

Le 17 juin 2024

# Gamme Axon et confidentialité des données

En tant que société Carrier, Aritech reconnaît l'importance des lois sur la confidentialité des données. Carrier a mis en place une gouvernance et une politique de confidentialité au niveau mondial afin de garantir leur respect.

## Lois sur la protection des données

Les gouvernements nationaux et régionaux du monde entier renforcent leur législation en matière de respect de la confidentialité des données, en introduisant de nouvelles lois plus strictes concernant l'utilisation et la conservation des données à caractère personnel. Les données personnelles sont toutes les informations relatives à une personne physique identifiée ou identifiable, qui peut être reliée, directement ou indirectement, aux données, notamment par référence à un numéro d'identification ou à un ou plusieurs facteurs spécifiques à sa spécification physique, physiologique, mentale, économique, culturelle ou sociale. De nombreuses lois sur la confidentialité des données ont une compétence étendue, ce qui signifie qu'elles s'appliquent à des entités établies en dehors de la région, mais qui font des affaires dans cette région ou qui se concentrent également sur des personnes concernées établies dans cette région. Carrier reconnaît l'importance de ces lois sur la confidentialité des données et a mis en place, au niveau mondial, un système de gouvernance interne et une politique de confidentialité.

Carrier a également obtenu des BCR (Binding Corporate Rules) dans l'UE, qui sont considérées comme la référence en matière de protection des données ([Approved Binding Corporate Rules | European Data Protection Board \(europa.eu\)](#)) et sont publiées ici : [lien](#). En outre, Carrier dispose d'une équipe mondiale chargée de la protection des données.

## Comment cela affecte-t-il le portfolio d'Axon ?

Axon, développé par Carrier Corporation ( qui exerce ses activités sous le nom d'"Aritech"), consiste en une gamme de produits et de solutions qui assurent la sécurité des propriétés en installant des fonctionnalités de détection d'intrusion et de contrôle d'accès. Axon et les produits dérivés comprennent du matériel, comme les centrales de sécurité intrusion, les extenseurs, les claviers et les lecteurs, ainsi que des applications logicielles permettant de configurer et de gérer les solutions.

Axon utilise le logiciel Advisor Management comme interface pour gérer et contrôler les installations de sécurité sur site ou à distance. L'utilisation des données personnelles est essentielle au système de contrôle de sécurité d'un utilisateur final pour gérer les mouvements et l'accès aux fonctions requises de ses employés et visiteurs. Les seuls champs de données obligatoires dans le logiciel Advisor Management sont le nom et, le cas échéant, un justificatif d'identité (numéro de badge, code PIN) utilisé pour relier un justificatif d'identité à une personne et définir les autorisations permettant de déterminer où et quand l'utilisateur peut accéder à la fonction ou à l'accès demandé.

L'entreprise qui installe la solution de sécurité Axon travaille avec l'utilisateur final pour définir les éléments de données à caractère personnel qui sont saisis dans le cadre du processus d'installation et de mise en service. Aritech n'installant pas et ne mettant pas en service la solution Axon, il incombe à l'installateur et à l'utilisateur final de s'assurer que la collecte et l'utilisation des données personnelles sont cohérentes afin de respecter la confidentialité des données.

L'identification unique et les droits d'accès associés sont disponibles via la centrale de sécurité pour une prise de décision instantanée. La présentation d'un identifiant (code pin ou carte) à un lecteur est comparée à l'identifiant enregistré dans le système et 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.

Parmi les champs qui peuvent être configurés pour optimiser la gestion de la sécurité dans Advisor Management, on peut citer les numéros internes et externes (souvent utilisés pour rassembler les numéros RH internes ou les numéros d'identification internes), l'adresse électronique, le sexe, la photographie et les niveaux d'accès. Ces données peuvent provenir d'une base de données RH par le biais d'un échange sécurisé de données à intervalles réguliers. L'accès aux champs de données et la possibilité de les ajouter ou de les modifier sont basés sur les décisions des utilisateurs finaux et contrôlés par des autorisations configurables par l'utilisateur final.

Les centrales de sécurité enregistrent les détails sous forme d'événements dans les journaux d'historique des événements. Les entrées du journal de l'historique des événements contiennent une description des événements avec l'heure et la date de l'événement. L'utilisateur final peut également configurer les journaux pour qu'ils contiennent des informations supplémentaires permettant 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 pour permettre d'identifier la personne impliquée dans un événement et de

lancer l'action appropriée. Pour les alarmes anti-intrusion, le stockage des événements et les rapports d'alarme sont conformes aux agréments de sécurité tels que la norme EN50131.

- **Identifier** Assurez-vous de savoir où sont conservées les données à caractère personnel.
- **Respecter** Gérer le traitement, l'accès et la suppression des données à caractère personnel et répondre aux demandes des personnes concernées.
- **Protéger** Établissez des procédures de sécurité pour protéger les données à caractère personnel.
- **Enregistrer** Conservez une trace de vos procédures.
- **Contrôler** Prévenir les violations de données et les signaler.

## La protection des données dès la conception « Privacy by Design »

Carrier adhère aux principes du "Privacy by Design", qui constituent désormais une obligation légale en vertu de nombreuses lois sur la confidentialité des données. Le principe "Privacy by Design" exige que la protection des données fasse partie intégrante de la conception des systèmes.

Si l'utilisateur final est responsable en dernier ressort de la saisie, du traitement et de la gestion des données personnelles dans les produits Axon, Aritech l'aide à respecter la confidentialité des données en intégrant les exigences de protection des données dans la conception du produit. Aritech s'engage à respecter la confidentialité dès la conception.

Nos produits sont conçus pour aider l'utilisateur final, car c'est lui qui détermine les données personnelles à introduire dans le système. Les produits Aritech offrent différents niveaux de sécurité pour protéger les données personnelles des personnes ayant accès aux locaux des utilisateurs finaux. Les normes industrielles respectées et les méthodes de cryptage conformes à l'ISO peuvent être configurées ou installées dans le système, telles que DESFire EV1 entre la carte et le lecteur, le cryptage entre le contrôleur et le serveur, et HTTPS pour une connexion sécurisée entre le serveur de l'application Advisor Management et les utilisateurs finaux. En outre, l'application prend en charge des restrictions complètes du système afin de limiter l'accès aux seules personnes autorisées.

Outre la conception du produit, l'installateur peut aider l'utilisateur final à déterminer comment traiter les champs obligatoires et les champs facultatifs dans nos produits. L'installateur peut fournir des informations supplémentaires sur les données et les journaux qu'il peut consulter et sur les sauvegardes créées pendant l'installation, la mise en service et la maintenance du produit.

## Assistance dans les tâches liées à la protection des données

Advisor Management permet aux administrateurs de sécurité d'un utilisateur final de définir des permissions pour s'assurer que les personnes ont accès aux fonctions et aux données de l'application nécessaires à l'accomplissement de leurs tâches, ainsi que de définir le type d'accès approprié.

Les centrales de sécurité Axon ne sont accessibles qu'aux personnes habilitées (installateurs, etc.), qui n'ont accès qu'aux fonctions et aux détails de configuration en fonction des autorisations qui leur ont été attribuées par l'utilisateur final.

Advisor Management permet de configurer les environnements d'accès, de contrôle d'intrusion et de surveillance des alarmes, y compris les autorisations d'accès de l'utilisateur final. Il permet l'application des mots de passe et peut prendre en charge l'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 la fonction, ainsi que les droits de lecture et d'édition.

Tout événement détecté par un détecteur est envoyé à la centrale de sécurité, puis transmis à une application de gestion de la sécurité connectée, telle que la "Advisor Management", ou à des outils de configuration et de diagnostic à des fins d'archivage et de diagnostic. Des données personnelles supplémentaires peuvent également être envoyées à un centre de télésurveillance pour assurer le suivi des alarmes, en fonction de la configuration décidée par l'utilisateur final.

Pour chaque événement lié à l'accès par les portes ou les zones d'intrusion, la description de l'événement et les détails associés sont d'abord capturés et conservés dans le matériel conformément aux exigences réglementaires en matière de sécurité et, lorsqu'ils sont connectés à l'application Advisor Management, ces événements sont également transmis et stockés dans l'application. Cela permet au personnel autorisé de vérifier ultérieurement les événements, le cas échéant, et aussi longtemps que nécessaire. La conservation des données est déterminée par l'utilisateur final ; les produits Axon ne prévoient pas de période de suppression par défaut, mais permettent à l'utilisateur final de la définir.

## Donner aux personnes le droit de contrôler leurs données

Advisor Management fournit un certain nombre de champs stockant des données personnelles dans le but d'identifier l'attribution des droits d'accès et de contrôler l'utilisation correcte des codes PIN, des cartes d'accès, des plaques

d'immatriculation ou d'autres types de justificatifs équivalents. Ces champs sont contrôlés par les opérateurs du logiciel Advisor Management.

Le logiciel Advisor Management stocke les informations relatives à l'utilisateur dans des journaux afin de vérifier l'utilisation correcte des droits d'accès dans l'application en tant qu'accès physique par des éléments de sécurité tels que des portes, des ascenseurs ou des zones d'intrusion. L'application Advisor Management offre des options permettant de limiter la période de stockage et de fournir des rapports sur les données personnelles stockées de toute personne ou de visualiser les opérateurs qui traitent les données personnelles.

La centrale Axon crée également des journaux comme l'exigent les réglementations et à des fins d'audit. Les centrales Axon fournissent des moyens d'anonymiser les données personnelles après une période de temps configurable, car les entrées de journal ne peuvent pas être supprimées.

## **À propos d'Aritech**

Aritech fournit des solutions de pointe en matière de sécurité et de protection des personnes pour les applications commerciales couvrant l'intrusion, la vidéo, la transmission et l'accès. En proposant des produits parmi les plus réputés du secteur et en s'appuyant sur des services et une assistance permanente de ses partenaires, Aritech aide ses clients à sécuriser et à protéger ce qui compte le plus. Aritech fait partie de Carrier Global Corporation, l'un des principaux fournisseurs mondiaux de solutions de construction et de chaîne du froid saines, sûres et durables. Pour plus d'informations, visitez [aritech.com](https://aritech.com) ou suivez-nous sur LinkedIn @Aritech.

*La langue de référence de cette brochure est l'anglais : [lien](#). En cas de conflit entre cette traduction et la version anglaise de la brochure, c'est cette dernière qui prévaut.*

©2024 Carrier. All Rights Reserved. Toutes les marques commerciales et marques de service mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs.. A Carrier Company. Ref. 1543 EN – 0405