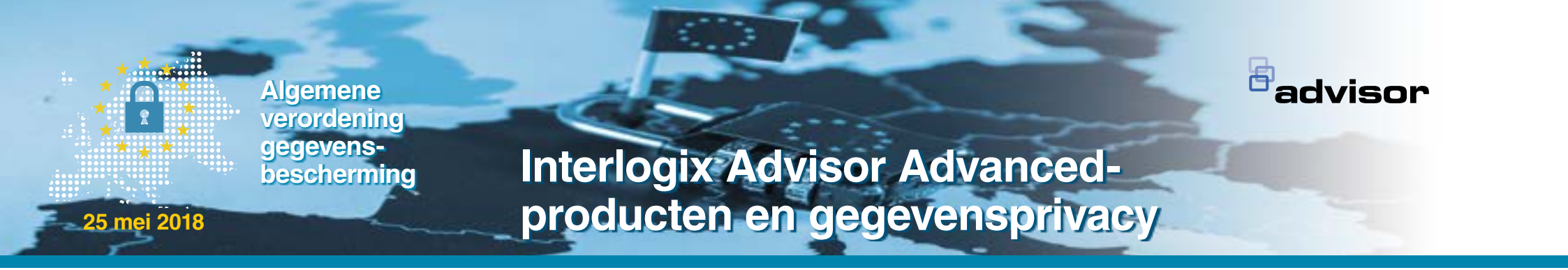

Algemene verordening gegevens-bescherming

25 mei 2018

Interlogix Advisor Advanced-producten en gegevensprivacy

advisor

AVG

De Algemene Verordening Gegevensbescherming (“AVG”), die op 25 mei 2018 van kracht werd, voorziet regels om persoonsgegevens te beschermen. Persoonsgegevens zijn alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon, die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatienummer of een of meer factoren die specifiek zijn voor zijn/haar fysieke, fysiologische, mentale, economische, culturele of sociale identiteit. Meer informatie over de AVG is beschikbaar op: **http://www.eugdpr.org**

De uitgebreide jurisdictie van de AVG is één van de belangrijkste wijzigingen in het Europese regelgevingslandschap voor gegevensprivacy, aangezien deze van toepassing is op alle in de EU gevestigde entiteiten, of de verwerking zelf plaatsvindt binnen de EU of niet, en op entiteiten die persoonsgegevens verwerken van betrokkenen die in de EU verblijven, door entiteiten die zelf niet in de EU zijn gevestigd.

United Technologies Corporation erkent het belang van de AVG en heeft wereldwijd Bindende bedrijfsregels (Binding Corporate Rules -”BCR’s”) geïmplementeerd, waaronder ons privacybeleid, evenals ons interne privacygerelateerde bestuursplan. BCR’s worden als de gouden standaard voor gegevensbescherming beschouwd. Onze BCR’s zijn openbaar beschikbaar in meerdere talen (**http://www.utc.com/Pages/Privacy.aspx**).

Welke invloed heeft dit op Advisor Advanced-producten?

Advisor Advanced, ontwikkeld door UTC Fire & Security Americas Corporation, Inc. (commercieel op de markt als “Interlogix”), bestaat uit een reeks producten die beveiliging bieden voor eigendommen door inbraakdetectie- en toegangscontrolefunctionaliteiten te installeren. Onze producten omvatten hardware, zoals beveiligingscontrolepanelen, uitbreidingen, keypads, lezers en softwaretoepassingen om oplossingen te configureren en te beheren. Persoonsgegevens zijn vereist voor de werking van de verschillende systemen. De installateur werkt samen met u als klant en eindgebruiker om te definiëren welke persoonsgegevensgerelateerde elementen worden ingevoerd als onderdeel van het installatie- en inbedrijfstellingsproces. Omdat Interlogix de Advisor Advanced-producten niet installeert of in gebruik neemt, zijn de installateur en de eindgebruiker verantwoordelijk voor het vaststellen of het verzamelen en gebruiken van persoonsgegevens al dan niet in overeenstemming is met de AVG-vereisten.

Hoewel de eindgebruiker uiteindelijk verantwoordelijk is voor het invoeren, verwerken en beheren van persoonsgegevens in de Advisor Advanced-producten, helpt Interlogix de eindgebruiker bij de naleving van gegevensprivacy door privacy-eisen op te nemen in het productontwerp. Interlogix hecht veel waarde aan ingebouwde privacy (Privacy by Design).

Onze producten zijn ontworpen om de eindgebruiker te ondersteunen, aangezien de eindgebruiker bepaalt welke persoonsgegevens in het systeem moeten worden ingevoerd. Interlogix-producten bieden verschillende niveaus van beveiliging om de persoonsgegevens van personen die toegang hebben tot de locaties van de eindgebruikers te beschermen. Gerespecteerde industriestandaarden en ISO-compatibele coderingsmethoden kunnen worden geconfigureerd of geïnstalleerd in het systeem, zoals DESFire EV1 tussen kaart en lezer en codering tussen controller en server en HTTPS voor een veilige verbinding tussen de server van de Advisor Management-app en de gebruikers. Bovendien ondersteunt de app uitgebreide systeembeperkingen om de toegang te beperken tot de personen die hiervoor toestemming hebben.

Naast het productontwerp, kan de installateur de eindgebruiker assisteren bij het bepalen hoe om te gaan met verplichte velden en optionele velden in onze producten. De installateur kan aanvullende informatie verstrekken over welke gegevens en logboeken het zichtbaar zijn en welke back-ups worden gemaakt tijdens installatie, inbedrijfstelling en productonderhoud.

Identificeren

Zorg dat u weet waar persoonsgegevens worden bewaard.

Voldoen

Beheer de verwerking, toegang tot en verwijdering van persoons-gegevens en voldoe aan de verzoeken van betrokkenen.

Beschermen

Implementeer veiligheidsprocedures om uw persoonsgegevens te beschermen.

Opslaan

Houd een register bij van uw procedures.

Monitor

Voorkom gegevensinbreuken en rapporteer ze.

interlogix
United Technologies

Algemene verordening gegevens-bescherming

Interlogix Advisor Advanced-producten en gegevensprivacy

Cyber Security

Interlogix is committed to the cyber security of its Advisor Advanced Products and services and protecting Personal Data. Interlogix is continuously working to improve its products with these goals in mind. To support this, United Technologies Corporation (UTC), Interlogix'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.

Ref. 1543 – Advisor NL – 1023