white paper

S2 SECURITY

Meeting GDPR requirements in your S2 Security environment

May 2018

What is GDPR?

The European Union's General Data Protection Regulation (GDPR) takes effect May 25, 2018 and applies to all businesses that handle EU citizens' personal data, which encompasses a broad range of data that may include the individual's name, address, email address, telephone number, along with any other data that identifies the individual. This white paper provides general guidelines to customers who have deployed S2 Security solutions in the EU. This paper is for informational purposes only. It is not legal advice and should not be relied upon as legal advice.

The regulation defines the rights of the Data Subject, and the responsibilities of the Data Controller and the Data Processor. The heaviest compliance burden falls to the Data Controller, the entity that decides which personal data to collect and has the ultimate responsibility for safeguarding it.

GDPR roles and responsibilities

- **Data Subject** owns his or her personal data and whose consent is needed to gather and store such data. The Data Subject has the right to know what personal data is currently stored by the Data Controller. The Data Subject also has the "right to be forgotten" by the Data Controller.
- **Data Controller** is the entity requesting collection of and access to the Data Subject's personal data. The Data Controller's responsibilities include safeguarding the Data Subject's personal data, notifying the Data Subject in the event of a data breach, and deleting personal data if there is no legal justification for keeping it upon the Data Subject's request to be forgotten. A company deploying S2 Security products on-premises typically is the legally responsible Data Controller.
- **Data Processor** is a third party who may be engaged by the Data Controller to process and manage the Data Subject's personal data. The Data Processor is responsible for safeguarding the Data Subject's personal data. In the event of a data breach, the Data Processor is responsible for notifying the Data Controller of the breach. The Data Controller is then responsible for alerting the Data Subjects whose personal data has been accessed. The Data Processor is not responsible for contacting the Data Subject directly in the event of a breach, only to inform the Data Controller.

It should be noted here that on-premises deployments of access monitoring and video management systems often do not involve a Data Processor because the Data Controller handles all personal data.

GDPR and your S2 Security on-premises infrastructure

It is important to understand that there is no such thing as GDPR-compliant hardware or software. Your infrastructure can assist in compliance, but it cannot ensure compliance. It is not possible to simply install hardware or software and instantly be in compliance with the regulation. Compliance requires the proper handling of personal data. We will describe best practices in three areas where GDPR regulations and physical security practices intersect.

- The Data Subject's **right to be forgotten**
- The **right to know what personal data is being gathered and stored** about the Data Subject
- The **responsibility to inform** the Data Subject **in the case of a data breach**

Applying these principles to all handling of personal data make compliance easier and minimize concerns by employees, customers, and guests regarding your data policies.

- Gather and store the **minimum personal data needed for business operations**.
- Be **proactive in explaining the data collected** and why it's necessary. Doing this fulfills the Data Controller's responsibility to share with the Data Subject the personal data that is gathered and stored.
- **Share** your data **retention policies** when asking for consent to gather personal data. You can then refer to those policies in the future should the Data Subject ask what personal data has been gathered.
- Set the **shortest retention policies** that work for your business.

Informing of a breach

In the case of a data breach that compromises the Data Subject's personal data, the Data Controller has the responsibility of alerting the subject within 72 hours of discovery of the breach. The Data Processor has the same responsibility to inform the contracting Data Controller entity of a breach, thus starting the Data Controller's 72-hour clock.

Access control best practices

After gaining the employee's consent, only place the minimum necessary personal data in the S2 Security access control database – specifically, only the information needed to verify identity and access level. This best practice is particularly important when there is an integration between enterprise HR system employee database(s) and the S2 Security access control database.

When employees leave the company, it is typical to delete their records from the S2 NetBox partition(s) they have been assigned. S2 Security recommends that customers establish a standard operating procedure to purge aging S2 NetBox and S2 Global archives in a timely manner.

Video management best practices

Identifying an individual's appearance in a video clip is a cumbersome and manual process. In most situations and installations, it's nearly impossible to be certain an individual appears (or doesn't appear) in a video file. The best policy to assure compliance is to set a retention policy for video of no longer than a few days. Unless you have the reasonable expectation of needing a video clip for legal purposes, it should be purged as quickly as possible.

A note on S2 Magic Monitor Forensics
S2 Security customers should be aware that S2 Magic Monitor Forensics users have the ability to publish personal data through its video export features. It is imperative to establish procedures and train system users on the proper handling of personal data in your organization.

S2 mobile and cloud solutions

It is important to note that when a customer contracts with S2 Security as a Data Processor for S2 NetBox Online, our mobile applications, and other cloud services, the customer retains the role and responsibilities of the Data Controller.

A note for customers deploying the S2 Mobile Security Professional mobile solution
Users of the S2 Mobile Security Professional application have access to your employees' personal data that you elect to store in S2 NetBox. It is imperative to rescind access to all of your S2 Security deployed applications including S2 Mobile Security Professional immediately upon a security professional's exit from the organization.

Concluding comments

Following some simple rules regarding personal data can prevent future issues. Gather the least amount of personal data you need for business operations. Retain that information for the shortest period of time necessary. And, perhaps most importantly, be transparent about your personal data practices.

References

Full text of the GDPR, April 6, 2016

GDPR FAQs, EU GDPR Portal, 2016

GDPR Best Practices, Dun & Bradstreet, 2017

There Is No Such Thing as GDPR-Compliant Software or SaaS Solution, Martin Kuppinger, June 30, 2017

How Physical Access Systems will be affected by GDPR, IFSEC 2017

Amazon Web Services EU Data Protection, December 2016

Video surveillance and the GDPR. What will change? Axis Communications, February 27, 2018

European Data Protection Supervisor Video Surveillance Guidelines, March 17, 2010

Regulation (EC) No 45/2001 of the European Parliament and Council, December 18, 2000