



Security.Improved

National Security Inspectorate

Sentinel House
5 Reform Road
Maidenhead
SL6 8BY UK

T +44 (0)1628 637512

F +44 (0)1628 773367

E nsi@nsi.org.uk

W nsi.org.uk

AWEW/mjc/NSI 001/15

23 January 2015

To: All NSI approved companies and applicants

Dear Colleague

CODES OF PRACTICE RELATING TO THE USE OF CCTV

This letter draws your attention to two codes of practice relating to CCTV. We recommend you obtain copies of these codes of practice and you review them for any impact on your business.

The first is the new **Information Commissioner's Office Code of Practice (ICO code)**, which provides recommendations on how the requirements of the Data Protection Act 1998 (DPA) can be met and in doing so aims to help organisations using CCTV to stay within the law.

The ICO code is relevant for example if you provide monitoring services for CCTV because you are likely to be using surveillance cameras to view or record individuals, or other information relating to individuals such as a vehicle registration marks.

The second is the **Surveillance Camera Code of Practice (POFA code)**, which provides guidance to relevant authorities in England and Wales operating surveillance camera systems on how to comply with the Protection of Freedoms Act 2012 (POFA). The relevant authorities are listed in Section 33 (5) of the POFA and include local authorities, police and crime commissioners, and any chief officer of a police force in England and Wales.

If you carry out work associated with surveillance camera systems for relevant authorities in England and Wales you should at least have an awareness of the content of the POFA code and you may need to have due regard to the POFA code where your contracts put you in a position of responsibility to do so.

A requirement of the POFA was the appointment of a Surveillance Camera Commissioner. We are working with the Commissioner to develop a scheme to award certification against the POFA code. If you operate CCTV and you are interested in taking part in a pilot we would be pleased to hear from you as soon as possible.

Further information, including how to obtain copies of the codes, is contained within the Annexes attached to this letter. Please do not hesitate to contact me if you would like to discuss matters further.

Yours sincerely

Tony Weeks

Head of Technical Services

Att.



0142



0142

ANNEX A

NEW ICO CODE OF PRACTICE FOR SURVEILLANCE CAMERAS AND PERSONAL INFORMATION (ICO CODE)

The Information Commissioner's Office (ICO) published a new code of practice in 2014 called "In the picture: A data protection code of practice for surveillance cameras and personal information".

This new code replaces the ICO CCTV code of practice published in 2008.

Even if you do not operate CCTV systems, as designers and installers for example you still have a duty of care to customers to ensure they are aware of their obligations under the DPA, for example by drawing their attention to the ICO code, and to provide them with CCTV systems that are capable of being used in a manner that does not breach the DPA. A good example would be the inclusion of a masking capability to ensure cameras do not view areas outside their intended purpose.

You can download a copy of the new ICO code of practice from the ICO website¹.

The DPA (and consequently the ICO code) is applicable throughout the UK.

For information, the Scottish Government has produced "A National Strategy for CCTV in Scotland"². The strategy provides a common set of principles that operators of public space CCTV systems in Scotland must follow. The principles aim to ensure that these systems are operated fairly and lawfully and are using technologies compatible with the DPA.

NOTES

Note 1: There is an overlap between the ICO code and the POFA code (see Annexes B and C) on matters relating to the DPA and for this reason the new ICO code makes reference to the POFA code.

Note 2: There should be no differences between the ICO and POFA codes in relation to the DPA.

Note 3: The ICO code states it is consistent with the POFA code and therefore following the guidance contained in the ICO code will also help you to comply with the POFA code (see ICO code for further details).

¹ <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

² <http://www.scotland.gov.uk/Publications/2011/03/18085554/0>

ANNEX B

SURVEILLANCE CAMERA CODE OF PRACTICE (POFA CODE)

A requirement of the Protection of Freedoms Act 2012 (POFA) was the appointment of a Surveillance Camera Commissioner to oversee the areas of legislation within the POFA concerning the use of surveillance cameras by “relevant authorities” in England and Wales. The “relevant authorities” are listed in Section 33 (5) of the POFA and include local authorities, police and crime commissioners, the Mayor’s Office for Policing and Crime, and any chief officer of a police force in England and Wales.

The POFA (and consequently the POFA code) applies in England and Wales only whereas the DPA (see Annex A) applies to the whole of the UK.

To provide guidance on how the relevant authorities operating surveillance camera systems in England and Wales are to comply with the POFA, the Home Office issued the “Surveillance Camera Code of Practice” (POFA code) in 2013.

Other operators and users of surveillance camera systems in England and Wales are encouraged to adopt the POFA code voluntarily.

The POFA code contains 12 guiding principles, which outline what relevant authorities are required to have due regard to when specifying and operating surveillance camera systems, and there is further detail in the POFA code about each principle.

The 12 guiding principles are listed in Annex C for ease of reference and are primarily concerned with ensuring camera systems are proportionate to the surveillance requirement and are compliant with the requirements of the POFA and the DPA.

Additionally the POFA code requires that before surveillance camera systems are procured a ‘pressing need’ is identified to justify the requirement, that the continuing operation of the system is reviewed on a periodic basis (nominally annually) to validate whether the system is still required and that systems are installed to a high standard to ensure the quality of any information obtained is fit for the intended purpose.

You can download a copy of the “Surveillance Camera Code of Practice” (POFA code) from the .GOV.UK website³.

A self assessment tool, issued by the Surveillance Camera Commissioner to measure compliance against the POFA code, is also available from the same .GOV.UK website.

Although the POFA code is not statutory apart from matters relating to the DPA, it is important to note the provisions of the POFA code are admissible in Court.

³ <https://www.gov.uk/government/organisations/surveillance-camera-commissioner>

ANNEX C

GUIDING PRINCIPLES IN THE SURVEILLANCE CAMERA CODE OF PRACTICE (POFA CODE)

Principle 1 - Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

Principle 2 - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

Principle 3 - There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

Principle 4 - There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

Principle 5 - Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

Principle 6 - No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

Principle 7 - Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Principle 8 - Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

Principle 9 - Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

Principle 10 - There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

Principle 11 - When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

Principle 12 - Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.