June 17th, 2024

Axon Portfolio and Data Privacy

As a Carrier company, Aritech recognizes the importance of data privacy laws. Carrier has implemented privacy-related governance and policy on a global level to enhance compliance.

Data Privacy Laws

National and regional governments around the world are increasing legislation for data privacy compliance, introducing new and more stringent laws concerning the use and retention of Personal Data. Personal Data is any information relating to an identified or identifiable natural person, who can be connected, directly or indirectly, to the data, in particular by reference to an ID number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social specification. Many data privacy laws contain extended jurisdiction, meaning that they apply to entities established outside of the region but doing business in or also focusing on data subjects established in that region. Carrier recognizes the importance of these data privacy laws and has implemented, on a global level, an internal privacy-related governance scheme and privacy policy.

Carrier also obtained BCR's (Binding Corporate Rules) in the EU, that are considered as the golden standard regarding data protection (Approved Binding Corporate Rules | European Data Protection Board (europa.eu)) and are published here: link. Furthermore, Carrier has a global Data Privacy Team.

How does this affect the Axon portfolio?

Axon, developed by Carrier Corporation (doing business as "Aritech"), consists of a range of products & solutions that provide security for properties by installing intrusion detection and access control functionalities. Axon and the derivative products include hardware, such as the security control panels, expanders, keypads and readers and software applications to configure and manage solutions.

Axon uses the Advisor Management software as the interface to manage and control security installations on-site or remotely. The use of Personal Data is central to an end-user's security control system to manage the movements and access to requested functions of their employees and visitors. The only data fields that are mandatory in Advisor Management are a name and - if required - a credential (Badge number, PIN) used for the purpose of linking a credential to a person and setting permissions for where and when the user can gain access to the requested function or access.

The installation company who will install the Axon security solution, works with the end-user to define what Personal Data elements are entered as part of the installation and commissioning process. Because Aritech does not install or commission the Axon solution, the installer and end-user are responsible for determining that the collection and use of Personal Data is consistent in order to be data privacy compliant.

The unique credential identification (ID) and associated access rights are available by security control panel for instant decision making. The presentation of a credential ID (pin code or card) at a reader is matched to the registered credential ID in the system and access to requested functions or doors/lifts is granted or denied depending on the security rules configured by the installer of the system at the end-user's premises.

Examples of fields that can be configured to optimize security management in Advisor Management are internal and external numbers (often used to gather internal HR numbers or internal ID numbers), e-mail address, gender, photograph and access levels. This data may be populated from an HR database through a secured exchange of data at regular intervals. Access to the data fields and the ability to add or modify it are based upon end-users' decisions and controlled by permissions configurable by the end-user.

The security control panels store details as events in the event history logs. Event history log entries contain events description with the time and date of the occurrence. The end-user may also configure the logs to contain additional information to identify the person involved and the location of the event. A person's name may also be sent to an alarm central station to be able to identify who is involved in an event and start the proper action. For intrusion alarms, the storage of events and alarm reporting is in line with security approvals such as EN50131.

- **Identify** Make sure you know where Personal Data is kept.
- **Comply** Manage processing, access to and deletion of Personal Data and comply with Data Subject requests.

- **Protect** Establish security procedures to protect Personal Data.
- **Record** Keep a record of your procedures.
- **Monitor** Prevent data breaches and report them.

Privacy by Design

Carrier adheres to “Privacy by Design” principles, which are now a legal requirement under many data privacy laws. At its core, Privacy by Design calls for the inclusion of data protection as an integral part of the design of systems.

While the end-user is ultimately responsible for entering, processing and managing Personal Data in Axon products, Aritech helps supports the end-user in data privacy compliance by incorporating privacy requirements in the product design. Aritech is committed to Privacy by Design.

Our products are designed to support the end-user as the end-user determines what Personal Data to input into the system. Aritech products offer varying levels of security to protect the Personal Data of individuals having access to the end-users’ premises. Respected industry standards and ISO-compliant encryption methods can be configured or installed in the system such as DESFire EV1 between card and reader, encryption between controller and server, and HTTPS for a secure connection between the server of the Advisor Management application and the end-users. Moreover, the application supports comprehensive system restrictions to limit access to only those that have been authorized.

In addition to the product design, the installer can provide assistance to the end-user in determining how to deal with mandatory fields and optional fields in our products. The installer can provide additional information on which data and logs it can see and what back-ups are created during installation, commissioning and product maintenance.

Assist with Data Privacy tasks

Advisor Management offers the ability to an end-user’s security administrators to define permissions to ensure individuals have access rights to those functions and data in the application required to perform their tasks as well as to define what type of access is appropriate.

Axon security control panels are accessible only to privileged individuals (installers, etc.), who have access only to functions and configuration details based on the permission assigned to them by the end-user.

Advisor Management can be used to configure the access, intrusion control and alarm monitoring environments, including end user access permissions. It provides password enforcement and can support single sign-on. System access can be restricted and limited to an individual’s functional responsibility by segmenting hardware, location, application and function, as well as reading and editing rights.

Any event detected by a sensor is sent to the security control panel and then transmitted to a connected security management application, such as Advisor Management or to configuration and diagnostic tools for record keeping and diagnostics. Additional Personal Data may also be sent to an alarm monitoring center to follow-up on alarms, depending on the configuration set-up decided by the end-user.

For each event related to access through doors or intrusion areas, the event description and associated details are captured and retained first in the hardware in accordance with security regulatory requirements and, when connected to the Advisor Management application, these events are also transmitted and stored in the application. This enables and allows for later verification of events by authorized personnel - if and as required - and for as long as necessary. Data retention is determined by the end-user; Axon products do not provide a default deletion period but allow the end-user to define it.

Empower people with the right to control their data

Advisor Management provides a number of fields storing personal data for the purpose of identifying the assignment of access rights and monitoring the proper use of PIN codes, access cards, license plates or equivalent credential types. These are controlled by the operators of the Advisor Management application.

The Advisor management application stores user related details in logs for the purpose of auditing proper use of access right in the application as physical access through security elements like doors, lifts or intrusion areas. Advisor Management offers options to limit the storage period and provide report on the stored Personal Data of any person or visualize which operators handle Personal Data.

The Axon control panels also create logs as required by regulations as well as for audit purposes. The Axon control panels provide means to anonymize the personal data after a configurable time period as log entries are not allowed to be deleted.

About Aritech

Aritech provides leading security and life-safety solutions for commercial applications covering intrusion, video, transmission and access. Offering some of the most trusted product names in the industry, and backed by ongoing partner services and support, Aritech helps customers secure and protect what matters most. Aritech is a part of Carrier Global Corporation, a leading global provider of healthy, safe and sustainable building and cold chain solutions. For more information, visit aritech.com or follow us on LinkedIn @Aritech.