Is your use of CCTV compliant with data protection legislation?

Data protection is a fundamental concern to all organisations which hold vast amounts of personal (and often sensitive) information relating to individuals. Breach of data protection legislation, which includes the Data Protection Act 1998 (DPA) can lead to fines, bad publicity and even criminal sanctions. It may or may not come as a surprise that CCTV recordings commonly used by organisations to track crime, anti-social behaviour and monitor communal areas are also covered by the DPA.

This article outlines the key obligations under the DPA in relation to the use of CCTV and considers the impact of the new General Data Protection Regulation.

Data protection obligations under the DPA in relation to CCTV

The DPA requires organisations to protect any "personal data" that they hold relating to individuals. Personal data is not just restricted to written text; CCTV recordings also fall within the scope if individuals can be identified from them.

The Information Commissioner's Office (ICO), which is the office responsible for the enforcement of the DPA and Freedom of Information Act, has published an updated code of practice for the use of surveillance cameras which provides practical advice and recommendations for complying with the DPA. (See: In the picture: A data protection code of practice for surveillance cameras and personal information, May 2015 "the Code").

"We were impressed by their commercial awareness, their speed and the top quality of their advice. They get things done."

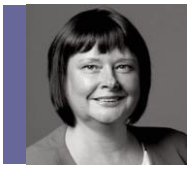
CHAMBERS UK 2016
The independent guide to solicitors in the UK

How can we help?

We advise on all aspects of data protection compliance and our experts regularly advise organisations on all aspects of their information governance and data protection requirements.

We design and deliver data protection and information governance workshops to organisations of all sizes and across the UK. Whether you want to train one person or a whole team, we can offer public courses or bespoke workshops. Each seminar is interactive and dynamic with lots of useful information and guidance to take away.

You can find out more about our Data Protection and Privacy Team and how we can help by visiting us at www.wrighthassall.co.uk. Alternatively, please contact a member of our team for further information or advice.



Paula Tighe
Information Governance Director
paula.tighe@wrighthassall.co.uk
01926 884697

Jo Goodworth
Senior Associate
jo.goodworth@wrighthassall.co.uk
01926 880737
07824 846107

Ensuring DPA compliance

The Code includes a number of recommendations in order to ensure compliance with the following DPA requirements:

- As with other types of personal data, every organisation that collects personal data by way of CCTV must have a legitimate reason for doing so. In the context of the use of CCTV, the purpose may be to detect crime, ensure the safety of the public or perhaps to monitor congestion or footfall. The use of CCTV must be a "necessary and proportionate response to a real and pressing problem". The Code recommends carrying out a privacy impact assessment to assess the extent to which CCTV is required, where it is required and at what times.
- The CCTV data must be used and kept only to fulfil its purpose. As such, if the purpose of holding the data is to identify individuals performing criminal activity, the recordings should be of sufficient quality to do so and be easily accessible if requested by the police. Access to the data should also be restricted to those that require access to it for the purpose for which it is held.
- The storage of CCTV recordings must be secure in order to prevent unauthorised access and hacking; this means using encryption wherever possible. (The ICO has recently released updated guidance on the use of encryption (May 2016)). In addition, the length of time that you store the recordings should also be reflective of the purpose for which it is recorded and in all cases should be stored no longer than necessary. Where it is not necessary to retain such data then it should be deleted.
- Subject access requests apply equally to CCTV recordings as to any other recorded data. Individuals therefore have a right to request a copy of their personal data, which includes footage held on a CCTV system, where they are the focus of the footage and/or they are clearly identifiable. If the request is valid and permissible under the exemptions of the DPA this data has to be supplied within 40 days of the request being deemed valid. Organisations should therefore ensure that they have appropriate systems and procedures in place to comply with these requests promptly.
- Organisations must also ensure that individuals, (Data Subjects) are provided with 'fair processing information' which means that they are fully informed of their rights and aware of the existence of CCTV cameras which may record their actions. The most effective way of doing this is by using prominent signs at the entrance to the area in which the cameras are located and reinforcing this with further signs inside the area and by publishing further fair processing information detailing Data Subjects' rights.

Tighter data protection legislation is on the way!

- The General Data Protection Regulation (GDPR) is the biggest shake up of data protection law for 20 years. The new EU rules, which are set to come into effect in just over two years' time on 25th May 2018, will be directly applicable in the UK without any further implementation. Breach of the new data protection law could now see organisations facing hefty fines from the ICO of up to €20 million or 4% of global turnover (whichever is higher) for serious breaches of the Act.
- Organisations, whose core activity consists of processing special categories of data or the systematic monitoring of individuals on a large scale, will be required to appoint a Data Protection Officer to monitor compliance with the rules. We would advise any organisation that may be caught by this rule to start making arrangements to appoint an officer if they have not already done so.
- Organisations will also have to demonstrate that an individual's consent to the processing of their personal data is 'freely given, specific, informed and unambiguous', and in most cases implied consent will not be sufficient. Although in relation to the use of CCTV it is still as yet unclear to what extent you will need to seek to obtain explicit consent from individuals to record them via a CCTV system, as is already the case, you are required to make the presence of cameras very clear.
- The increased fines will immediately apply in respect of any non-compliance after implementation so all organisations should now take heed that they have two years to implement policies and procedures to comply with the new rules. All organisations that process data would be well advised to get up to speed and address their data protection obligations now, before it is too late.

Things you need to consider

If your organisation has CCTV systems in operation, you should consider the following:-

- Have you performed a Privacy Impact Assessment (PIA) and do all your CCTV cameras serve a legitimate purpose?
- Have you made sure the CCTV system has the ability to be switched on or off, if this is appropriate, so that recording of footage is not continuous? The system should also have the ability to stop capturing either footage and/or sound recordings both of which should work independently of each other. Capturing both could be deemed excessive and you would need to demonstrate clearly the reasons for recording both and what legitimate grounds you are relying on to justify this.
- If you capture sound recordings are they obtained when it is absolutely necessary and for this specific purpose? CCTV surveillance systems should not normally be used to record conversations between members of the public or members of staff as part of a working environment. Recording conversations is highly intrusive and unlikely to be justified and performance of a PIA would identify this.
- Are recordings from the CCTV system securely stored and are you able to restrict access to them?
- Are your CCTV recordings of sufficient quality to be fit for their intended purpose and is there a regular check that the date and time stamp recorded on images is accurate?
- Are you able to access recordings easily at particular locations or times in order to comply with a subject access request or police investigations?
- Are there sufficient security safeguards in place to prohibit interception and unauthorised access?
- Do you have an information retention policy which is documented and understood by those who operate the CCTV system?
- Do you ensure that you delete CCTV recordings when they no longer serve a purpose?
- Have you notified individuals with fair processing information including letting them know when they are in an area where a surveillance system is in operation and their right to access their recordings/images?
- Have you put in place appropriate CCTV policies and do your staff know how to respond to requests from individuals for access to CCTV recordings?

Find out more

You can find out more about our Data Protection and Privacy Team by visiting us at www.wrighthassall.co.uk.

Alternatively, please contact a member of our team for further information or advice.

Wright Hassall
Olympus Avenue, Leamington Spa, Warwickshire CV34 6BF
DX 742180 Leamington Spa 6
T: 01926 886688 F: 01926 885588 wrighthassall.co.uk

WRIGHT HASSALL