CCTV's GDPR minefield

Andrew Crowne-Spencer *examines how – a year down the line – general data protection regulations are standing up and discovers where CCTV is concerned, there is still work to be done*

CCTV has been with us for over 75 years, since as far back as 1942 during World War II, when the Germans set up a system developed by Siemens to monitor their rocket testing. The first commercial use of it was in 1949 when an American Government contractor began promoting it. Little is known about the equipment used, but the video couldn't be recorded and could only be used as a live monitoring system. Technology gradually progressed, but the invention of the VCR was a game changer. It advanced CCTV's potential dramatically and in 1968 New York was the first city in the world to install CCTV cameras along a main street. The rest, as they say, is history.

We've come a long way since those early days and CCTV cameras are now a fact of life and surround us wherever we go. In 2001, following the 9/11 attacks in New York, CCTV became a key tool for fighting terrorism and the use of surveillance cameras rocketed around the world. As technology progressed further, with the introduction of digital recording and then IP cameras – which sent, received and stored images via the net – sophisticated surveillance systems became accessible and readily available for private, public and commercial use.

IF COMPANIES DON'T PROPERLY COMPLY WITH GDPR THEY CAN BE PENALISED FINANCIALLY

Six years ago, the British Security Industry Association (BSIA) estimated there were nearly 6 million cameras in the UK, including 750,000 in "sensitive locations" such as schools, hospitals and care homes, and there are some 15,600 on the London Underground network alone. Other estimates put the national tally far lower at 1.85 million but it's virtually impossible to clarify the figures with any degree of accuracy without checking every single property and street from Scotland to Cornwall as they are seemingly everywhere. Whichever figure is nearer the truth, that's still a lot of cameras, which may persuade some people we live in a 'surveillance society', anathema to those who champion their right to privacy and civil liberties. However, there is no doubt CCTV protects businesses, homes and public property while providing police forces and security organisations with a vital tool for both deterring and solving crime. Given the increasing current paranoia about terrorism, especially in high-profile buildings and travel hubs, and the development of more refined technology, one wonders just how many cameras there are watching us at any given time. Lack of mains power is no deterrent as CCTV can now be run from mobile vans or sited on temporary towers and run via solar power, making it ideal for everything from construction sites to agricultural locations, events and festivals. No doubt critical locations are also observed from a satellite in space. There is definitely nowhere CCTV can't go.

INTRODUCTION OF GDPR

With the exponential rise of our use of the internet for everything from social media to shopping and email, collection and use of people's private information became a concern and inevitably regulation to cover data collection and storage was introduced. Across the UK and EU there are now stringent General Data Protection Regulations (GDPR), expanded and updated just a year ago in May 2018, which also cover the use of CCTV and storage of images… but just how good are organisations at complying with them?

A recent investigation by Clearway Services has revealed alarming levels of non-compliance with GDPR where the use of CCTV is concerned. The reasons for this worrying discovery are multiple, but appear mainly to be because the management responsible hasn't bothered to read all the regulations in enough detail, don't think they apply to them, are too lazy to comply with it all or simply don't understand them. These findings are supported by a recent Osterman study which discovered that only 42 percent of organisations have trained their employees around data management and GDPR, meaning 58 percent left their employees completely in the dark. IT functions in companies generally have a good idea about data management, but compliance to GDP Regulation should be shared across the whole organisation and raising awareness of the rules is crucial to prevent data breaches which could impact on an organisation's finances and reputation.

Since our streets and buildings bristle with CCTV cameras recording details and images of our comings and goings (it is estimated that the average Briton is captured on CCTV around 70 times per day) most people believe this is a small compromise to privacy necessary for improved protection from crime. However, facilities, building and security managers or property owners

Picture credit: Getty

really need to check their compliance with regulations is up to scratch before someone complains and they face a hefty fine. One year on from the introduction of the new legislation, GDPR fines totalled €56 million, with more than 200,000 investigations, 64,000 of which were upheld. Admittedly, €50 million of the €56 million total was a single fine against Google by France's National Data Protection Commission, but the figures on investigations can't be denied and of the 64,000 upheld complaints, countries like Slovakia and Sweden have yet to issue a single fine, but countries such as Poland, Portugal, Spain and the Netherlands have fined companies several hundred thousand Euros.

So far three fines have been imposed by the Austrian DPA, all of which involved illegal video surveillance and the fines ranged from €300 to €4,800. It took the Austrian regulator (DSB) no more than four months to issue its first fine for GDPR violation. It was issued to a sports betting cafe owner who had installed a CCTV camera in front of his establishment that also recorded a large part of the pavement where the public were walking past. The DSB found this act to be in violation of the Regulations as large-scale monitoring of public spaces is not permitted. In addition, a further offence was lack of signage about the presence of a camera conducting video surveillance, meaning that the applicable transparency obligations had not been fulfilled.

This is surely only the beginning as each country's data commissioners get a grip on the situation, and as time progresses more companies will face investigation unless they are scrupulous and not sloppy in their compliance. The public tend to accept the fact that wherever they go, inevitably they're on someone's camera, somewhere; it's a fact of life and reassuring in most cases. However, when you think about it, when you are out and about yourself, do you really see or notice advisory signs about CCTV, as much as you should – which is what GDPR demands? The Austrian businessman is by no means a lone offender. And have you any idea where all these images are stored, if they're deleted after a short time or perhaps shared with other parties? Who really knows where you are going or what you are doing?

I believe the answer is a resounding no. The whole point of CCTV is security, and its deterrent factor in part, as well as recording the criminal activity to assist law enforcement bodies in detecting the perpetrators. Therefore, if trespassers or criminals don't even realise

they're on camera, what sort of useless deterrent is that? Furthermore, just how good are the images the cameras are supplying? If they're grainy or blurred due to old or faulty equipment or not set up correctly, that doesn't help anyone except the trespassers or criminals. Ten years ago it was reported that 95 percent of murder cases investigated by London's Metropolitan Police used CCTV footage as evidence, yet latest data suggests 80 percent of footage now available is of such poor quality it's almost worthless. That apart, I find it staggering that these companies, even public sector ones, don't seem to realise that if they're not properly complying with the GDPR they can be penalised financially because of it?

SIX YEARS AGO THE BSIA ESTIMATED THERE WERE NEARLY SIX MILLION CAMERAS IN THE UK

The following example was found on one site recently. It's a great illustration of common compliance failings: The DVR from the security CCTV feeds was sitting on the organisation's reception desk in the building foyer with the monitor on top showing the images. No one was on regular duty at reception and while we watched, a visitor leaned over the desktop to look at the monitor to see if their taxi was at the front door and was busily watching the feed from all the cameras. Moreover, the username and password for the system was on a sticker attached to the monitor. Then, when we walked outside, we discovered all of the CCTV signage was so worn and old that the contact details had faded away and were illegible.

In a second example, a court case was involved. There had been a break-in to a building covered by CCTV and the intruder had been found and arrested by police. The individual was prosecuted and when the case came to court, the lawyer for the defendant asked for all the CCTV footage from different cameras around the site to be shown. This lawyer had obviously done his homework as when the videos were run the intruder was seen on two feeds at exactly the same time. This was because the settings on the equipment hadn't been set right, specifically the correct date and time, and the equipment hadn't been synced properly. The clever lawyer therefore claimed the key CCTV evidence was inadmissible as it was clearly inaccurate since the intruder couldn't be in two places at once. To everyone's frustration, except the burglar and his lawyer, the case was dismissed due to lack of proper evidence.

The message from all this is simple: no matter if you are working for a multi-national, run a small business or are even employed by a security organisation check the CCTV systems you are responsible for are doing what they should and you are complying with GDP Regulation. Because someone, somewhere will be watching what you're doing sooner or later ●

Andrew Crowne-Spencer UK CCTV & Technical Manager at Clearway Services, Dartford, is an expert in physical and electronic security, risk assessment and video analytics.

Failure to ensure that information pertaining to a CCTV camera is legible is a commonly experienced problem

Picture credit: Getty