must respond within 20 working days from receipt of the request.

Section 40 of FOIA contains a two-part exemption relating to information about individuals. If you receive a request for surveillance system information, you should consider the following questions:

- Is the information personal data of the requester? If so, then that information is exempt from FOIA. Instead, you should treat this request as a data protection subject access request.
- Is the information personal data of other people? If it is, then you can only disclose the information if:

First condition: disclosure does not contravene one of the data protection principles.

Second condition: disclosure does not contravene an objection to processing.

Third condition: the information is not exempt from the right of access.

In practical terms, if individuals are capable of being identified from the relevant surveillance footage, then it is personal data about those individuals. Where the information includes personal data of third parties, you should consider applying redaction techniques to obscure images. It may be appropriate to do this rather than exempting the information.

If you are a public authority who has surveillance systems, you may also receive requests for information under FOIA relating to those surveillance systems. For example, requestors may ask for information about the operation of the systems, the siting of them, or the costs of using and maintaining them.

If you hold this information, then you need to consider whether it is appropriate to disclose this information under FOIA. You should provide any information you hold unless you can show that an exemption applies. For example, if providing details of the location of cameras is likely to prejudice the prevention or detection of crime.

This is not an exhaustive guide to handling FOI requests and we have further [guidance about handling such requests](#).

Note: Even where footage is exempt from FOIA, it may be lawful to provide it on a case-by-case basis without infringing data protection legislation if you have taken the reason for the request into account.


Further reading

For further information on FOIA, including how to handle requests for information, please refer to the ICO's [Guide to Freedom of Information](#).

For further information on Freedom of Information (Scotland) Act 2002 (FOISA), please refer to [The Scottish Information Commissioner](#).

Checklist for limited CCTV systems

This checklist is for users of limited CCTV systems monitoring small premises, such as retail or other small business properties. It outlines the core data protection considerations for the use of such systems.

In addition, [the Biometrics and Surveillance Camera Commissioner \(BSCC\)](#)  also offers a buyers’ toolkit which assists small and medium enterprises that are thinking about using surveillance systems.

This CCTV system and the images produced by it are controlled by:

.....

who is responsible for how the system is used under the UK GDPR and Data Protection Act 2018.

We (.....) have considered the need for using CCTV and have decided it is necessary for the prevention and detection of crime and for protecting the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate.

	Checked (Date)	By	Date of next review
If our system is processing footage of identifiable individuals and is processing personal data, we have registered as a controller and submitted a relevant data protection fee to the Information Commissioner’s Office (ICO). We have also recorded the next renewal date.			
There is a named individual who is responsible for the operation of the system.			
Prior to processing we have clearly defined the problem we are trying to address. We regularly review our decision to use a surveillance system.			
We have identified and documented an appropriate lawful basis for using the system, taking into consideration Article(s) 6, 9 and 10 of the UK GDPR and relevant Schedules of the DPA 2018.			
Our system produces clear images which we can easily disclose to authorised third parties. For example when law enforcement bodies (usually the police) require access to investigate a crime.			
We have positioned cameras in a way to avoid any unintentional capture of private land or individuals not visiting the premises.			

There are visible signs showing that CCTV is in operation. Contact details are displayed on the sign(s) if it is not obvious who is responsible for the system.

We securely store images from this system for a defined period and only a limited number of authorised individuals may have access to them.

Our organisation knows how to respond to individuals making requests for copies of their own images, or for images to be erased or restricted. If unsure the controller knows to seek advice and [guidance](#) from the Information Commissioner's Office (ICO) as soon as a request is made.

Please keep this checklist in a safe place until the date of the next review.