SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

# **Data protection impact assessments** guidance for carrying out a data protection impact assessment on surveillance camera systems

## Introduction: a collaborative approach

1. The Surveillance Camera Commissioner (SCC) and the Information Commissioner's Office (ICO) have worked together on this guidance. By doing this we've responded to requests from operators of surveillance camera systems who have asked for coordinated advice when processing personal data in this way. The template we've provided should support you through the process, but you may prefer to use alternatives. It is perfectly acceptable to do this, provided that they satisfy statutory requirements (see legal obligations set out below).

## The roles of the Commissioners

2. The SCC is responsible for encouraging relevant authorities[1] to be compliant with the Home Secretary's Surveillance Camera Code of Practice; to review the operation of the code and to provide advice about it. Relevant authorities in England and Wales are required to have due regard to the code when they are operating surveillance cameras, as defined at section 29(6) of the Protection of Freedoms Act 2012, in public places. The SCC also has a statutory responsibility to encourage voluntary adoption of the code by organisations not listed in the Act.

3. The ICO is responsible for regulating and enforcing data protection law, namely the General Data Protection Regulation and the Data Protection Act 2018.[2] It has published detailed guidance on data protection impact assessments (DPIAs), for general processing and for the law enforcement purposes, which you should read in conjunction with this advice. All organisations in the UK must comply with data protection law, and in certain cases, carrying out a DPIA is a mandatory requirement.

## Who is this advice for?

4. This advice is intended for organisations in England and Wales that must have regard to the Surveillance Camera Code of Practice under Section 33(5) of the Protection of Freedoms Act 2012. However, it will also be of value to the wider community of public authorities and any other bodies, whether public or private, who perform public functions as well as private organisations operating surveillance cameras anywhere in the UK.

5. When considering the deployment of a surveillance camera system, you must have a clear understanding of each organisation's responsibilities under data protection law. If you are making decisions on the use of the personal data captured as a controller, or joint controllers, you are chiefly responsible for compliance with data protection law, including the requirement to carry out a DPIA. However, other organisations acting under the instruction of controllers (i.e. processors) also have responsibilities, including assisting controllers in developing DPIAs.

6. If you then process this data for different purposes, you will also need to consider these in any assessment. In some cases, if the processing is for different purposes, you may be required to carry out more than one DPIA.

## Your legal obligations

7. Principle 2 of the Surveillance Camera Code of Practice[3] states that the use of a surveillance camera system must take into account its effect on individuals and their privacy. Processing of

---

[1] Listed in the Protection of Freedoms Act 2012 (s33.5) – police forces, police and crime commissioners, local authorities and parish and district councils.
[2] Regulation (EU) 2016/679 of the European Parliament and European Council, also known as the General Data Protection Regulation, was transposed into UK law through the Data Protection Act 2018. Any processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences is regulated under Part 3 of the Data Protection Act 2018 which transposes Directive (EU) 2016/680, also known as the Law Enforcement Directive, into UK law.
[3] Surveillance Camera Code of Practice issued by the Home Secretary in June 2013 under Section 30(1)(a) Protection of Freedoms Act 2012.

personal data using a surveillance camera system will be considered 'likely to result in high risk to rights and freedoms' under data protection law. For instance, where it can systematically monitor public spaces on a large scale, or can involve innovative technology or the processing of biometric data. As processing using a surveillance camera system is likely to be high risk you must conduct a DPIA **before** the system is installed and review it regularly. Carrying out a DPIA means that you can determine whether deployment is lawful, and will also be a record of how you have considered and addressed any risks or wider concerns about your project. This addresses Principle 2 of the Surveillance Camera Code of Practice as well as requirements of data protection law.

8. What a DPIA must cover and when they are required by law is set out in Article 35 of the GDPR (general processing) and Section 64 DPA 2018 (law enforcement processing). The ICO has also identified further types of general processing where a DPIA is mandatory, because the processing is likely to result in **high risk**[4] to individuals' rights and freedoms. This can also indicate to controllers who are processing for law enforcement purposes where there may be high risk. Surveillance camera systems are very likely to sit within the scope of this high risk requirement.

9. There are situations when you must consider a DPIA, for example:

- When you are introducing a new surveillance camera system.
- Before you process any special categories of personal data on a large scale.
- If you are considering introducing new or additional technology that may affect individuals' rights and freedoms (e.g. facial recognition technology, automatic number plate recognition (ANPR), audio recording, body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high-resolution cameras).
- If your system involves any form of data matching.
- When you are changing the location or field of view of a camera or other such change that may raise privacy concerns.
- When you are reviewing your system to ensure that it is still justified. Both the SCC and the ICO recommend that you review your systems regularly, for example as part of annual procedures.
- When you change the way you record images and handle, use or disclose information.
- When you increase the geographical area captured by your surveillance camera system.
- When you change or add an end user or recipient for the recorded information or information derived from it.

Remember that the ICO has identified specific circumstances when a DPIA is required.

## Assessing risk

10. Likelihood of high risk means that the type of processing has a higher chance of harming individuals. This could be as a result of decisions taken using this data, or because of an individual's lack of control over how their information is used. 'Likely' does not mean that your project **will** harm individuals, however it does mean that you are required to assess your project before it starts, to ensure you reduce any risks you identify.

11. The GDPR identifies certain types of processing where the likelihood of high risk is engaged, for example stating specifically that a DPIA "shall in particular be required in the case of…systematic monitoring of publicly accessible places on a large scale" (Article 35).

---

4 Examples of high risk could be surveillance cameras, such as body worn video, that also record audio or CCTV fitted with automatic facial recognition capabilities. There is further information about when to carry out a DPIA on the ICO website.

12. 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. It is important to embed DPIAs into your organisational processes such as project planning and other management and review activities, and ensure the outcome can influence your plans prior to implementation.

13. A further benefit of carrying out a DPIA is that it will help to address statutory requirements under the Human Rights Act 1998 (HRA). Section 6(1) HRA provides that it is unlawful for a public authority to act in a way which is contrary to the rights guaranteed by the European Convention on Human Rights (ECHR). Therefore, in addition to the above, as a public body or any other body that performs public functions you must make sure that your system complies with HRA requirements.

14. When conducting a DPIA you should consider the nature, scope, context and purposes of the surveillance camera activities and their potential to interfere with the rights and freedoms of individuals, as set out in Human Rights law. For example:

- the right to freedom of assembly;
- freedom of thought, belief and religion;
- freedom of expression;
- freedom of association; and
- the protection from discrimination in respect of those rights and freedoms.

15. Data controllers should consider how the processing is lawful and fair, in order to be compliant with the first principle of data protection law.

16. If your DPIA identifies a residual high risk that you cannot mitigate adequately, data protection law requires that you must consult the ICO before starting to process personal data. This should be when you are planning your surveillance camera system or making changes to it that will impact on individuals' rights and freedoms.

17. To support you in preparing your assessment the accompanying template includes:

- **DPIA** to describe and assess your planned deployment of surveillance cameras;
- **Appendix One** to record and evaluate your camera locations, equipment and software;
- **Appendix Two** with suggested steps involved in carrying out a DPIA; and
- **Appendix Three** a sample risk matrix.

## Governance of DPIAs

18. You must carry out a DPIA prior to the processing in the first instance. If the deployment goes ahead, you should review the DPIA regularly to maintain relevance. You should be aware that failure to complete a DPIA prior to the deployment of a surveillance camera system could result in the ICO taking enforcement action.

19. As an organisation that operates a surveillance camera system you will also be the controller of the personal data captured by its cameras. Under DPA 2018 (Sections 69-71), a data controller is under a legal obligation to designate and resource a data protection officer and to seek their advice when carrying out a DPIA.

20. Consultation is an important part of the DPIA process. You should obtain the views of people who are likely to come under surveillance or their representatives. This can often be achieved by existing local consultation mechanisms such as local area committees or safer neighbourhood team meetings. You can consider other methods, such as face to face interviews, online surveys,

and addressing focus groups, crime and disorder partnerships and community forums. You should also consult internally, for example with your legal department, and staff who will be recorded. Your DPO may be able to offer advice on how to carry out consultation. The Surveillance Camera Commissioner's Passport to Compliance (paragraph 1.5.3) also includes detailed advice on consultation which will be of use.

21. Principle 2 of the Surveillance Camera Code of Practice also requires that you must carry out regular reviews to ensure your use of surveillance camera systems remains justified. You should factor a review of your DPIA into your ongoing risk assessment procedures to consider any significant changes to the risks of operating an existing system (for example extended access to footage to additional parties, or changing the location or capabilities of the system).

## DPIA Template

22. The questions in the DPIA will enable you to determine:

- Are surveillance cameras the right solution to the problem you are trying to solve?
- What are the risks to data subjects raised by the deployment of surveillance cameras?
- Is the impact on individuals' rights and freedoms proportionate to the problem you are addressing?
- Can the risks be reduced to an acceptable level?

The tools at Appendix Two and Three may also assist you to do this.

**Appendix One**

23. When undertaking a DPIA, it is important to be able to identify where your cameras are located. It is good practice to maintain an asset register for all of your hardware (including cameras), software and firmware. This allows the system operator to record each site and system component of a surveillance camera system.

24. The template at Appendix One is designed to give you a clear and systematic format for recording camera locations, other hardware, software and firmware on your surveillance camera system, and demonstrate the mitigations of risk particular to specific camera locations and functionality.

25. This approach allows you to document a generic and methodical approach to any intrusion into privacy, catalogue your cameras by type and location, and identify specific privacy risks with particular cameras.

26. If any new site or installation sits outside of the pre-defined fields, or additional integrated surveillance technologies are added, then you can add new categories as required.

**Appendix Two** demonstrates suggested steps in the lifecycle of a DPIA.

**Appendix Three** shows an example of a risk assessment matrix.