General Data
Protection Regulation

Aritech Advisor Advanced products and Data Privacy

GDPR

The General Data Protection Regulation (“GDPR”), effective since May 25, 2018, provides rules to protect Personal Data.

One of the more significant changes to the EU’s regulatory landscape for data privacy comes with the extended jurisdiction of the GDPR, as it applies to all entities established in the EU, whether the processing itself takes place within the EU or not, and to entities processing the Personal Data of Data Subjects residing in the EU, by entities not located in the EU.

Carrier Corporation recognizes the importance of the GDPR and has implemented, on a global level, a privacy compliance program, which include our privacy policy, as well as our internal privacy-related governance scheme.

How does this affect Advisor Advanced products?

Advisor Advanced, developed by Carrier Corporation, (doing business as “Aritech”), consists of a range of products that provide security for properties by installing intrusion detection and access control functionalities. Our products include hardware, such as the security control panels, expanders, keypads and readers and software applications to configure and manage solutions. Personal Data is required for the different systems to function. The installer works with you as the Customer and 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 Advisor Advanced products, the installer and end-user are responsible for determining that the collection and use of Personal Data is consistent with GDPR requirements.

While the end-user is ultimately responsible for entering, processing and managing Personal Data in Advisor Advanced 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.

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.

GDPR effective at 25 May 2018

General Data
Protection Regulation

Aritech Advisor Advanced products and Data Privacy

Cyber Security

Aritech is committed to the cyber security of its Advisor Advanced products and services and protecting Personal Data. Aritech is continuously working to improve its products with these goals in mind. To support this, Carrier Corporation (Carrier), Aritech's parent company, has a dedicated Product Security Officer.

Advisor Advanced products permit the end-user to store Personal Data in the product. The unique credential identification (ID) and associated access rights are available by security control panels 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.

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.

Examples of fields that can be configured to optimize security management in Advisor Management are: internal and external number (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 a 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 an event description containing: the time and date of 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.

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.

Advisor 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 and intrusion control and alarm monitoring environments, including 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 functions, 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; Advisor Advanced products do not provide a default deletion period but allow the end-user to define it.

Personal Data is any information relating to an identified or identifiable natural person (called a "data subject" in GDPR); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

About Aritech

Aritech provides leading security and life-safety solutions for both commercial and residential 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.

GDPR effective at 25 May 2018

Ref. 1821 GDPR Advisor Advanced – EN-EU – 0324