General
Data
Protection
Regulation

May 25, 2018

OnGuard®

Lenel OnGuard and data privacy

GDPR

The General Data Protection Regulation ("GDPR"), which becomes effective on May 25, 2018, provides rules to protect Personal Data. Personal Data is any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. More information about the GDPR is available at: **http://www.eugdpr.org/the-regulation.htm**

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.

United Technologies Corporation recognizes the importance of the GDPR and has implemented, on a global level, Binding Corporate Rules ("BCR's"), which include our privacy policy, as well as our internal privacy-related governance scheme. BCR's are considered as the golden standard regarding data protection. Our BCR's are publicly available in multiple languages (**http://www.utc.com/Pages/Privacy.aspx**).

How does this affect Lenel OnGuard?

The prime responsibility for entering, processing and managing Personal Data into a security system lies with the entity protecting their people, buildings and assets. However, UTC Fire & Security Americas Corporation, Inc. ("Lenel") enables compliance with data privacy requirements. Personal Data is inherently required for the system to function, but this can only be entered into the system as part of the installation and commissioning process. In other words, as the manufacturer of the security system, UTC does not determine what Personal Data Is input into the system; those decisions are made by the customer.

Lenel has designed its products to allow customers to use them in GDPR-compliant ways. Lenel OnGuard offers varying levels of security to protect the Personal Data of employees and visitors. Respected industry standards and ISO-compliant encryption methods can be configured in the Lenel OnGuard system such as DESFire between card and reader, OSDP between reader and controller, TLS1.2 between controller and server, and HTTPS for a secure browsing experience. Moreover, Lenel OnGuard supports comprehensive system restrictions to limit access to authorised personnel and supports the application of limited data fields, to that which is minimally required for the system to function.

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.

LENEL
United Technologies

General Data Protection Regulation

May 25, 2018

Ref. 1543 EN – 0426

Privacy by Design and Cyber Security

Lenel adheres to “Privacy by Design” principles which are now a legal requirement under the GDPR. At its core, Privacy by Design calls for the inclusion of data protection as an integral part of the design of systems. Our company’s product emphasises data privacy and cyber security compliance.

Lenel is committed to the cyber security of its products and services and protecting data privacy and is continually working to improve its products with those goals in mind. To support this, United Technologies Corporation (UTC), the parent company of Lenel, has a dedicated Cyber Security Group and a global Privacy team.

Whereas Personal Data is stored in the Lenel OnGuard database, the unique credential identification (ID) and associated access rights are distributed down to system-controllers 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 is granted or denied depending on the Lenel OnGuard contained security rules. If biometrics are used for identity purposes, then these are encrypted and stored securely as an algorithmic array of minutiae points, on a card, in a reader, in the controller and/or in the database.

The use of Personal Data is central to an entity’s access control system to manage the movements of their employees and visitors. The only data fields that are mandatory in Lenel OnGuard are Name and Badge ID used for the purpose of linking a credential to a person and setting permissions for where and when the cardholder can gain access. Examples of fields that can be configured to optimise security management are: Location, Department, Function, Photograph and Access Rights. Such data, restricted by the use in security, may be populated from a HR database through a secured exchange of data. Fields in user forms are freely configurable allowing much flexibility for the application, but the use thereof will need to comply with the corporate security policy of the entity.

Assist with Data Privacy tasks

Lenel OnGuard can be administered to configure the access control and alarm monitoring environments, including user access permissions. Lenel OnGuard provides password enforcement and can support single-sign-on for certain applications. System access can be restricted and limited to the user’s functional responsibility by segmenting hardware, location, application and functions, as well as reading and editing rights.

For each transaction, the badge ID (and associated name), time and location are captured and retained in the system for later verification by authorised personnel, if and as required, for as long as necessary. Data retention is determined in accordance with corporate security regulations; Lenel OnGuard does not provide a default deletion period but provide the possibility to define it. Appropriate permissions are required to delete data. Other use of Personal Data includes providing the entity with an individual’s last known location.

As well as utilising standard reporting capabilities, Security Managers can also use the optional OnGuard WATCH (Web Access Trending and Comprehensive Health), which collects system data and displays it on customizable, user-friendly dashboards. Or Security Managers can use OnGuard Policies to ensure Lenel OnGuard is correctly configured according to corporate security policies.

Empower people with the right to control their data

The optional OnGuard Credential Self Service allows the individual to change their pin-code, request visitor access and view which access rights they have. A full view of all card-holder data in Lenel OnGuard, including user definable fields (UDF), can be obtained from the web clients Credentials and OnGuard Access Manager. Through the web interface, these clients can provide every authorised administrator an overview in case of requests.

As part of its prime responsibility regarding data privacy, an entity must obtain the consent from visitors, such as contractors, suppliers and customers before processing their Personal Data. For the applications OnGuard Visitor Self Service and BlueDiamond Mobile, a consent button is included and, upon data entry, supporting document can be pre-loaded to aid the user’s understanding of their data usage, application and storage duration.