European General Data Protection Regulation (GDPR)

Implications for video surveillance

AXIS COMMUNICATIONS

Table of contents

European General Data Protection Regulation (GDPR) comes into effect on May 25th 2018. It aims to give individuals more control over how data held on them is collected, processed and shared, which has implications for installers, systems integrators and users of video surveillance technology.

GDPR provides a structure that helps make roles and responsibilities clearer for businesses, and also gives individuals more opportunities to control how their personal data is used.

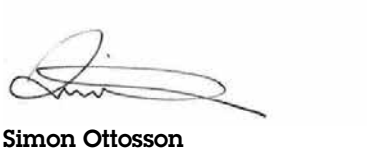
The regulation governs both organizations based in the European Union (EU), and those processing and holding the personal data of data subjects residing in the EU – regardless of the organization's location.

As an organization, Axis has always been committed to respecting and safeguarding individuals' privacy. As such, Axis is wholeheartedly behind the introduction of GDPR and, while working towards full compliance for Axis itself, will provide support to its customers in order to facilitate their compliance in the best possible way.

Axis has taken steps to put in place a model for GDPR compliance. Part of this strategy includes continued testing and review to ensure that activities Axis undertakes regarding data processing remain secure.

Many organizations have questions regarding GDPR. Why do we need this new regulation now? What does the regulation entail? How does it impact video surveillance? And what steps should be taken to ensure compliance?

This white paper explores the implications of GDPR and aims to help players in the video surveillance sector navigate the challenges and opportunities of GDPR.



Simon Ottosson
Legal counsel
Axis Communications

Edwin Roobol
Regional Director Middle Europe
Axis Communications

1. What is GDPR?

General Data Protection Regulation (GDPR) is a set of rules that governs all forms of personal data that is held by an organization. GDPR gives every individual ownership of their personal data, and, on the organization's side, introduces accountability at all stages of data processing and storage. GDPR achieves this by affording a number of rights to individuals and putting corresponding obligations on the organizations that process personal data.

What is personal data?
A key part of understanding GDPR is being clear on the legal definition of personal data. The legislation defines personal data as any information relating to an identified or identifiable person. An identifiable person is someone who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier such as IP addresses or cookie identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Geographical reach of GDPR
GDPR always applies to a company's processing of personal data if the company is established within the EU. If the company does not have an establishment within the EU, GDPR applies if the processed data concerns persons who are in the EU, if the data processing is related to the offering of goods or services to these persons when they are in the EU, or the monitoring of these persons behaviour when they are in the EU. So, clearly, this European regulation has global impact.

Different responsibilities for organizations
Any organization that is processing or storing personal data must take responsibility for ensuring that they do that in a GDPR compliant manner.

GDPR classifies organizations in two categories: *data controllers*, and *data processors*, each with its own legal obligations:

Data controller: A data controller is someone who determines the purpose and means of processing of personal data, for example a store owner that uses a CCTV system for surveillance purposes.

Data processor: A data processor is someone who processes personal data on behalf of and in accordance with instructions provided by the data controller. A processor could be a company that manages data gathered from a CCTV system on behalf of and in accordance with instructions provided by someone that has a CCTV system for surveillance purposes, for example a store owner.

Privacy by design and privacy by default
According to GDPR, the controller of personal data, when processing such data, has an obligation to implement technical or organizational measures which are designed to implement the data protection principles set out in GDPR. GDPR refers to this as *privacy by design*. In the context of a camera including firmware, a relevant example of privacy by design would be a feature that digitally allowed the user to restrict image capture to a certain perimeter, preventing the camera from capturing any imagery outside this perimeter that would otherwise be captured.

The controller also has an obligation to implement technical or organizational measures which by default ensure the least privacy intrusive processing of the personal data in question, GDPR refers to this as *privacy by default*. In the context of a camera including firmware, a relevant example of privacy by default could be a feature that automatically prompted the user to set the exact image capture perimeter according to the above example.

The rights of individuals
One of the main driving forces behind GDPR is the need to give individuals greater protection and a set of rights governing their personal data. There are some very specific requirements under the terms of the regulation, all of which mean that the party processing or storing personal data has a responsibility to keep this data private.

The regulation also gives individuals the right to be made aware when their personal data is being collected at the point of capture, and how it will be used. In the case of video surveillance, for example, these will mean appropriate signage in and around the area where video surveillance is being used.

2. How does GDPR affect video surveillance?

Much of the debate around GDPR has focused on securely storing and processing more traditional data – such as a list of names and email addresses stored in a spreadsheet or database. There's been much less focus on the moving image, but it's an area that companies need to be equally aware of.

To the extent surveillance video contains personal data, it will be subject to the provisions of GDPR.

GDPR impact on the use of surveillance equipment, such as camera products and solutions
When it comes to products and solutions sold by Axis, it is the user, as controller, of the product or solution that is primarily responsible for making sure that any such use of a product or solution to process personal data is GDPR compliant. This means that in the context of products and solutions, GDPR compliance or instances of breach at large depend on how the customer uses the product or solution.

GDPR impacts the use of specific hosted services
In the case of services, GDPR compliance depends to some extent on how the service is provided, which is the responsibility of Axis. But still, GDPR compliance or instances of breach largely depend on how the service is used by customers. What type of GDPR obligations that arises and who has those obligations must be examined on an application-specific basis.

Let's take a hosted service, AXIS Guardian, as an example. This is how GDPR will typically be applied and who will be responsible for what:

> *Alarm operator's customers:* Data controller for personal data contained in the video material that is captured by the user's camera surveillance system and uploaded in AXIS Guardian.
> *Alarm operator:* Data processor on behalf of users for personal data uploaded in AXIS Guardian by the user (e.g. user employee information and captured video).
> *Axis:* Data processor on behalf of alarm operator for personal data uploaded in AXIS Guardian by alarm operator (e.g. alarm operator employee information) and personal data sub-processor on behalf of alarm operator for personal data uploaded in AXIS Guardian by alarm operator's customers (captured video).
> *Amazon Web Services:* Data sub-processor on behalf of Axis for personal data uploaded in AXIS Guardian by alarm operator and alarm operator's customers (users).

2.1 Steps towards GDPR compliance

GDPR is a regulation that is going to influence how organisations handle data, including video data, in the future.

As a minimum, each organization that processes personal data will need one or more designated persons responsible for making sure that that the organization handles personal data in line with GDPR and company policy (the number of man hours allocated for this will of course depend on the size of the organization and the amount of personal data collected and processed). In addition, for some organizations GDPR will require the appointment of a formal Data Protection Officer (DPO) to perform these tasks.

There will also be changes in the administrative process. Under GDPR, organizations need to keep detailed and accurate records of their data processing activities. There's a range of details that must be recorded, including but not limited to:

- What category of individuals the processed personal data relate to (e.g. customers, employees, store visitors, etc.)
- For what purposes the personal data is used
- Whether the personal data is going to be transferred – to other companies and/or outside the EU
- How long the personal data will be stored
- Measures taken by the organization, in relation each separate data processing activity, to ensure GDPR compliance

All of this is relevant when it comes to stored surveillance video.

Organizations are obligated to explain why a video camera is in a particular place, what is being filmed and why. In the case of video surveillance, appropriate signage in and around the area where video surveillance is being used should be used to provide information about this.

The data controller may be obliged to carry out a Data Protection Impact Assessment (DPIA) when it comes to setting up a camera in a public place. A DPIA should include (the exact features of a DPIA must be decided on a case specific basis):

- A systematic description of the intended processing operations and processing purposes
- An assessment of the necessity and proportionality of the processing operations in terms of purpose
- Risk assessment for individuals' rights and freedoms
- Planned measures to address these risks, including safeguards and mechanisms to ensure the protection of personal data and compliance with GDPR (this should take into account the rights and legitimate interests of individuals and other affected persons)

One of the key features of the new regulation is that those who are being monitored need to be fully informed about what data is being held on them and how it's being used.

The regulation sets out some clear ground rules about encryption and how data should be protected. The fact that data is in the form of video doesn't alter this requirement.

Companies storing video, therefore, have clear responsibilities when it comes to storing personal data and must put into place the robust measures to prevent unauthorized access. This means that it's important to set out, in writing, who will have access to the cameras and recordings.

Organizations should also have a procedure in place for when an individual chooses to exercise their right of access to personal data or request its deletion. This is so that they can stay within the prescribed month-long window within which they must comply with these requests under GDPR. When making such a request, it is reasonable to expect the enquirer to provide adequate information in order to locate this data – for example an approximate timeframe, and the location where the footage was captured.

Companies should use strong measures to prevent unauthorized access to the personal data that they are storing. The tactics used by each company will be unique to the challenges they face, however, in all instances companies must employ robust security controls, stay up-to-date with cybersecurity best practice, and ensure that they are working with trusted partners who provide secure hardware, software and thorough aftercare.

3. Conclusion

It is ultimately the user of surveillance equipment, surveillance solutions and surveillance services that is responsible for GDPR compliance and the safeguarding of the rights of the individuals whose personal data the user processes. Organizations that have done little or nothing will need to get their house in order. Businesses who have done their homework and paid attention to their responsibilities under the regulation have less to worry about.

As a user of surveillance equipment, surveillance solutions and surveillance services, it is therefore important to partner with suppliers and vendors that are committed to respecting and safeguarding individuals' privacy and protecting personal data. As a user of surveillance equipment, surveillance solutions and surveillance services, you should also be able to rely on support and technical aid from your suppliers and vendors to facilitate your GDPR compliance.

Additional resources:

Full details of GDPR

European Data Protection Supervisor website

Data Protection guidance for small and medium businesses website

72045/EN/R1/1804

Axis Communications in perspective

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance, access control and audio systems, as well as video analytics.

Axis has more than 2,800 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Founded in 1984, Axis is a Sweden-based company listed on the NASDAQ Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.

AXIS COMMUNICATIONS