11/07/2019

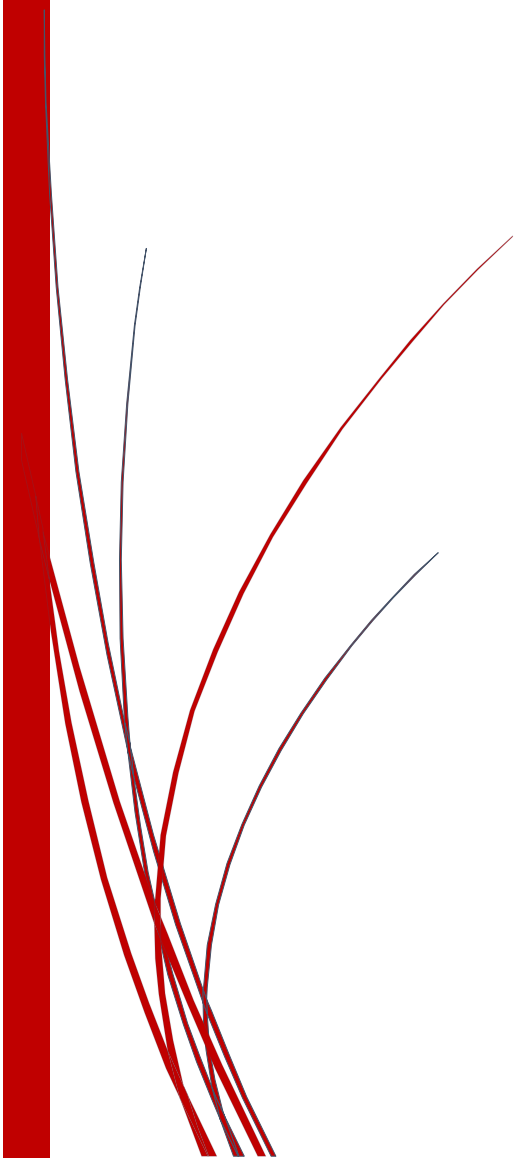
SINCE 1972

POINTER

inform & protect

GDPR and Video Systems

How does GDPR affect the operation and management of Video Systems? How Pointer approaches the challenges.



Samantha Borland

POINTER LTD

CONTENTS

GDPR AND SECURITY

'ORGANISATIONS IN THE UK HAVE BEEN HIT BY OVER 10,000 DATA BREACHES SINCE THE ARRIVAL OF THE GENERAL DATA PROTECTION REGULATION (GDPR) ON MAY 25TH, 2018, A STUDY FINDS.' (DLA PIPER)

That puts the UK as 3rd after Germany and the Netherlands in terms of the number data breaches which were reported within the first 8 months of the introduction of GDPR. These three countries alone made up 65% of the breach notifications that were reported from May 25th, 2018 to Jan 28th, 2019.

Many companies have already suffered penalties for violation of GDPR. One of the more recent fines imposed by the ICO has been to British Airways for a staggering £183 million which is 1.5% of its annual global turnover. This was due to a data breach relating to the theft of customers' personal and financial information between August 21st 2018 and September 5th 2018. This sounds like a huge fine, however the ICO can impose penalties of up to 4% of a company's annual global turnover depending on the severity of the data breach, therefore this fine could have been be a lot higher.

GDPR has affected how companies operate all over the world, forcing them to change their protocols and policies to accommodate GDPR. This document outlines how GDPR affects your Video Systems and how we at Pointer can help you to address these challenges. As trusted advisors to our customers, we work together to highlight areas where current systems may fall short of the standards of compliance and give advice on how to address this both from a technology and policy perspective.

WHAT DOES THIS MEAN FOR YOUR ORGANISATION?

The introduction of GDPR means that **you** have a duty of care for any data that can identify an individual. As a result, it is up to **you** to put in place the necessary security measures and protocols to ensure that this valuable information is kept secure and protected. **You** are now responsible for the management of this valuable data and therefore responsible for possible data breaches that could occur.

95,180 COMPLAINTS HAVE BEEN MADE TO EU NATIONAL DATA PROTECTION AUTHORITIES (DPAS) BY INDIVIDUALS WHO BELIEVE THEIR RIGHTS UNDER THE GDPR HAVE BEEN VIOLATED. THE MAJORITY OF THESE COMPLAINTS CONCERNED TELEMARKETING, PROMOTIONAL EMAILS, AND VIDEO SURVEILLANCE/CCTV

Lexolgy.com/library

VIDEO SYSTEM BREACHES

CCTV/Video Surveillance is one of the three highest complaints regarding breaches in GDPR Regulation.

Recent studies by the British Security Industry Association (BSIA) show that there are between 4 million and 5.9 million CCTV cameras in the UK. This includes both private and public facing cameras.

This is a huge amount of surveillance which has left many people feeling that their privacy has been violated. The introduction of GDPR has highlighted the privacy issues that the installation of Video Systems creates and enforced strict guidelines to ensure that the use of Video Systems does not impose upon a person's right to privacy.

DATA PROTECTION ISSUES AND VIDEO SYSTEMS

There are several things that need to be considered when installing and using a Video system in order to make sure that it complies with GDPR.

1. What do you have to see?
2. Why do you need to see it?
3. What are you going to do with the information that you capture?

Cameras can, and should, only be used strategically, and should only target potential security or operational risk areas you have identified. This will ensure maximum security coverage and minimize the gathering of irrelevant footage. The cameras use must be justified, and this information should be recorded in your GDPR policy document.

Individuals potentially affected by video surveillance must be informed upon its installation about the areas monitored, its purpose and the length of time it is retained and by whom. There should be strict camera use policies in place, reviewed on a regular basis to ensure that they comply fully with GDPR and any other data protection legislation.

The timely and automatic deletion of footage is essential. No images and information should be stored beyond the retention period stated in your GDPR policy document relating to the purpose of the Video system. These images should subsequently be deleted once their purpose has been discharged.

HOW DOES POINTER ADDRESS THIS?

Since the introduction of GDPR, Pointer have provided our staff with the necessary training to ensure that they are aware of the precautions that they need to take in order to install Video Systems and security systems that are compliant with current GDPR regulations.

Our approach to GDPR compliance is threefold;

1. Intelligent use of Video Systems
2. Restrict access to Video footage
3. Advise and inform customers

INTELLIGENT USE OF VIDEO SYSTEMS

The installation of Video systems needs to be done with care. 'Intelligent Use' of Video Systems, takes into consideration factors such as the field of view deemed necessary for optimal security operations, data capture and storage and how this relates to your GDPR policy.

Camera positioning is also very important as you want to be able to capture footage that is relevant to your security or operational needs without capturing excessive footage that could lead to non-compliance. This also applies to any audio as this also subject to GDPR legislation.

One way that we do this by carrying out a Privacy Impact Assessment which identifies and documents the following:

- field of vision required for your security and operational needs e.g. security of your staff or premises, occupancy levels etc
- the areas that are more public where privacy masking should be deployed.

This report should be kept alongside your GDPR policy document and reviewed annually during one of our system health check visits. The annual review is strongly recommended as the external environment around your premises may change e.g. new buildings erected or change of use for residential property where previously it was commercial warehouse etc

Video Systems must also be correctly sign posted with appropriate information as to the purpose of the Video Recording in the area. Notices need to be clear and concise to indicate what footage is used for e.g. for security purposes or monitor manufacturing processes. This needs to be reflected in the signage used and policies implemented.

RESTRICTED ACCESS TO RECORDED FOOTAGE

It is important to restrict access to recorded footage to avoid sensitive data falling into the wrong hands. Pointer uses the latest technological developments to ensure that all footage is encrypted and recommend that system access is restricted by linking to the client's employee database such as Microsoft Active Directory. This means the client has only one data base to update to ensure only authorised personnel have the required access to carry out their job function.

Our cyber security specialists can provide protection against both internal and external threats. GDPR has imposed a duty of care to anyone that handles or processes the public's personal information, therefore it is your responsibility to manage it responsibly and provide appropriate measures to protect it.

ADVISE AND INFORM CUSTOMERS

Pointer have been trusted advisors to their customers since the company was founded in 1972. We advise our customers on best practices for their security systems. This information is generally used to inform training sessions for your staff to ensure that those who have access to your security systems are properly trained to use them, in terms of functionality and GDPR policy implementation.

Ignorance is no excuse for anyone who has implemented a Video system and can have huge consequences if it is deemed as a breach to GDPR. This could be because of improper signage or a privacy policy that doesn't include all factors of the purpose of the use of your CCTV.

One company that fell victim to this downfall was True Visions Productions who were filming a documentary for Channel 4. They set up cameras and microphones in examination rooms at the clinic at Addenbrooke's Hospital in Cambridge. The ICO has since issued a £120,000 fine for unfairly and unlawfully filming patients.

In a statement they said, 'although TVP had the hospital trust's permission to be on site, TVP did not provide patients with adequate information about the filming'. This is just one of many examples of the effects of improper use of Video Recording Equipment.

WHERE DO WE GO FROM HERE?

Video Systems are a valuable tool to protect your business from external threats, gather valuable operational business information and you should not see GDPR as a threat to the use of Video Systems, but instead as a set of guidelines to improve the effectiveness of your Video Systems without impacting those around you in a negative way.

Providing that you choose a security solutions integrator with the relevant skills and experience, installing Video Systems should be an easy, painless process. You need to remain mindful of all privacy legislation and continue to adhere to it at all costs as you do not want to fall foul of the legislation like some of the companies previously mentioned in this article. Potential penalties can easily be avoided by making sure that you choose the correct security systems integrator for your security needs.

For more information on GDPR, please read the section at the end of this document entitled, ‘What is GDPR?’.

For more information or advice please contact Pointer via our website at

https://www.pointer.co.uk/contact-us/

REFERENCES

European Commission publishes statistics on GDPR enforcement activities

https://www.lexology.com/library/detail.aspx?g=179a6306-d3b0-4373-9f66-46000e785914

https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf

EU GDPR.ORG

https://eugdpr.org/

European Data Protection Supervisor

https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en

BSIA: CCTV Privacy Masking- a guide

https://www.bsia.co.uk/Portals/4/Publications/197-cctv-privacy-marking-02%20(2).pdf

Hanwha Techwin Europe: GDPR for CCTV Systems

https://www.hanwha-security.eu/wp-content/uploads/2018/05/Hanwha-Techwin-GDPR-White-Paper-for-CCTV-Systems.pdf

British Firms Suffer 10000 data breaches in GDPR era

https://gdpr.report/news/2019/02/11/british-firms-suffer-10000-data-breaches-in-gdpr-era/

WHAT IS GDPR?

The General Data Protection act, introduced to the EU in 25th May 2018, is the most important change to data privacy regulations in 20 years. It completely changed the structure of data privacy and affected all business sectors both private and public across the EU. It was designed to protect all EU citizens and to give them the right to know exactly what their private information was being used for, helping citizens to make informed decisions about their own personal information.

KEY PRINCIPLES OF GDPR

GDPR brought about a huge overhaul of the way that information was managed and how it was stored and protected. The key principles, outlined by eugdpr.org, are as follows;

Increased Scope: One of the biggest changes brought by GDPR legislation is extended jurisdiction of data protection as it applies not only to organizations that reside in the EU but also to any organization that processes public information of EU citizens but are not established in the EU. In other words, to operate an organization that deals in the EU, you must abide by GDPR regulations regardless of location.

Penalties: Organisations that breach GDPR Regulation are subject to major penalties and can be fined up to 4% of annual turnover or 20 million, whichever is higher.

Consent: Companies must now make asking for consent, a clear straight forward process. Lengthy, jargon filled consent policies must now be simplified to provide clear and concise information to customers and it must be as easy to withdraw consent as it is to give consent.

Breach Notification: If there has been a data breach, it must be reported within 72 hours of becoming aware of the breach.

Right to Access: EU citizens have the right to ask any organization that is using their data, to give them information on exactly what their data is being used for and if requested, they must provide an electronic report of this.

Right to be Forgotten: Citizens have the right to have their data erased and cease any further use of their data. The conditions for this include the data no longer being relevant to the original purposes it was collected for or the data subject withdrawing their consent.

Data Portability: This is the right for a person to be able to have access to any of the personal data that concern them in a 'commonly use and machine-readable format'.

Privacy by Design: This involves the controller of any personal data to design their systems in a way that meets the requirements of GDPR. It should only hold and process the data

necessary for the completion of its duties as well as limiting access to personal data to only those who need to have access.

Data Protection Officers: Organisations now have internal record keeping requirements in relation to GDPR and DPO appointment is only necessary for those organisations whose core activities require regular monitoring and use of personal data.