Règlement Général sur la Protection des Données

25 mai 2018

Produits Interlogix Advisor Advanced et confidentialité des données

advisor

GDPR

Le règlement général sur la protection des données (ou « RGPD »), en vigueur depuis le 25 mai 2018, est une loi visant à protéger les données à caractère personnel. Celles-ci comprennent toute information se rapportant à une personne physique identifiée ou identifiable qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale. Plus d'informations sur le RGPD sont disponibles à l'adresse suivante : **http://www.eugdpr.org**

La portée étendue du RGPD, qui s'applique à toutes les entités établies dans l'UE (que le traitement des données y ait lieu ou non) ainsi qu'aux entités traitant des données relatives à des résidents européens, constitue l'un des changements majeurs apportés aux réglementations de l'Union européenne.

United Technologies Corporation reconnaît l'importance du RGPD et a mis en œuvre, au niveau mondial, des règles d'entreprise contraignantes, telles qu'une politique de confidentialité et un système de gouvernance interne relatif à la confidentialité. Ces règles sont considérées comme une norme en matière de protection des données. Elles sont publiquement disponibles en plusieurs langues (**http://www.utc.com/Pages/Privacy.aspx**).

Comment cela affecte-t-il les produits Advisor Advanced ?

La gamme des produits Advisor Advanced développés par UTC Fire & Security Americas Corporation, Inc. (opérant sous le nom « Interlogix ») sont des solutions de sécurité proposant la détection d'intrusion et des fonctionnalités de contrôle d'accès. Il peut s'agir de produits matériels (centrales de sécurité, extensions, claviers, lecteurs et applications logicielles) permettant de configurer et de gérer ces solutions. Les données personnelles sont nécessaires au fonctionnement des différents systèmes. L'installateur, le client et l'utilisateur final collaborent avec vous pour définir les données personnelles qui sont saisies dans le cadre du processus d'installation et de mise en service. Interlogix n'installant ni ne mettant en service les produits Advisor Advanced, il revient à l'installateur et à l'utilisateur final de déterminer si la collecte et l'utilisation des informations personnelles sont conformes aux exigences du RGPD.

Bien que l'utilisateur final soit responsable de la saisie, du traitement et de la gestion des données personnelles liées aux produits Advisor Advanced, Interlogix aide l'utilisateur final à se conformer aux normes de confidentialité en concevant des produits répondant à ces exigences. Interlogix assure la protection de la vie privée dès la conception.

Étant donné que l'utilisateur final détermine les données personnelles qui doivent être entrées dans le système, nos produits sont conçus dans son intérêt. Les produits Interlogix offrent différents niveaux de protection des données personnelles liées aux personnes ayant accès aux données des utilisateurs finaux. Il est possible d'intégrer des normes reconnues et des méthodes de chiffrement ISO au système (par exemple, le système DESFire EV1 dans un lecteur de cartes, le chiffrement entre contrôleur et serveur, ou le protocole HTTPS permettant de sécuriser la connexion entre le serveur de l'application Advisor Management et les utilisateurs finaux). En outre, l'application propose des fonctionnalités complètes de restriction système, qui permettent de limiter l'accès aux individus autorisés uniquement.

En plus du produit lui-même, l'installateur peut aider l'utilisateur final à déterminer comment traiter les champs obligatoires et facultatifs de nos produits. L'installateur peut fournir des informations supplémentaires sur les données et les journaux qu'il peut lire et sur les sauvegardes créées lors de l'installation, de la mise en service et de la maintenance du produit.

Identification

Assurez-vous de savoir où sont conservées les données personnelles.

Conformité

Gérez le traitement, l'accès aux données personnelles ainsi que leur suppression, et respectez les demandes des personnes concernées.

Protection

Établissez des procédures de sécurité pour protéger les données personnelles.

Enregistrement

Gardez une trace de vos procédures.

Contrôle

Empêchez les violations de données et signalez-les.

interlogix
United Technologies

Règlement Général sur la Protection des Données

Produits Interlogix Advisor Advanced et confidentialité des données

Cybersécurité

Interlogix s'engage à assurer la cybersécurité de ses services et produits Advisor Advanced et à protéger vos données personnelles. Nous travaillons continuellement à l'amélioration des produits tout en tenant compte desdits objectifs. À cette fin, United Technologies Corporation (UTC), la société mère d'Interlogix, emploie un responsable chargé de la sécurité des produits.

L'utilisateur final a la possibilité de stocker des données personnelles dans un produit Advisor Advanced. L'identifiant unique (ID) et les droits d'accès associés sont disponibles via les panneaux de contrôle pour encourager la prise de décision instantanée. L'identifiant (code PIN ou carte) présenté sur le lecteur doit correspondre à celui enregistré dans le système. L'accès aux fonctions demandées ou aux portes/ascenseurs est accordé ou refusé en fonction des règles de sécurité configurées par l'installateur du système dans les locaux de l'utilisateur final.

Les données personnelles représentent un élément incontournable des systèmes de sécurité conçus pour contrôler les accès des employés et visiteurs. Les seuls champs obligatoires dans Advisor Management sont ceux liés au nom d'utilisateur et, si nécessaire, à un identifiant (numéro de badge, code PIN) associé à une personne afin de définir les autorisations d'accès de l'utilisateur.

Voici des exemples de champs pouvant être configurés pour optimiser la gestion de la sécurité dans Advisor Management : numéro interne et externe (souvent utilisé pour rassembler des numéros RH ou ID internes) ; adresse e-mail ; sexe ; photographie ; et niveaux d'accès. Ces données peuvent être alimentées à partir d'une base de données RH via un échange sécurisé de données à intervalles réguliers. Les accès aux champs de données ainsi que la possibilité d'en ajouter ou de les modifier sont fondés sur les décisions des utilisateurs finaux et contrôlés par des autorisations configurables par ces derniers.

Les panneaux de contrôle conservent les informations sous forme d'événements dans les journaux de l'historique des événements. Les entrées de l'historique contiennent une description de l'événement, accompagnée de l'heure et de la date associées. L'utilisateur final peut également configurer les journaux de sorte que d'autres informations y soient consignées afin d'identifier la personne impliquée et le lieu de l'événement. Le nom d'une personne peut également être envoyé à une centrale d'alarme afin d'identifier les individus impliqués et de prendre les mesures appropriées. Pour les alarmes d'intrusion, le stockage des événements et les rapports d'alarme sont conformes aux autorisations de sécurité (comme la norme EN50131).

Aide pour la confidentialité des données

L'application Advisor Management permet aux administrateurs de sécurité en charge des utilisateurs finaux de définir des autorisations et un type d'accès.

Celles-ci leur assurent les droits nécessaires pour effectuer leurs tâches.

Les panneaux de contrôle Advisor sont accessibles uniquement aux personnes autorisées (installateurs, etc.), qui ont accès aux fonctions et détails de configuration définis par les autorisations attribuées par l'utilisateur final.

L'application Advisor Management peut être utilisée pour configurer les centrales d'intrusion et environnements de surveillance des alarmes, notamment en matière d'autorisations d'accès. Elle propose la mise en place d'un mot de passe et peut prendre en charge un système d'authentification unique. L'accès au système peut être restreint et limité à la responsabilité fonctionnelle d'un individu en segmentant le matériel, l'emplacement, l'application et les fonctions, ainsi que les droits de lecture et de modification.

Tout événement détecté par un capteur est envoyé à la panneau de contrôle, puis transmis à une application de gestion connectée telle qu'Advisor Management ou à des outils de configuration et de diagnostic, afin d'être conservé et analysé. Des données personnelles supplémentaires peuvent également être envoyées à un centre de surveillance pour assurer le suivi des alarmes, si la configuration est ainsi définie.

Dans le cas de chaque événement lié à l'accès par une porte et aux zones d'intrusion, sa description et les détails associés sont d'abord capturés et conservés au niveau matériel (conformément aux exigences réglementaires de sécurité). Une fois la connexion à l'application Advisor Management établie, ces informations sont transmises à celle-ci. Ainsi, les événements peuvent, le cas échéant, être examinés ultérieurement par le personnel autorisé pendant une durée illimitée. Pour les produits Advisor Advanced, l'utilisateur final détermine la période pendant laquelle les données sont conservées, aucune date de suppression par défaut n'est définie.

Ref. 1543 – Advisor FR – 0211