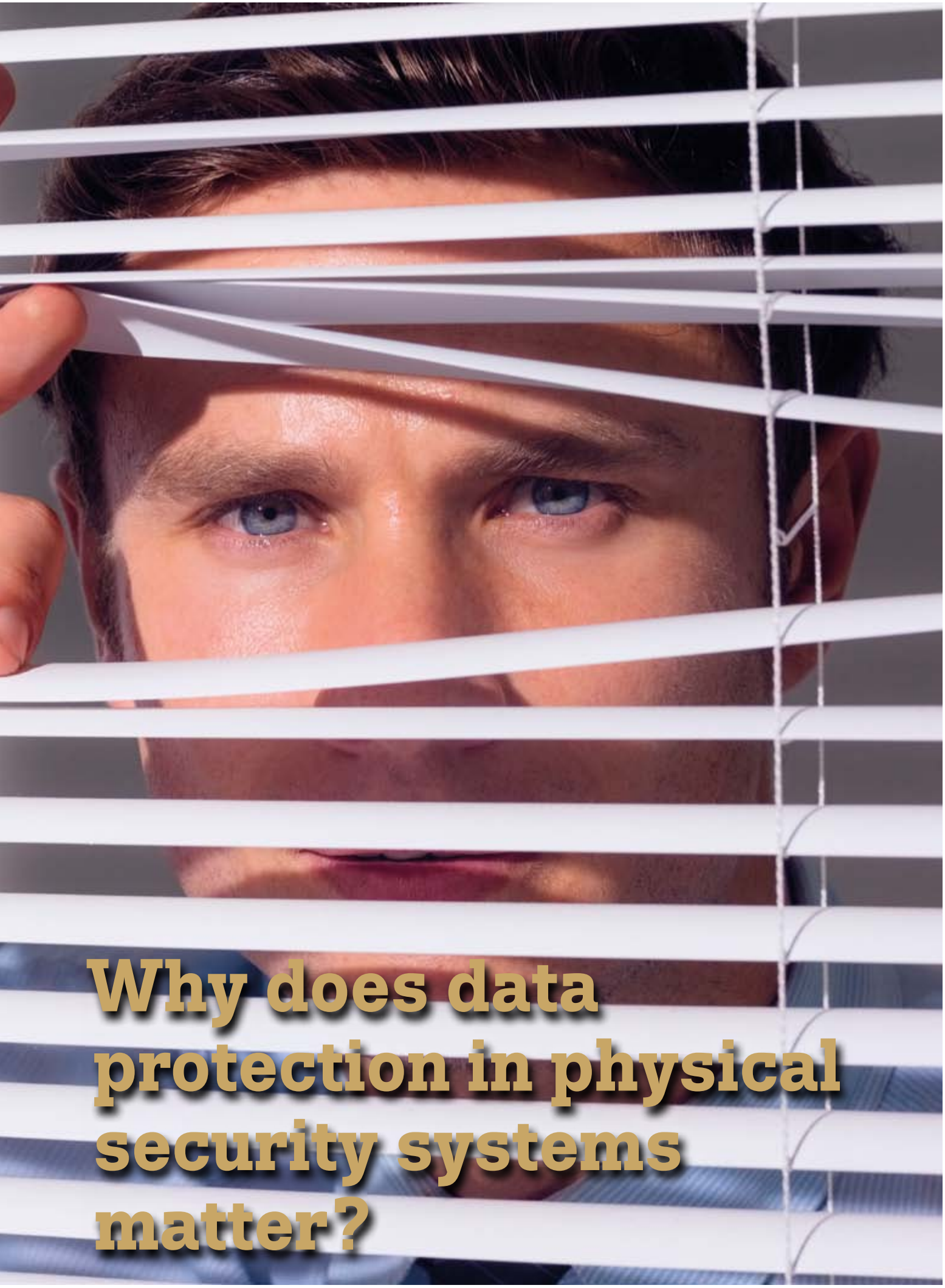

Why does data protection in physical security systems matter?

In the digital world, people own personal information just like they own physical assets such as cash, keys and clothes in the real world. But because personal information is intangible, its value has been overlooked by many for a very long time. With the increase in cyber crimes on personal data and the infamous Snowden affair, this issue has become more prominent. To improve the transparency of data collection and processing, and to give people control over their personal data, the European Commission has proposed a new regulation for data protection (General Data Protection Regulation 2012/0011(COD) (GDPR)) and brought the issue to a new level.

by Fei Liu

GDPR has defined four roles in order to safeguard the rights: Data Protection Authority (DPA), data controller, data protection officer (DPO) and data processor, as shown in Figure 1. DPA is the supervisory authority from member states, which monitors the application of the regulation and contributes to its consistent application throughout the Union. The data controller, DPO and data processor are active at a company level, performing various data protection tasks.

As with most other industries, physical security systems will be influenced significantly by this new regulation. They generally collect, record and process large amounts of personal data, some of which may be very critical and sensitive. For example, a physical security system often records very personal information about a cardholder, such as their name, social security number, employee number and so on. It may also store a PIN code, fingerprints and video footage of the cardholder. If someone else were to use this person's identity and authentication information, they could access restricted areas that they're unauthorised to enter.

Security systems also record cardholders' access events. So, by studying these events, you can easily trace someone's behavior pattern. Currently, cardholders are often unaware of the personal data captured in a security system – for example how long it will be stored for, whether it has been stored safely, where the data has been distributed to and whether it has been processed for other uses.

All above-mentioned doubts can make a cardholder feel insecure about a security system. Currently, security systems are most often viewed as protecting a building's security, while the protection of cardholders' personal data is often neglected and can be easily violated. A system administrator, for example, usually has the right to view logged events from all cardholders on the request of a criminal investigation. Such a right can be abused, however, by browsing the information with other purposes or even just for fun. This is a very typical case of data breach. The security of buildings and cardholder information are both very important, and should be protected. One shouldn't conflict with the other; a well-designed system should be able to achieve a win-win situation for both.

According to GDPR Article 10a(2), GDPR empowers people (data subjects) with the right to control their personal data. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of his or her personal data, the right of access, rectification and erasure of their data, the right to obtain data, the right of object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.

Nedap Security Management
Fei Liu
Research & Development

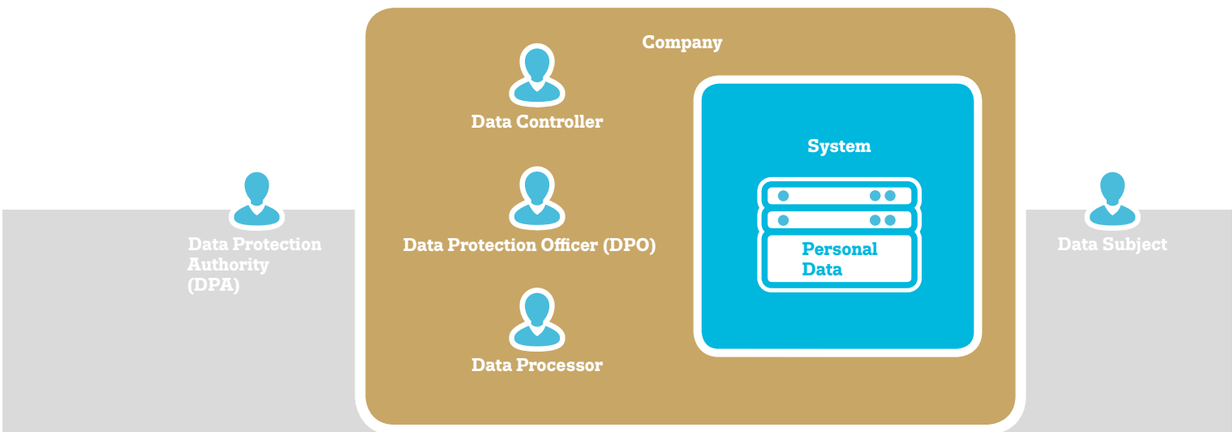

Figure 1 Various functions for data protection in GDPR

What can we do to secure security systems?

There must certainly be an increased focus on information security to improve data protection in physical security systems. Data protection should be an integral part of PIAM (physical identity and access management) and PSIM (physical security information management), and GDPR has provided a nice guideline. In general, a well-designed physical security system should:

- Include data protection and data security in the design phase. This means applying various technologies to perform database security, identity and access management, network connection security, secure data processing and link authentication.
- Ensure data subjects' rights. It should provide full functionality to enable data subjects (for example cardholders) to access, obtain, edit and erase their data.
- Assist data controllers and DPOs in performing their tasks. In particular, the system should be able to:
  - Provide a platform to manage and act on requests from data subjects and the supervisory authority.
  - Help data controllers and DPOs to define security policies and monitor data processing.
  - Monitor and report on data protection breaches, and perform specific tasks under the direction of data controllers and DPOs.

Anyone installing a physical security system should consider the following aspects regarding data when they deploy the system.

- The categories and retention time of personal data held in the system, and the reasons for collecting and processing this data.
- What defines a data breach in the system.
- The relationship between data held and relevant laws and regulations.
- The relationship between data held and services provided.
- How access and identity management can protect personal data in the system.
- Establishing varying levels of access rights to the data in the system.

On 12 March 2014, GDPR passed the EU plenary vote with the vast majority in favour. The European Commission will start adopting GDPR at the end of 2014 and is expected to enforce it in 2016.