Regolamento generale sulla protezione dei dati

25 maggio 2018

Prodotti Interlogix Advisor Advanced e Privacy dei dati

advisor

GDPR

Il regolamento generale sulla protezione dei dati ("GDPR"), in vigore dal 25 maggio 2018, mira alla protezione dei dati personali. Per Dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile, che possa essere identificata, direttamente o indirettamente, facendo riferimento a un numero di identificazione o a uno o più fattori specifici della sua identità fisica, fisiologica, mentale, economica, culturale o sociale. Ulteriori informazioni sul GDPR sono disponibili alla pagina: **http://www.eugdpr.org**

Una delle modifiche più significative al panorama normativo dell'UE in materia di riservatezza dei dati è l'estesa giurisdizione del GDPR, in quanto si applica a tutte le entità stabilite nell'UE, indipendentemente dal fatto che il trattamento stesso avvenga all'interno dell'UE o meno, e alle entità che trattano i dati personali di Soggetti residenti nell'UE, mediante entità che non si trovano nell'UE.

United Technologies Corporation riconosce l'importanza del GDPR e ha implementato, a livello globale, le Binding Corporate Rules ("BCR", Regole aziendali vincolanti), che includono la nostra Informativa sulla privacy, nonché il nostro schema di governance interno relativo alla privacy. Le BCR sono considerate lo standard aureo per la protezione dei dati. Le nostre BCR sono disponibili pubblicamente in più lingue (**http://www.utc.com/Pages/Privacy.aspx**).

In che modo influisce sui Prodotti Advisor Advanced?

Advisor Advanced, sviluppata da UTC Fire & Security Americas Corporation, Inc. (che opera come "Interlogix"), è costituita da una gamma di prodotti che forniscono sicurezza per le proprietà installando funzionalità di rilevamento delle intrusioni e controllo degli accessi. I nostri prodotti includono hardware, come i pannelli di controllo di sicurezza, gli espansori, le tastiere e i lettori e le applicazioni software per configurare e gestire le soluzioni. I dati personali sono necessari affinché i diversi sistemi funzionino. L'Installatore collabora con il Cliente e l'Utente finale per definire quali elementi dei Dati personali vengono inseriti nell'ambito del processo di installazione e messa in servizio. Poiché Interlogix non installa né commissiona i Prodotti Advisor Advanced, l'Installatore e l'Utente finale sono responsabili della determinazione che la raccolta e l'utilizzo dei Dati personali siano coerenti con i requisiti del GDPR.

Sebbene l'Utente finale sia in definitiva responsabile dell'inserimento, del trattamento e della gestione dei Dati personali nei Prodotti Advisor Advanced, Interlogix supporta l'Utente finale nella conformità alla privacy dei dati integrando i requisiti di riservatezza nella progettazione del prodotto. Interlogix si impegna a rispettare la Privacy by Design.

I nostri prodotti sono progettati per supportare l'Utente finale in quanto l'Utente finale determina i Dati personali da inserire nel sistema. I prodotti Interlogix offrono vari livelli di sicurezza per proteggere i Dati personali delle persone che hanno accesso alle sedi degli Utenti finali. Nel sistema possono essere configurati o installati standard del settore e metodi di crittografia conformi agli standard ISO come DESFire EV1 tra scheda e lettore, crittografia tra controller e server e HTTPS per una connessione sicura tra il server dell'applicazione Advisor Management e gli Utenti finali. Inoltre, l'applicazione supporta restrizioni di sistema complete per limitare l'accesso solo a coloro che sono stati autorizzati.

Oltre alla progettazione del prodotto, l'Installatore può fornire assistenza all'Utente finale nel determinare come gestire i campi obbligatori e i campi opzionali nei nostri prodotti. Il programma di installazione può fornire ulteriori informazioni su quali dati e registri è possibile visualizzare e quali backup vengono creati durante l'installazione, la messa in servizio e la manutenzione del prodotto.

Identificazione

Assicurati di sapere dove vengono conservati i Dati personali.

Conformità

Gestisci l'elaborazione, l'accesso e la cancellazione dei Dati personali e soddisfa le richieste di Soggetti interessati.

Protezione

Stabilisci procedure di sicurezza per proteggere i Dati personali.

Registrazione

Tieni un registro delle tue procedure.

Monitoraggio

Previeni le violazioni dei dati e segnalale.

interlogix
United Technologies

Regolamento generale sulla protezione dei dati

Prodotti Interlogix Advisor Advanced e Privacy dei dati

Sicurezza informatica

Interlogix si impegna per la sicurezza informatica dei suoi prodotti e servizi Advisor Advanced e per la protezione dei Dati personali. Interlogix lavora costantemente per migliorare i propri prodotti tenendo conto di questi obiettivi. A supporto di ciò, United Technologies Corporation (UTC), società madre di Interlogix, dispone di un Responsabile della sicurezza dei prodotti dedicato.

I prodotti Advisor Advanced consentono all'utente finale di memorizzare i Dati personali nel prodotto. L'identificativo di credenziali univoco (ID) e i diritti di accesso associati sono disponibili dai pannelli di controllo della sicurezza e consentono di prendere decisioni immediate. La presentazione di un ID di credenziali (codice pin o carta) in un lettore è abbinata all'ID di credenziali registrato nel sistema e l'accesso alle funzioni o alle porte/ascensori viene concesso o negato in base alle regole di sicurezza configurate dall'installatore del sistema presso la sede dell'Utente finale.

L'uso dei Dati personali è fondamentale per il sistema di controllo di sicurezza di un Utente finale al fine di gestire i movimenti e l'accesso alle funzioni richieste dei propri dipendenti e visitatori. Gli unici campi dati obbligatori in Advisor Management sono un nome e, se richiesto, una credenziale (numero badge, PIN) utilizzati allo scopo di collegare una credenziale a una persona e impostare le autorizzazioni per dove e quando l'utente può accedere alla funzione o all'accesso richiesti.

Esempi di campi che possono essere configurati per ottimizzare la gestione della sicurezza in Advisor Management sono: numero interno ed esterno (spesso utilizzato per raccogliere numeri HR interni o numeri ID interni), indirizzo email, genere, fotografia e livelli di accesso. Questi dati possono essere popolati da un database delle risorse umane attraverso uno scambio protetto di dati a intervalli regolari. L'accesso ai campi dati e la possibilità di aggiungerli o modificarli sono basati sulle decisioni degli Utenti finali e controllati da autorizzazioni configurabili dall'Utente finale.

I pannelli di controllo della sicurezza memorizzano i dettagli come eventi nei registri della cronologia eventi. Le voci del registro della cronologia eventi contengono una descrizione dell'evento contenente: l'ora e la data dell'occorrenza. L'Utente finale può anche configurare i registri affinché includano informazioni aggiuntive per identificare la persona coinvolta e la posizione dell'evento. Il nome di una persona può anche essere inviato a una stazione centrale di allarme per essere in grado di identificare chi è coinvolto in un evento e avviare l'azione corretta. Per gli allarmi anti-intrusione, l'archiviazione degli eventi e la segnalazione degli allarmi sono in linea con approvazioni di sicurezza come EN50131.

Gestire le attività di Privacy dei dati

Advisor Management offre la possibilità agli amministratori di sicurezza di un Utente finale di definire le autorizzazioni per garantire che gli individui abbiano i diritti di accesso a tali funzioni e dati nell'applicazione richiesta per svolgere i loro compiti, e per definire quale tipo di accesso è appropriato.

I pannelli di controllo di sicurezza di Advisor sono accessibili solo a utenti privilegiati (installatori, ecc.), che hanno accesso solo alle funzioni e ai dettagli di configurazione in base all'autorizzazione loro assegnata dall'Utente finale.

Advisor Management può essere utilizzato per configurare gli ambienti di controllo degli accessi e delle intrusioni e di monitoraggio degli allarmi, comprese le autorizzazioni di accesso degli utenti. Fornisce l'applicazione della password e può supportare il single sign-on. L'accesso al sistema può essere limitato alla responsabilità funzionale di un individuo mediante la segmentazione di hardware, posizione, applicazione e funzioni, nonché dei diritti di lettura e modifica.

Qualsiasi evento rilevato da un sensore viene inviato al pannello di controllo di sicurezza e quindi trasmesso a un'applicazione di gestione della sicurezza connessa, come ad esempio Advisor Management o strumenti di configurazione e diagnostica per la conservazione dei registri e la diagnostica. Ulteriori dati personali possono anche essere inviati a un centro di monitoraggio per il follow-up degli allarmi, a seconda dell'impostazione della configurazione decisa dall'Utente finale.

Per ogni evento relativo all'accesso attraverso porte o aree di intrusione, la descrizione dell'evento e i dettagli associati vengono acquisiti e conservati per primi nell'hardware in conformità ai requisiti normativi di sicurezza e, quando connessi all'applicazione Advisor Management, questi eventi vengono anche trasmessi e archiviati nell'applicazione. Ciò consente e permette la successiva verifica degli eventi da parte del personale autorizzato - se e secondo necessità - e per tutto il tempo necessario. La conservazione dei dati è determinata dall'utente finale; i Prodotti Advisor Advanced non forniscono un periodo di cancellazione predefinito ma consentono all'Utente finale di definirlo.

Ref. 1543 – Advisor IT – 1206