General Data Protection Regulation (GDPR) Impact on Video Surveillance

Summary

The General Data Protection Regulation (EU2016/679) ("GDPR") is a European Union regulation to protect the personal data of Europeans. If you are a citizen of a country in the European Economic Area, or live, work or travel through in one of these countries, then your personal data is covered by this regulation. Personal data collected in Europe is covered regardless of where the company that collects or processes the data is located. Enforcement of the GDPR begins on May 25th 2018.

The GDPR protects personal data regardless of where processed. For example, an US company selling products or services to people in the UK must comply with the GDPR, even though it is based in the US. One reason this law has the attention of organizations is that regulators could **fine a company up to the GREATER of €20 million or 4% of the company's global annual revenue**.

At Johnson Controls, we care about privacy and security and are committed to protecting personal data in accordance with fair information practices and applicable data privacy laws, including the GDPR. Privacy and security are important requirements that we take into account throughout the product lifecycle. However, under the GDPR, you need to decide what policies and procedures are required for your company to comply.

Privacy regulations can be complicated, highly dependent upon individual circumstances, and individual countries have laws that may differ from the requirements of the GDPR. This document is intended to provide you with more information about how the GDPR may affect your organization, but it is not a substitute for professional advice regarding your processing, storage or use of personal data. ***Johnson Controls makes no representation or warranty, express or implied, as to the efficacy of the privacy practices described in these materials for ensuring compliance with the GDPR or any other privacy law or regulation and disclaims all liability for any damages that may occur despite compliance with the recommendations contained in these materials.***

Definitions

Before getting into what the GDPR means for security systems in general and video surveillance solutions more specifically, there are some definitions you need to understand:

- **Personal Data** are data that can, directly or in combination with other information, be used to identify a living individual. Examples of personal data are email addresses, telephone numbers and images.
- **Data Subject** is the living individual who is the subject of Personal Data.
- **Data Controller** is the person or organization that decides the means and manner in which Personal Data are processed.

- **Data Processor** is a person or organization that collects or stores Personal Data on behalf of a Data Controller.
- **Supervisory Authority** is an independent public authority established by an EU Member State. The supervisory authority will ensure that organizations are complying with the GDPR.
- **Data Protection Officer** coordinates an organization's communication and compliance with the GDPR. Under the GDPR, some organizations are required to have a Data Protection Officer.

Most organizations that operate a security system are data controllers because they collect some Personal Data from Data Subjects, like employees, contractors and visitors. Video surveillance systems routinely capture images of people. Because these images can identify living individuals, they are considered Personal Data, and the organization that is responsible for their collection, use and storage is a Data Controller.

Overview

The GDPR, like other privacy laws, incorporates a number of fundamental principles, including transparency and fairness, ensuring that there is a legitimate purpose for processing Personal Data, limitation of Personal Data processing, ensuring accuracy and ensuring that Personal Data are properly protected. In addition, individuals have specific rights under the GDPR, and organizations that processes Personal Data need to ensure that they accommodate the exercise of those rights. Every organization that processes Personal Data should ensure that it has a program in place to ensure that such Personal Data is handled correctly. A minimal privacy program should start with: (1) an understanding of what Personal Data the organization processes and why; (2) a good privacy policy and a privacy notice that is integrated with the organizations terms of service, if appropriate; (3) a process for responding to a Data Subject's request to exercise his or her rights; (4) policies to ensure that Personal Data are used for the purposes intended, and additional rules for other uses, such as opt-in/opt-out practices for marketing; (5) a procedure for responding to Personal Data breaches; and (6) an employee education program.

Privacy Policies and Practices

Ensuring transparency and fairness means ensuring that individuals are informed about what Personal Data will be processed, for what reason, by whom, and other relevant information. For some activities, the Data Subject may need to give permission (consent or opt-in) before their Personal Data can be used. That consent must be freely given and based on full information about how the Personal Data will be used. Organizations that process Personal Data need to ensure that they provide appropriate notice to Data Subjects about how Personal Data is treated.

Once you have a good understanding of what information you process and how, your organization should ensure that it has a privacy notice that accurately informs Data Subjects of your practices. Make sure that you have processes in place to limit what Personal Data you collect to what you really need. In order to process anyone's Personal Data, you need to have a legitimate reason to do so. For example, you would legitimately need identifying and contact information to complete a sale. Likewise, helping to ensure the safety and security of employees on your premises may be a legitimate basis. Personal Data should only be used for the purpose originally collected. New uses may require new notice to

customers. Also, be aware that specific uses may have additional requirements. For example, many marketing activities require consent, or opt-ins, and you must always honor requests to opt-out of marketing.

Data Subject Rights

Under the GDPR, Data Subjects have certain rights to control their Personal Data. Organizations handling Personal Data need to understand these rights and ensure that they can respond to requests to exercise them promptly. Under the GDPR, you must acknowledge receipt of a request within seven days, and respond within a month. You may be able to request additional time for very broad or complex requests. The rights afforded to Data Subjects under the GDPR consist of the following:

1. The **right of access,** which means knowing; if, where and why their Personal Data are being processed.
2. The **right to rectification** of Personal Data, which is the right to correct inaccurate data. Data Subjects must be specifically informed of this right.
3. The **right to withdraw** consent that has been previously given.
4. The **right to erasure**, also known as the right to be forgotten, allows certain Personal Data to be erased. Data Subjects must be specifically informed of this right.
5. The **right to restriction of processing**, which means limiting the processing of Personal Data in certain circumstances. Data Subjects must be specifically informed of this right.
6. The **right to data portability**, which means individuals, can ask to transfer their Personal Data to a new Data Controller. This right is limited to Personal Data provided by the subject, processed automatically and processed based on a contract or the subject's.
7. The **right to object** to processing primarily applies to the automated processing of Personal Data. Examples would be profiling for characteristics or behavior for marketing, or processing Personal Data for statistical or research purposes. In these circumstances, an individual could say they do not want their Personal Data processed.
8. The **right not to be subject to solely automated processing,** which means that a Data Subject could ask for human intervention in an otherwise automated process.
9. The **right to lodge a complaint**, either with the organization processing their Personal Data, or with a supervisory authority.

With those rights in mind, organizations need to assess the types of data they currently process, how they processes that data, and what controls they have in place. This includes identifying what types of Personal Data, such as recognizable facial images they have, where it is stored and who has access to it.

Protecting Personal Data and Data Breaches

A key data protection requirement is limiting access to Personal Data. This can be accomplished in several ways including data collection minimization for physical security systems. Video surveillance solutions typically have password protection and some form of multi-level privilege management, as well as actively monitoring to ensure that only authorized personnel can gain access to Personal Data in

the system. It is important for security teams to give thought to who should have access to Personal Data, and have a set of policies and procedures in place to review operator privileges.

For example, a security guard who should not have access to Personal Data accidentally views an individual's personnel record. The organization discovers the incident immediately, adjusts privileges to prohibit future access and, since there is no harm to the Data Subject, the incident is logged and forgotten. The GDPR defines a reportable "personal data breach" as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed." You could view the above example as unauthorized access, even if unintentional, and one that did not cause any obvious harm. However, if there is a risk to the "rights and freedoms" of a Data Subject, meaning financial or reputational harm, or perhaps even loss of control over their Personal Data, then the breach might need to be reported to the Supervisory Authority "without undue delay", but not more than 72 hours. The notice must describe the breach and measures taken to remediate the situation. Failing to report breaches of Personal Data can have serious consequences under the GDPR, as fines can reach up to the greater of €10 million or 2% of an organization's annual turnover for this type of incident.

Develop a plan

Organizations should review their physical security systems and the Personal Data stored by those systems. This does not just include electronic systems, but also any other processes, such as paper-based systems (i.e., visitor logs), that may collect Personal Data. The following steps can help your organization to develop a plan for compliance:

1. Identify the types of Personal Data they have stored on all of their security systems, including paper-based, hosted or stored off-premises or in the cloud.
2. Understand how Personal Data are used in your organization, specifically the data flow and access points.
3. Minimize the Personal Data collected and stored, and ensure that only properly authorized people have access to it.
4. Make sure you are getting consent from Data Subjects if needed.
5. Assess current policies and procedures to ensure that you have documented how your organization handles Personal Data – both to inform Data Subjects, and to make sure your employees know the rules.
6. Have plans for handling requests from Data Subjects and for data breaches if they happen.
7. Train your employees to handle Personal Data properly by limiting what they collect, keeping it safe, and deleting it when no longer needed.

Organisations that are using or planning to use video surveillance systems, must plan for data privacy and have robust privacy processes in place.

Johnson Controls, Security Products Video

It is important to note that product and/or product solutions are not by themselves GDPR compliant. Any company that is subject to the GDPR will need to decide what policies and procedures are required to comply with their responsibilities under the regulation, and to procure, configure and use products and/or product solutions in a manner that is compliant.

Johnson Controls' Video product portfolio includes a number of features and functions that can ease some aspects of GDPR compliance – specifically its requirements for security and limitation of data processed. Such features may include encryption, role-based access control to limit which users can access data, and logs to which provide audit trails for data access and transfers. However, compliance with the GDPR can only be achieved through deployment designs and operator policies created specifically to meet the application needs of each individual customer. Therefore, GDPR compliance cannot be solved by a product's feature set. While the product's feature set can make GDPR compliance easier to achieve, there will inevitably be deployment specific and customer specific actions required to assure compliance with the GDPR. GDPR privacy laws also contain restrictions about where data is stored, what information is stored and user consent requirements that product features cannot address.

The GDPR requires Data Controllers to limit the Personal Data they process, using only the data that is actually needed. Video Products is working to introduce "Face Redaction" into their Illustra camera range and video management software /network video recorder portfolio. This password protected function will allow individual faces to be "pixilated", hiding facial features but allowing the rest of the image to be clearly seen.

Conclusion

Enforcement of the GDPR starts on May 25th, 2018, and all organizations whose physical security systems collect Personal Data from Europeans will need to ensure their processes meet the regulations. It is important to understand how the GDPR may affect your organization and take steps to mitigate the risks you identify.

Resources

The data protection supervisory authority in your region can provide additional information about how to comply with privacy laws. Several of these authorities have produced guidelines:

UK - Information Commissioner's Office (https://ico.org.uk/): The ICO site contains a number of well-written guides for businesses, with guides specifically tailored to a number of sectors. There is also a comprehensive guide to the GDPR. Note that Brexit may affect data protection in the UK, but it is unclear at this time how that issue will be resolved.

Ireland - Data Protection Commissioner (https://dataprotection.ie/docs/Home/4.htm): With many technology giants domiciled in Ireland, the Irish data protection authority is expected to be at the center of many data protection issues under the GDPR. The Commissioner's site has information on data protection for organizations, and on the GDPR. There is a *Data Protection and You* site with easy to understand guidance on the GDPR for organizations.

France - Commission Nationale de l'Informatique et des Libertés (CNIL) https://www.cnil.fr/: The CNIL site is published in both French and English. The CNIL has general publications, as well as some free tools for Data Processors on its site.

The **European Commission** site for Data Protection (in English) is at https://ec.europa.eu/info/law/law-topic/data-protection_en.

A list of **European data protection authorities** and their websites are located on the European Commission site at http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080.