Data Protection in Physical Security Systems*

Why does data protection 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 cybercrimes on personal data and the high profile data breaches, 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 Parliament has approved the new regulation for data protection (General Data Protection Regulation (GDPR) Regulation (EU) 2016/679) and brought the issue to a new level.

GDPR empowers people (data subjects) with the right to control their personal data. Chapter III of the regulation, for example, lists the rights of data subjects such as the right of access, rectification and erasure of their data.

version 1.0, 2018

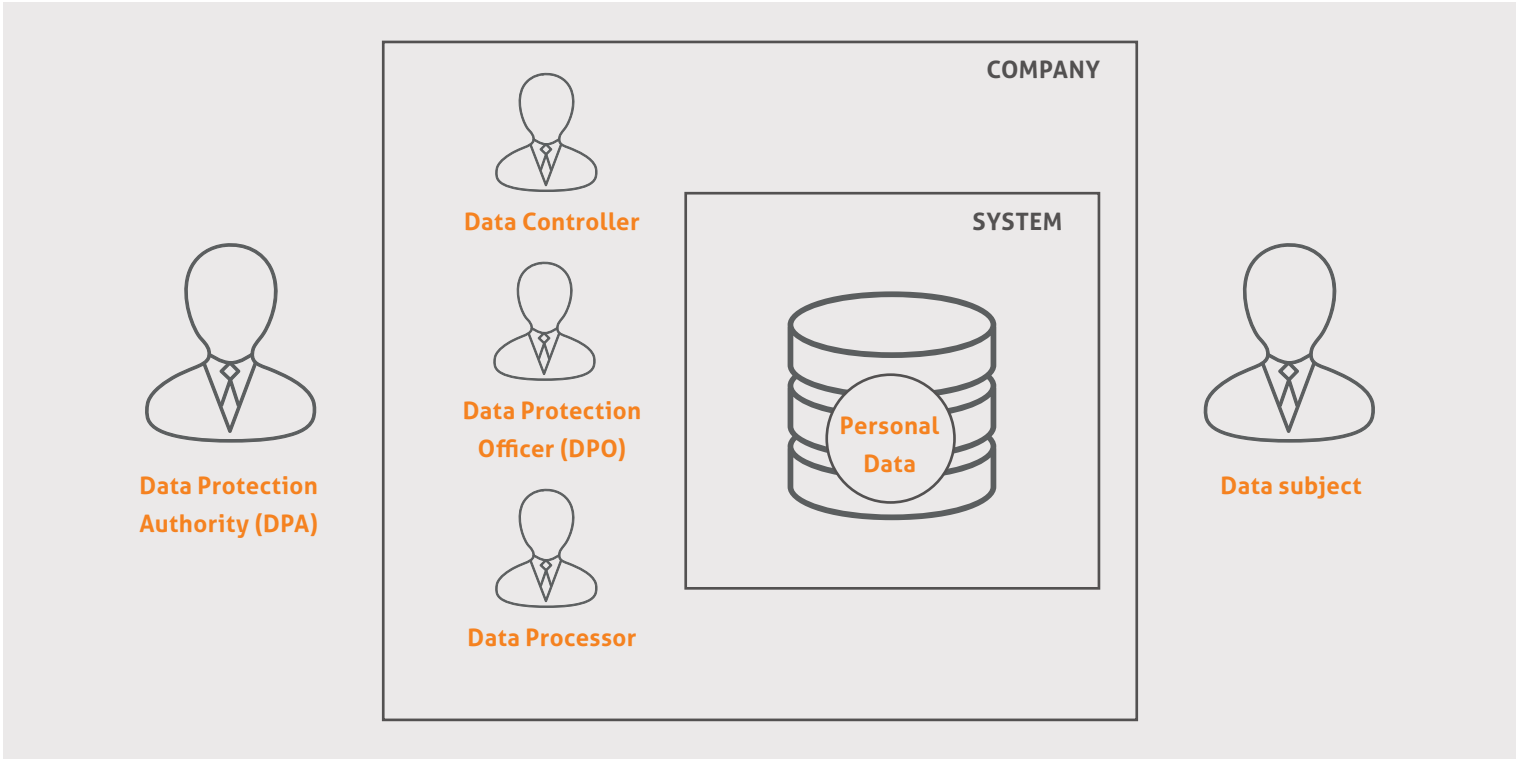

Figure 1 Various data protection functions, as defined by GDPR.

To safeguard these rights, GDPR has defined four roles: 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 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, 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 are unauthorised to enter.

Security systems also record cardholders' access events. So, by studying these events, you can easily trace someone's behaviour 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 these 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 overlooked 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 for 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.

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 an excellent 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 it addresses the requirements concerning the processing of personal data and offers the possibility to access, rectify and erase such 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 deploying the system.

- The categories and retention time of personal data held in the system, and the reasons for collecting and processing this data.
- 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.
- Conducting a Data Protection Impact Assessment (DPIA) to determine any possible risks in processing personal data that may require mitigating measures.

Data protection in AEOS

Whereas AEOS is concerned, it can support end-users, i.e. data controllers and data processors, in complying with the GDPR in that it addresses the requirements concerning the processing of personal data. It offers the possibility of, amongst others, accessing, rectifying and erasing such data and access to the system and the data in it is role based.

All user actions and changes in AEOS are logged, providing an audit trail for the data controller.

Carrier (employee, visitor, contractor, vehicles) records can be changed and can be erased after a certain amount of time. Unless purposely configured otherwise, AEOS controllers contain no personal data but only reference numbers of those carriers who have access to the door(s) connected to that controller. This data is refreshed at least once a day or, for example, right after a carrier record is changed. So if an access badge is withdrawn, the data on the AEOS controller is erased.

Although most end-users enter personal data of their employees, contractors and visitors into their access control system, AEOS can also be configured in such a way that no personal data is entered at all. A number, for example a personnel number as listed in a HRM system, would suffice to create a carrier record and assign identifiers to grant the carrier access to the end-users premises.

AEOS can be configured in many different ways, offers multiple free fields and can be connected to third party systems. End-users may therefore find it useful to take the following into consideration when determining what kind of personal data they wish to enter into their access control system and where to store this data;

- **Purpose:** Data is used for identifying carriers in order to grant or deny access to the end-users premises.
- **Data:** End-users determine what kind of data is to be processed in AEOS and who has access to that data.
- **Method:** Data can be entered into AEOS manually or can be imported from a third party system, for example the end-users HRM system. The method of data collection is subject to the end-users company policy.
- **Storage:** Data is stored in the AEOS database on premise. When determining the location of the servers on which AEOS and the database are installed, end-users may need to consider additional, local, regulations.
- **Third party:** Personal data of carriers can be shared by or with third party systems connected to AEOS. Which data is shared, and how, depends on the third party system. Details on how data is shared can be found in the AEOS manuals.
- **Retention:** Data in AEOS is stored until erased. This can be done manually or automatically, depending on the system's configuration.

1. General Data Protection Regulation (GDPR) was approved by the EU Parliament in April 2016. Regulation (EU) 2016/679 came into force on May 24th 2016 and will apply from May 25th 2018.
2. Additional local legislation may apply.

For questions concerning AEOS
in relation to GDPR please contact us:
www.nedapsecurity.com
privacy@nedapsecurity.com