ic2 DESIGN INSTALL PROTECT

Q&A guide: CCTV code of practice and Data Protection Act compliance

The ICO surveillance camera code of practice, the DPA and avoiding financial penalty for non-compliance in protecting personal information

www.ic2cctv.com

INTRODUCTION

October 2014 saw the publication of 'In the picture: A data protection code of practice for surveillance cameras and personal information' by the Information Commissioner's Office (ICO).

This root and branch overhaul of best practice and regulatory code for security and surveillance systems was long overdue. Indeed, since the first guidance was issued in 2000 under the Data Protection Act (DPA) 1998, an awful lot has happened to shape the discussion around security. Some of the issues we face as a result include:

- Significant and increasing threat from terrorist activity
- Increasing cyber security concerns - threats from internet crime and cyber warfare
- Phone hacking by News International and Trinity Mirror media group newspapers
- Intelligence whistleblowing – WikiLeaks & Edward Snowden
- The advent of military and law enforcement Body Worn Video (BWV)
- The development of wearable internet-connected computers capable of recording
- The increasing use of unmanned aerial systems/vehicles with cameras - 'drones'

The ability of such complex issues to impact our everyday lives was shown by The Sun in January 2015, when it ran the double-page feature 'I'm a CCTV star'. This showed just how widespread the use of video surveillance technology is in the built environment with the story of how a journalist was captured on camera 500 times in one day. Another everyday impact saw a man wearing a Google Glass smart eyewear computer attacked in a San Francisco bar by other customers that objected.

At the heart of the debate are two very important principles: Security and Privacy. Some in the security industry have tried to position the issue as Security Versus Privacy. However, this is unacceptable to most people because its ultimate conclusion is that in order to have total security you have to totally forfeit privacy.

In a democratic and free society, the most reasonable way to look at this is that privacy and security are not mutually exclusive. They have to co-exist side by side. In combination with the DPA, the ICO code of practice is designed to bring the two together, by safeguarding privacy without throwing insurmountable obstacles in the way of security. Although this is a simple idea it is not without its challenges.

In this Q&A guide we answer some key questions that enable your organisation to meet its regulatory obligations and avoid the penalties for failing to meet its compliance requirements.

Q1. What are the fines for breaking the ICO code of practice?

Answer:

It's not that straightforward. Essentially there are no fines for breaking the ICO code of practice. The code is not enforceable; it is a guide to best practice. However, the majority of surveillance systems are used to monitor or record the activities of individuals, or both. This means that you are collecting and processing the information of individuals - their personal data. The collection and processing of the personal data of specific people brings you into scope of the DPA. DPA compliance is a legal requirement. Any action that results in financial penalties would be for breaching the DPA.

Q2. What is the fine for breaching the DPA?

Answer:

At the moment the ICO has a range of options for dealing with breaches of the UK Data Protection Act:

- Financial penalty notices of up to £500,000 for serious breaches of the DPA
- Prosecutions and custodial sentences are an option for deliberately breaching the DPA
- Undertakings for organisations to commit to a particular course of action to improve compliance and avoid further ICO action
- Enforcement notices requiring organisations in breach of legislation to take specific steps in order to comply with the law

New EU General Data Protection Regulations (GDPR) proposes fines of up to 5% of global turnover. Recent figures show between January 2013 and October 2014 there were 66 enforcement notices issued by the ICO for DPA infringements and financial penalties totalling £2.17M were issued.

Q3. Which companies does the ICO code and DPA compliance apply to?

Answer:

All companies and organisations are governed by the code and the DPA. Whether you are a multinational company or a mid-market enterprise running a system to monitor the entry and exit of staff and visitors to and from your premises, or a small retailer recording information to help prevent shoplifting or assault, you should be guided by the code and are in scope of the DPA. The use of surveillance systems for limited household purposes is exempt from the DPA.

Q4. What 'surveillance' systems are covered by the code and DPA?

Answer:

For the purposes of the code and DPA compliance the following systems may fall under the broad definition of 'surveillance':

- Closed-circuit television CCTV
- Automatic Number Plate Recognition (ANPR)
- Body worn cameras (BWC)
- Surveillance drones (SD)

Additionally, close consideration should be given to the implications of using systems such as:

- Electronic Access Control Systems (EACS)
- Biometric Recognition (BR)
- Voice conversations
- Telephone data

Q5. For the purposes of the code and DPA who is legally responsible?

Answer:

From the perspective of the ICO and the DPA the individual in control of personal information is defined as the 'data controller' and is legally responsible. Depending on the precise scenario, this could be a Landlord, Managing Agent or Buildings Manager. Third-parties such as 'operational controllers', employed by external service providers to oversee the running of surveillance systems on a day-to-day basis, are not defined as data controllers.

Typically, the data controller makes decisions such as what is recorded, how the information is used and to whom it may be disclosed. Where more than one organisation is involved, both should take steps to understand its responsibilities and obligations. If decisions are made jointly about the intended purpose or any operational matters relating to the system, then both are responsible under the DPA.

Q6. What documentation do we need to maintain?

Answer:

Documentation requirements vary depending on the size of your organisation, the quality of the information (such as resolution of image data), and the extent to which you collect and use information.

- Small-scale users, such as small retailers, are unlikely to have sophisticated systems, so many of the code's more detailed provisions will be inappropriate and documentation requirements are reduced
    - Appendix 2 of the code provides special guidance for scenarios where there is very limited use of surveillance systems and privacy risks are small and resources limited
- For larger business with more sophisticated systems producing higher quality data across more diverse surveillance system types, the full code applies. Key documentation that should be maintained includes:
    - Surveillance Systems Policy
    - Annual Privacy Impact Report
    - Management Audit
    - Systems operational assessment

Q7. What is the best way to follow the code and make sure we don't break the DPA?

Answer:

The ICO code, the DPA and additional legislative instruments and guidance weave together to create quite a complex framework. While it is not rocket science, it is easy to breach compliance unintentionally because the handover points from one to the other may not be completely clear. The main elements of this framework include:

- Freedom of Information Act (FOI)
- Human Rights Act 1998 (HRA)
- Surveillance Camera Code of Practice
- Protection of Freedoms Act (POFA)

One of the best ways of making sure you follow best practice and don't breach the DPA is to engage the services of an expert security company. While it is perfectly feasible to manage compliance as an internal function, as with any compliance-led requirements, it is advisable to seek out expert help.

SUMMARY

How iC2 helps you follow ICO best practice and avoid breaking the DPA

iC2 is a leading mid-market security systems provider and was established in 2001. The business is owned and managed by a team with a collective experience of over 100 years in the electronic security business. iC2 holds CCTV and security accreditations with NSI and BSI.

Whether the requirement is solely for CCTV, or for a new fully integrated system, iC2 provides the consultancy led services to specify, supply, install and support a full range of integrated electronic security solutions. This includes HD CCTV, Wireless CCTV, ANPR (Automatic Number Plate Recognition), Remote Monitoring, Access Control, Gates & Barriers, PA Systems, Fire Alarms and Intruder Alarms.

The advent of greater regulatory control makes it an imperative for organisations and businesses of all types and sizes to take control of their surveillance system compliance obligations. iC2 offers a complete compliance service tailored to the size and needs of each client.

iC2 CCTV and surveillance compliance services helps:

- Smaller businesses to meet their obligations while avoiding unnecessary cost and complexity
- Larger businesses to take complete control by understanding and meeting the compliance requirement in full

A prestigious client list including luxury international boutique brands, top flight sporting venues, retail developments and educational and social environments demonstrates how solutions are deployed to meet a variety of requirements.

From deterring theft of high value luxury goods, to sports fan and public safety and child protection, solutions are deployed to meet a range legitimate purposes for which they are appropriate and fit for purpose.

REFERENCES AND FURTHER READING

Surveillance Camera Code of Practice
Home Office; 2013

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

In the picture: A data protection code of practice for surveillance cameras and personal information
ICO; CCTV Code of Practice; 2014

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

I'm a CCTV star - Intrusion or protection? Sun man spends a day in surveillance Britain
The Sun print edition double page feature; January 2015 (Online version behind paywall)

http://www.thesun.co.uk/sol/homepage/features/6270771/Sun-man-shares-shocking-facts-about-CCTV-in-Britain.html

iC2 DESIGN INSTALL PROTECT

T: 020 3747 1800

E: info@ic2cctv.com

W: www.ic2cctv.com

About Us

Keeping you safe and secure at all times

iC2 provide you with innovative solutions tailored to you and your sector. We are London-based with a national team of surveyors and engineers that work closely with our clients throughout the UK and internationally.

Our unique consultative approach allows us to tailor bespoke systems to your individual requirements, ensuring that your operational requirements are met.

We appreciate the need to demonstrate the best value to you every time and as a technology-led company, you can expect our cutting-edge and ground-breaking approach to serve your needs for many years to come.

Please feel free to contact us to discuss any requirements you may have. We are happy to give you impartial advice, should you have any queries.