Is Your Security Network Ready for GDPR?

Probably Not – and the Cost Will Surprise You.

As you're finalizing the budget for your next fiscal year, you may want to include a line for millions of dollars that you may need to pay for fines related to a data breach. Thousands of organizations are at risk of facing such financial penalties today and they have no idea the rules even apply to them. And that doesn't even touch on the lawsuits and sanctions that may also ensue as a result of a data breach.

To avoid costly oversights to your data security protocols, proactively protect your company from these threats. Not only will you prevent breaches, you will maintain customer trust, limit your liability, and potentially save millions in fines and lost productivity.

Johnson Controls

What is GDPR and what does it mean to my company?

The General Data Protection Regulation (GDPR) is a new European Union (EU) law that went into effect on May 25, 2018 to give consumers more control of their personal data collected by companies. While GDPR applies to the personal data of people from the European Economic Area (the EU plus Iceland, Lichtenstein and Norway), **in reality, it pertains to data anywhere in the world.**

PII PERSONALLY IDENTIFIABLE INFORMATION

GDPR governs how personally Identifiable information (PII) is managed and covers any system that is collecting PII. These data protection standards pertain to any information that can, directly or indirectly, identify a living person (e.g. a name, email address, ID number, geolocation information, or picture).

Small to large organizations face new data security regulations

Even if your business operates wholly in another country or region, the way you manage personally identifiable information may be subject to GDPR.

Could you fully disclose a data breach within three days?

Equifax waited six weeks. It took LinkedIn and Yahoo **years** to reveal to consumers that data was stolen.

Under GDPR, an organization now has only 72-hours after becoming aware of the data breach to fully disclose when personal data has been stolen. The organization must provide the supervisory authority with information about the nature of the breach, its extent and likely effects, and its response and mitigation efforts.

Failure to comply with the new GDPR regulations may come with a heavy fine – up to 4% of a business' annual revenue for the prior year or $20M, whichever is greater.

Johnson Controls

Are you vulnerable?

Most companies don't realize how their data is being collected and used within their organization, let alone know that they may be breaking the law.

Is your security system an enormous liability?

Every day situations may now be considered non-compliant. Do any of these scenarios sound familiar?

Scenario One:

Your security system captures personal information and you want to know how it is being used throughout the business.

Your Solution:

Video and access control systems like badge readers and biometric devices collect personal data. You initiate a data compliance audit to understand the current state of data usage within the organization, which is then used to implement a data governance program that documents and tracks how that personal data is being used across the security equipment network.

Scenario Two:

You want to help key stakeholders by providing them with better analytics and visuals with improved security system dashboards.

Your Solution:

You propose to install an ongoing data management monitoring platform that would assess compliance to governance processes in real-time. It is eliminated from the budget. Your current system provides a snapshot of the past – it seems like a waste to invest money just to have the information a little sooner when you have to hit short-term revenue targets.

Scenario Three:

Your building's access control system for your global company has been tracking a service representative's activities for three years. The representative requests his profile data so he can share his performance metrics with a potential employer.

Your Solution:

Per your organization's policy, you purge access control system information every year. You apologize to the service representative and offer to provide them with the information you still have on file for the year.

Scenario Four:

Several former employees request that you redact all of their information from the security network.

Your Solution:

You are able to delete their access control data, but you are not able to remove video captures because you don't have a way to identify people based on facial recognition. You do not notify them of the issue nor do you form a plan to correct the situation. A few months later, a crime is committed just outside your main entrance so you have it on video, but can't identify the perpetrator for authorities. Since the victim was not one of your employees, you assume that your liability is low.

If these scenarios cause you concern, keep reading - because your liability may be much greater than you imagine.

Johnson Controls

Do you have the following business rules in place to limit your liability?

- Retention periods that follow all applicable laws/regulations
- A data governance program that can identify and stop a data breach prior to the retention expiry period
- The ability to trace data processing activities throughout the data chain
- Software and processes that will IMMEDIATELY stop unintentional data leaks and monitor for nefarious cyber-theft of data
- A holistic program that both changes behaviors regarding acceptable data usage AND places safeguards for stopping leaks

Are your video and access control systems vulnerable to hackers and GDPR fines?

Security networks can host thousands of IP devices such as video cameras, NVRs, PoE switches, UPS, access control systems, emergency phones, HVAC systems, and any building Internet of Things (IoT) devices. Since video and access control platforms capture PII data, they are under the authority of GDPR data protection and rightly so. Hackers target these devices and exploit device IP connections in order to gain access to deeper networks and databases where PII is stored.

A video or access control swipe may now cost millions of dollars in lost revenue

Security system stakeholders assume that GDPR regulation pertains to credit card information. They will be surprised to learn that the information accumulating on security systems also puts them at risk.

Cyber thieves are using more sophisticated techniques to access your data. Make sure your cyber doors are locked. Take steps today to identify your risks.

Johnson Controls

How much is your identity worth?

GDPR regulations were implemented due to the growing number of data breaches that organizations have experienced and the vulnerability and financial hardship people face when their PII is stolen. Sadly, this is a growing problem as hackers are becoming more adept at finding ways to circumvent data protection measures.

Cyber thieves use an arsenal of common tactics that are highly effective, such as malware, ransomware, phishing, DoS attacks, man-in-the-middle attacks, or cross-site scripting (XSS). Cyber breaches tend to exploit network and human security weaknesses. Thieves might implement a bot-net bombardment approach like DoS or credential reuse whereby they go for quantity over quality. Or, thieves may use a slow and patient approach, waiting for the opportune time when the victim makes a mistake like accidentally clicking on a phishing link and unknowingly providing credentials. Once cyber thieves infiltrate the outer layer of the network, they can work their way to exploitable data, which could take up-to a year or longer to accomplish.

The hackers often sell the PII data on the black market (also known as dark web marketplaces) where it can be used to steal victims' identities and money. The payout can be lucrative:

CREDIT CARD NO. W/ CARD VERIFICATION VALUE (CVV2)	US	UK	CANADA	AUSTRALIA	EU
Random	$5–$8.00	$20–$25.00	$20–$25.00	$21–$25.00	$25–$30.00
With bank ID number	$15.00	$25.00	$25.00	$25.00	$30.00
With date of birth	$15.00	$30.00	$30.00	$30.00	$45.00
With complete info (Full name, billing address, payment card no., expiration date, PIN No., social security no., mother's maiden name, date of birth, and CVV2)	$30.00	$35.00	$40.00	$40.00	$45.00

Source: McAfee Labs

OTHER INFORMATION	UNITED STATES	
Bank account w/ $2,000 balance	$200.00	(about 10% of account value)
Denial-of-service (DoS) attacks	$10.00	per hour
Email accounts (e.g. Gmail/Yahoo)	$.70 - $1.20	
Amazon account	$.70 - $6.00	(depending on balance and country)
Uber, Netflix account	$1 - $2.00	
Social Security No.	$1.00	
Healthcare ransomware	$20,000.00	average
Healthcare individual	$18,000.00	healthcare insurance fraud average

Source: CSID (an Experian Company)

Personal data is almost a new form of currency in the digital world. Protecting that data is becoming more and more difficult as more hackers are entering the black market workforce.

Johnson Controls

How do you ensure that your security network is GDPR compliant?

1

Review your business rules around the following:

- ☐ User transparency
- ☐ Video retention period
- ☐ Right to consent
- ☐ Right to data portability
- ☐ Data redaction
- ☐ Incident response time

2

Assess your level of GDPR compliance compared to your business rules.

3

Update your business processes to mitigate your risk and ensure ongoing GDPR compliance.

Johnson Controls