D-Link®

A Guide to GDPR:
What Will It Have in Store for Video Surveillance?

By Neil Patel, Director European Marketing and Business Development

Over the last 20 years, various crisis and initiatives have come and gone that have resulted in huge consultancy and IT bills - now GDPR has become the latest golden goose which has the industry feathers ruffled. There are numerous "consultants" and companies out there offering services that are being marketed as the panacea to this issue, though how many of these companies are legitimate needs to be seen. What is glaringly clear, however, is that GDPR is seen as the current gravy train within the IT industry. Here, Neil Patel at D-Link Europe, explores and debunks some of the claims being made relating GDPR and its impact on Video Surveillance.

So, starting out, what is GDPR? GDPR, or the General Data Protection Regulation directive, is the result of four years of negotiation by the EU to bring its data protection legislation in line with the new way our data is used. The new EU Legislation imposes new regulations onto organisations both within and outside the EU to protect personal data, how it's accessed and the security around it, combined with tougher penalties for breaches of these rules. 'Personal data' is defined as any information relating to an identified or identifiable person directly or indirectly. In practice this can cover names, email addresses, their phone number - or even a face if it can be linked to a database.

This broad definition has wide ranging implications for companies and individuals using video surveillance, if appropriate action is not taken to ensure compliance. Some outlandish claims are already appearing with suppliers claiming to make GDPR products, but quite simply there is no such thing as a GDPR compliant product. In order for a video surveillance system to be considered as GDPR compliant, the whole solution and/or the organisation running the system must endeavour to be conformant.

After May 25th 2018, the way CCTV video footage is captured and handled must change to fit with the new GDPR guidelines introduced by EU, ensuring that more stringent rules and regulations are implemented in order for business owners and organisations looking to install new CCTV systems. A business owner will now need to have a valid reason for CCTV placement within their businesses, which requires viable reasoning. One such reason may be to help

protect their stocks or assets, the wellbeing of their employees when it comes to health and safety, or to capture footage of any incidents that may occur within the company. Obviously, CCTV cannot be fitted to explicitly monitor on staff. There is a basic requirement for employers to have a valid reason for video surveillance implementation and in what specific areas. Employers using CCTV will need to communicate in advance to their employees the lawful basis for using CCTV in the workplace. Camera positioning and how they are used will need to be reasonable and proportionate - for example, monitoring all employees at general entrance, rather than monitoring a select group of people in view of a positioned CCTV camera.

However, if an employee objected to the use of CCTV in a particular area, GDPR regulations put the burden on the employer to demonstrate that it has a compelling, legitimate reason for processing the employees' personal data, the CCTV images, which outweigh the employees' rights, or grounds for establishing exercising or defending legal claims.

We can accept that businesses that use CCTV are collecting personal data of anyone who is visible within the cameras field of view. To inform people who operate in and around the business, you are already obliged to disclose that CCTV is in use and that their image could be captured on any footage that is obtained. The most common method to do this is to have clearly displayed signs warning people or, in some regions, a contact number for anyone wanting to contact the CCTV operator if they have any queries is required.

Typically footage that has been recorded from CCTV operations is retained for a period of time. The duration of this time varies based on the application and the operator, and around 31 days video retention is not uncommon. In professional deployments, the video is typically recorded and stored to a VMS (Video Management System), or a Network or Digital Video Recorder (NVR). This approach ensures video footage is recorded centrally, which facilitates the ability to enable access control to the footage and log user access. However, with the introduction of more affordable cameras and the rapid adoption of high capacity SD Cards, videos can now also be recorded locally to these cards in the camera itself. This introduces new risk since there is now the possibility that someone can eject and retain the SD Card containing the video leading to security breach. So, for professional installations it is strongly advised that a professional VMS and/or NVR be used.

If the footage needs to be kept for longer time periods, then a risk assessment needs to be carried out to document the reasons for this concession. Images and videos that are acquired through CCTV system might be requested by emergency services, for example. Typically, they will usually view the CCTV footage onsite and this would not warrant any concerns for the leak of the data; as long as they have a written request, ensuring GDPR compliance. Recorded material should be stored in a way that maintains the integrity of the information. This is to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used effectively for its intended purpose. To do this, you need to carefully choose how the information is held and recorded, and ensure that access is restricted. You will also need to ensure that the information is secure and, where necessary, encrypted.

Encryption can provide an effective means to prevent unauthorised access to images processed in a surveillance system. When access is provided, a log of where, what, by whom and how the data was accessed must be retained. In this instance the Fundamental Data Protection principles of GDPR are applicable, the data controller not only accepts accountability for compliance, but also needs to clearly demonstrate their processes to ensure accountability. Lawful processing and special categories of personal data, GDPR contains similar conditions for lawful processing of personal data as defined in local data protection laws.

As far as public authorities' use of CCTV systems is concerned, it should be noted that the condition that the processing of personal data is 'necessary for the purposes of legitimate interests pursued by the data controller' will not apply to public authorities. Instead, a public authority will need to consider whether it can plausibly make use of one of the other conditions, e.g. 'performance of a task carried out in the public interest' to justify the use of CCTV.

It's becoming increasingly common to find security cameras being deployed in residential domestic properties these days, either installed professional or by doing it yourself. These DIY Home Surveillance solutions typically use Wi-Fi to communicate with the cameras and record video to the cloud. Even though these domestic installations are simply designed, they equally have stringent restrictions which most consumers are unaware. Everybody has the right to protect their property; security lights, alarms, locks, CCTV are just some of the possible security measures that can be taken. CCTV is the most overt solution, in fact, before getting a CCTV system for your home, there are a couple of considerations that need to be deliberated first. You must consider how your CCTV system might have an impact on the privacy of your

neighbours and their properties. Legally, home CCTV use can be a bit of a grey area. As long as the cameras are being used to monitor your property only, and within its boundaries, you should be ok as a rule. Unless you're streaming the footage publicly, so in effect broadcasting images of the visitors to your home, then similar rules apply as to when cameras capture footage beyond your property fences – such as public pavements, roads and neighbouring properties.

If a domestic CCTV system is monitoring the movements of strangers outside the property boundaries, then it is effectively collecting data on those individuals. It is therefore covered by GDPR regulation, this requires that the individual who is operating the system register with their local Information Commissioner as a data controller, which will have an annual fee associated with it. Most home security cameras will inevitably capture footage from beyond the property boundary, it's often unavoidable. So it is important to ensure that clear signs stating that CCTV is in operation. The home owners needs to ensure that the footage is used for security use only is retained securely for the minimum number of days. The footage should not be released to third parties. However, where a camera has been captured a crime, the footage can be kept for as long as needed to detect and prosecute the crime. The footage captured can also be passed on to the police and other authorities to achieve this.

Article 8 of The European Convention on Human Rights Act 1998 states that an individual has the right to respect for their private and family life, and of their home. If security cameras monitor the activities of their neighbours – that would be a breach of their human rights and could open the home owner up to prosecution.

A case brought to the European Court of Justice (EJC) clearly highlights how grey an area this can be, the case related to a Czech man, František Ryneš, who installed a surveillance camera after he and his family were subjected to attacks by unknown individuals. His cameras filmed areas including public footpaths and the entrance to the house opposite. Ryneš CCTV system captured someone firing a catapult at his home and breaking a window. The video footage was passed to police, enabling them to identify two suspects who were subsequently prosecuted. One of the suspects challenged the legality of the recording and the retention if of the images. The local Czech office for the protection of personal data, ruled that although Ryneš had been legitimately trying to expose a crime, he had infringed the local data protection laws and issued him with a fine. Ryneš appealed against the ruling and the supreme administrative court in the Czech Republic referred the case to the ECJ, asking whether European data-protection directive

rules on the processing of personal data applied. The court decided Ryneš was not liable for the fine because he had acted to help prosecute a criminal. However, the judgment suggested that if a crime had not been committed he would have breached European data regulations. The judges said: "The operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the homeowners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision." This ruling can contradict the application of the directive in some countries like the UK, this makes the application of GDPR in a domestic setting open to interpretation. New technological advancements such as the Internet of Things (IOT) and their application in the home leading to trends like smart homes will further muddy the waters. With the high level of integration becoming common place with industry initiatives like Amazon Alexa, Google Thread or Apple Home making interaction between different products from different vendors easier to achieve, technological development will test the boundaries of GDPR. One such case, is the use of cameras that incorporate (directly or the cloud) intelligent video analytics such as face recognition to help recognise family members so that doors, lights, heating etc. are activated.

A recent survey conducted by Commvault revealed that only 1 in 8 of global IT organisations understood how GDPR would affect their cloud services. Selecting the right cloud service provider will give business a significant commercial advantage, since the supply chain partners who have taken the appropriate steps to achieve GDPR compliance will be in a better position with the regulators. There are already a number of standards that apply to cloud though they are not specific to GDPR such as, ISO27001, PCI compliance and Sarbanes-Oxley Act compliance (or SOX) for example are cloud regulations that are not directly related to the General Data Protection Directive. But to demonstrate that GDPR-compliance is being addressed directly and comprehensively, an organisation utilising a cloud provider needs to ensure that there is a legal contract defining the restrictions around the key Data Controller and Processor relationship concepts of the new regulation.

From a video surveillance perspective, it is critical for people and businesses using any cloud recording service to know the location where their data/footage is being processed or stored. Data is seldom stored where the cloud provider is headquartered, the data can be moved around between a supplier's data centres, meaning it can reside anywhere in the world unknowingly.

Individuals or business using cloud based recording services should take adequate security measures to protect the recorded data from loss, alteration, or unauthorised processing. They should only collect and retain "necessary" video data and limit the processing of "special" data, as well as confirm what data processing is being conducted. As well as ensure that they clearly own the data and that they do are share the data with third parties. Further a defined data or video retention policy should be in place so that after predetermined amount of time anything that is not needed for legal reason is erased. Make sure that the any cloud recording service clearly states that once you download your own data immediately, and they will erase all your video data once you've terminated service. Confirm how it will take them to do this. The more immediate (in less than a week), the better, as lingering data carries a higher risk of noncompliance.

What is evident is GDPR will have a major impact on the use of video surveillance, how it applies to the different uses of cameras and video retention remains to be seen. What is evident, is that with the introduction of GDPR in May 2018, the use of cameras coupled with the evolution of cloud based video recording services will have to planned and considered carefully, with local legislation undergoing some major changes to accommodate this new law.

For more information: www.dlink.com

Updated April 2018