

Fiche de confidentialité des produits

Centre de sécurité Genetec™

Ce document est un complément à la Politique de confidentialité de Genetec disponible sur www.genetec.com/fr/legal/confidentialite (la « politique de confidentialité ») et s'applique au produit Genetec suivant (le « **Produit** ») : Centre de sécurité Genetec™.

Aperçu

Dans le cadre de votre utilisation du Produit, vous (soit vous en tant qu'individu, soit l'entité juridique que vous représentez, le cas échéant; ci-après « **vous** », « **votre** » ou « **le vôtre** »), ou vos utilisateurs, pouvez télécharger, recevoir ou générer des données (« **Données** »). Ce document décrit quel type de données est concerné et dans quelle mesure Genetec (également désigné « **nous** », « **notre** » ou « **nos** ») peut accéder, stocker, utiliser ou traiter de toute autre manière (ci-après « **traitement** », « **processus** » ou d'autres mots similaires) vos données.

Environnement de déploiement

Veuillez garder à l'esprit que l'environnement de déploiement du Produit peut avoir un impact sur la portée du traitement des Données. Il est donc essentiel de déterminer comment le Produit sera déployé afin de bien comprendre les implications de l'accès aux Données.

Le déploiement dans un « **environnement local** » signifie que le Produit est déployé dans une infrastructure non fournie par Genetec, que toutes les Données sont stockées dans les systèmes d'hébergement de Données et les serveurs que vous fournissez et qu'elles ne sont pas mises à la disposition de Genetec, sauf dans les cas décrits dans le présent document.

Le déploiement dans un « **environnement cloud** » signifie que le Produit est déployé dans l'environnement d'hébergement fourni par Genetec (et hébergé par Microsoft Azure dans ses centres de données Azure sécurisés). L'environnement contiendra normalement les Données d'autres clients Genetec, mais les Données respectives de chaque client sont séparées logiquement afin qu'aucun client ne puisse voir ou accéder aux Données d'autres clients. Vos Données ne seront visibles par aucun autre client utilisant son instance du Produit à partir du même environnement cloud.

Lorsque le Produit est fourni dans une combinaison d'un environnement cloud et d'un environnement local, nous appelons ce déploiement un **environnement hybride**. Dans ces cas, l'accessibilité aux Données

variera en fonction de la conception du Produit déployé. Veuillez vous référer à la description des cas d'utilisation des Données ci-dessus pour déterminer comment ces Données seront traitées par nous.

Quel type de Données sera capturé par le Produit ?

Composantes communes

Répertoire

Le répertoire du centre de sécurité (« **Répertoire** ») est la composante du Produit qui gère toutes les configurations système, les paramètres et les autres Données répertoriées ci-dessous, qui resteront dans le Produit jusqu'à ce qu'ils soient supprimés.

Données utilisateur : Le Répertoire est responsable de l'authentification de toutes les connexions utilisateur et, à ce titre, capture les identificateurs d'utilisateur pour identifier de manière unique les utilisateurs autorisés. Cela inclut leur nom, leur adresse électronique et leurs coordonnées configurées dans le Produit. En outre, le Produit conserve un enregistrement de toutes les activités de l'utilisateur dans le cadre de sa piste de vérification, qui peut également inclure des modifications à la configuration du système apportées par chaque utilisateur. Par défaut, ces Données sont stockées pendant une période de 90 jours, mais vous pouvez désactiver leur capture.

Données d'utilisation : Le Répertoire capture certaines Données statistiques et d'utilisation non personnelles, telles que le type d'action de l'utilisateur, le type de capture (manuelle ou automatique), etc. Les Données d'utilisation ne contiennent aucune de vos Données personnelles ou confidentielles.

Configuration du système : Diverses Données concernant vos paramètres de configuration seront capturées par le Produit via le Répertoire, telles que le langage du système d'exploitation utilisé, votre identification du Produit, la version des produits Genetec installés sur votre appareil, etc.

GUS et SAM

Le Produit comprend deux services connectés que vous pouvez activer à votre discrétion : GUS et SAM.

Le premier, le service de mise à jour Genetec (GUS), vous permet de mettre à jour votre Produit lorsqu'une nouvelle version devient disponible pour vous. GUS vous permet notamment de recevoir des mises à jour automatisées de logiciels et de micrologiciels, des notifications de sécurité et d'autres contenus non marketing pertinents. Pour ce faire, GUS collecte des Données sur l'utilisation de votre système, composées de répertoires, de rôles, d'unités, d'entités que vous avez dans votre système de sécurité et de leur disponibilité (heures de disponibilité et d'arrêt), qui ne contiennent aucune information personnelle.

Le second, le moniteur de disponibilité du système (SAM), permet à vos administrateurs système (qui peuvent inclure votre intégrateur système) d'avoir une vue d'ensemble générale de l'état et de la disponibilité de tous les systèmes de sécurité connectés au Produit. Pour ce faire, SAM utilisera les mêmes données que celles collectées par GUS pour compiler des statistiques sur la disponibilité et l'intégrité du Produit, telles que le pourcentage de disponibilité, le temps moyen entre les erreurs et le temps moyen qu'une entité prend pour revenir en ligne. SAM nécessite un abonnement actif au programme Advantage Genetec™ pour fonctionner.

Pour faciliter un support proactif et améliorer la communication, GUS et SAM sont configurés pour permettre à Genetec de recevoir les Données décrites ci-dessus par défaut. Vous pouvez choisir d'activer GUS et SAM sur une base anonyme, ce qui signifie que toutes les Données soumises à Genetec seront conservées de manière agrégée avec les Données similaires d'autres clients de Genetec et nous ne serons pas en mesure de vous identifier comme la source de ces Données. Vous pouvez également choisir de désactiver GUS et SAM, auquel cas aucune Donnée ne sera collectée. Veuillez noter, cependant, que ces deux dernières options pourraient limiter certaines des capacités des services respectifs.

Composantes facultatives

Comme le Produit est une plate-forme modulaire, vous devez obtenir une licence pour utiliser un ou plusieurs de ses composantes facultatives afin de profiter pleinement des fonctionnalités du Produit. Les Données collectées par le Produit varieront en fonction de la composante couverte par votre licence, tel que décrit ci-dessous.

Omnicast™

Omnicast™ est notre système de gestion vidéo, dont la fonction principale est d'enregistrer et de vous permettre de gérer des séquences vidéo à partir de vos caméras connectées. Omnicast™ n'est disponible que pour le déploiement dans les environnements locaux et ainsi aucune des Données répertoriées ci-dessous ne sera mise à la disposition de Genetec.

Enregistrement vidéo et métadonnées : le Produit capture l'enregistrement vidéo de chaque caméra inscrite dans le Produit, y compris les métadonnées associées, y compris les horodatages, la géolocalisation, etc.

Données de l'appareil: Le Produit capturera également des Données sur les caméras connectées, telles que leur nom et leur modèle respectifs. Ces informations seront également utilisées par le Produit pour recommander et mettre à votre disposition des mises à jour du micro-logiciel disponibles pour ces caméras, où la fonctionnalité est prise en charge.

AutoVu™

AutoVu™ est notre système de reconnaissance automatique des plaques d'immatriculation. AutoVu™ fonctionne en mode natif avec nos caméras AutoVu™ Sharp. Ces caméras sont conçues pour capturer des Données pertinentes vous permettant de les utiliser avec les systèmes AutoVu™, Genetec Patroller™ et / ou Genetec Motoscan™. Pour procurer une protection contre les défaillances du système ou du réseau, ces appareils sont conçus pour capturer et entreposer à l'interne, l'identification des plaques d'immatriculation, les images et les métadonnées (y compris les horodatages et la géolocalisation) jusqu'à ce que ces Données soient déchargées.

Vous trouverez ci-dessous une liste des Données collectées et stockées dans le cadre de votre utilisation d'AutoVu™, quelle que soit l'infrastructure dans laquelle vous déployez le Produit. Les systèmes AutoVu™ sont disponibles pour les déploiements dans des environnements locaux, cloud ou hybrides. En outre, les Données collectées tel que décrit ci-dessous sont stockées en fonction des périodes de conservation que vous définissez, qui peuvent varier en fonction du type de données.

Identification de la plaque d'immatriculation: Le Produit capturera et reconnaîtra l'identification de la plaque d'immatriculation pour vous permettre de localiser géographiquement le véhicule identifié à l'aide du produit. Cela inclut le numéro de plaque d'immatriculation et l'état / la province / le pays de délivrance.

Images et métadonnées : Le Produit capture en outre des images d'un véhicule identifié à l'aide du Produit, ainsi que les métadonnées d'image associées, telles que la marque, le modèle, la vitesse, la direction et la classification du véhicule. Cela peut inclure des images de la plaque d'immatriculation du véhicule, du véhicule lui-même et des images des zones environnantes, qui peuvent inclure des images de personnes qui passent au moment où les images ont été capturées.

Données de l'appareil: Le Produit capture les données de l'appareil sur les caméras AutoVu™ Sharp connectées à votre système AutoVu™, y compris le nom et le modèle des caméras connectées. Le Produit saisira en outre les identifiants uniques de l'appareil sur les appareils utilisés pour capturer les Données du véhicule identifié à l'aide du Produit, qui peuvent inclure des identifiants uniques de caméras, d'ordinateurs, de capteurs et d'autres matériels ou logiciels utilisés pour capturer et traiter ces données dans le cadre de l'utilisation du produit.

Données d'événement: En fonction de votre configuration du Produit, celui-ci utilisera l'identification de la plaque d'immatriculation, les images et les métadonnées (tel que décrit ci-dessus), ainsi que l'heure à laquelle l'événement capturé s'est produit et sa géolocalisation pour générer des Données liées à l'événement, telles que les informations sur les périodes de stationnement et les transactions de billets de stationnement.

Vous pouvez également choisir d'importer des Données supplémentaires dans le Produit, telles que des listes de licences et des listes critiques. Avec ces Données importées, vous avez la possibilité de configurer davantage le Produit afin de gérer les événements et d'inclure de vérifier si un véhicule est recherché ou non, si un permis est valide ou non, le stationnement visité, des informations descriptives sur les véhicules que vous recherchez, etc.

Genetec Patroller™ et Genetec Motoscan™

Tout comme AutoVu™, Genetec Patroller™ et Genetec Motoscan™ sont nos logiciels spécialisés de reconnaissance des plaques d'immatriculation. Cependant, Genetec Patroller™ est destiné aux déploiements de véhicules uniquement, tandis que Genetec Motoscan™ est destiné aux déploiements de motocyclettes et véhicules mobiles similaires. Genetec Patroller™ et Genetec Motoscan™ peuvent se connecter à votre exemplaire d'AutoVu™, mais sont conçus pour être autonomes et déconnectés. Selon vos besoins, vous pouvez ainsi choisir de stocker toutes les Données localement, jusqu'à ce qu'elles soient déchargées dans AutoVu™.

Données de plaque d'immatriculation: Le Produit capturera les mêmes Données de plaque d'immatriculation que celles capturées par AutoVu™ et décrites ci-dessus.

Données d'événement: Le Produit capturera les mêmes Données que celles capturées par AutoVu™ et décrit ci-dessus.

Paramètres de configuration : Le Produit collectera diverses informations concernant ses paramètres, à savoir, notamment, si le Produit est configuré à des fins de circulation ou d'application de la loi, et la version Genetec Patroller™ utilisée.

Adresse IP : Enfin, le Produit partagera son adresse IP avec votre instance d'AutoVu™ et vice-versa, pour s'assurer que les deux systèmes s'interconnectent pour vous permettre de décharger vos Données de Genetec Patroller™ vers AutoVu™.

Synergis™

Synergis™ est notre système de contrôle d'accès et vous permet de contrôler l'accès et le flux des personnes sur votre site.

Données sur les utilisateurs permanents et les visiteurs : Pour vous permettre de configurer les droits d'accès, le Produit collectera diverses Données sur les personnes à qui vous accordez ces droits d'accès, qu'il s'agisse d'utilisateurs permanents (tels que vos employés ou sous-traitants) ou de visiteurs. Cela comprend le prénom et le nom de famille de ces personnes, ainsi que tout autre attribut que vous choisissiez d'entrer pour identifier une personne. Selon votre choix, ces champs personnalisés peuvent inclure des Données personnelles. Ces Données seront stockées dans le produit jusqu'à ce que vous décidiez de le supprimer.

Historique d'accès : Le Produit collectera des Données concernant l'historique d'accès d'un utilisateur permanent ou d'un visiteur, telles que les lieux visités, l'heure d'enregistrement et de départ, si un accès a été refusé ou accordé et la raison de l'accès refusé, etc. Par défaut, les Données de l'historique d'accès seront conservées dans le Produit pendant une période de 90 jours, mais vous avez la possibilité de configurer une période de conservation différente.

Données de l'appareil: Pour tirer parti du Produit et associer les droits d'accès aux points d'entrée, diverses Données relatives aux appareils et à l'emplacement physique qu'ils contrôlent seront collectées, telles que le nom et le modèle des capteurs de porte, le nom des lecteurs de contrôle d'accès, le format des cartes d'accès, le nom de la porte, le nom d'un secteur ou d'une zone, etc.

Federation™

Federation™ vous permet de connecter plusieurs instances d'installation du Centre de sécurité que vous utilisez pour sécuriser vos locaux dans un seul système virtuel. Federation™ vous permet d'utiliser des instances individuelles du Centre de sécurité pour afficher, gérer et contrôler à distance d'autres instances d'installation du Centre de sécurité compatibles faisant partie de votre système virtuel.

Federation™ ne stocke aucune Donnée et autorise uniquement l'accès à distance et le transfert de vos Données entre des instances du Centre de sécurité interconnectées faisant partie de votre infrastructure de sécurité. Cependant, certaines Données relatives à vos systèmes fédérés seront conservées dans le répertoire de votre système de Centre de sécurité local, telles que le nom de vos caméras connectées et d'autres données non personnelles. Dans le cas de Synergis™, une copie de vos Données d'utilisateurs et de visiteurs permanents (telles que définies ci-dessus) sera également stockée dans le répertoire. La période de rétention de ces données est configurée par vous.

Genetec Citigraf™

Genetec Citigraf™ vous permet de connecter des capteurs et d'autres sources de Données pour avoir une vue centralisée de vos opérations. Il permet uniquement l'accès à distance aux Données à partir de sources connectées et n'est pas conçu pour stocker ces Données. Genetec Citigraf™ peut toutefois vous permettre de conserver la géolocalisation et les horodatages des événements que vous choisissez de suivre pour améliorer les capacités de recherche d'événements.

Genetec Citigraf™ n'est disponible que pour le déploiement dans les environnements locaux.

Genetec Mission Control™

Genetec Mission Control™ est notre système collaboratif de gestion des décisions. Disponible pour le déploiement uniquement dans les environnements locaux, Genetec Mission Control™ accède à distance aux Données des capteurs et des dispositifs de sécurité connectés pour guider votre équipe de sécurité à suivre les processus spécifiques à votre organisation lorsqu'un événement (tel qu'un incident) se produit.

Genetec Mission Control™ permet l'accès à distance aux Données à partir de sources connectées et n'est pas désigné pour stocker des Données de cette source.

Données sur les incidents : Pour permettre une gestion efficace des incidents, le Produit recueillera diverses Données liées à chaque incident capturé, y compris l'heure à laquelle il s'est produit et la source de

l'événement. Ces Données seront conservées dans le Produit par défaut pendant une période de 90 jours, mais vous avez la possibilité de configurer une période de conservation différente.

Données sur les performances de l'opérateur : Vous pouvez surveiller davantage les performances de vos opérateurs et les mesures prises pour résoudre l'incident. À cette fin, le Produit conservera donc le temps de réponse et le temps de résolution de chaque incident. De plus, le Produit vous permet de préregler des questions auxquelles vos opérateurs doivent répondre et prévoit une section si vous ou vos opérations souhaitez ajouter des commentaires en relation avec un incident spécifique. Ces Données seront conservées dans le Produit par défaut pendant une période de 90 jours, mais vous avez la possibilité de configurer une période de conservation différente.

Sipelia™

Sipelia™ vous permet d'effectuer, de recevoir et de gérer des appels vocaux et vidéo basés sur le protocole d'initiation de session (PIS) sur un réseau.

Enregistrement audio/vidéo et métadonnées : Pour vous permettre de gérer vos appels, que ce soit pour y répondre, les transférer ou les mettre en attente, le Produit capturera diverses Données liées aux appels reçus. Ceci inclut l'enregistrement audio et vidéo de l'appel, l'heure de début et de fin d'appel, le type d'appel, l'état d'appel, etc. Par défaut, ces Données seront conservées pendant une période de 30 jours, mais vous avez la possibilité de configurer une période de conservation différente. Le Produit vous permet également de conserver uniquement du contenu vidéo ou audio, ou ni l'un, ni l'autre, dans le cadre de votre configuration de rétention.

Informations sur l'appareil : le Produit capture les Données relatives aux périphériques qui y sont connectés, telles que le nom de l'interphone, l'extension d'interphone, etc. Ces Données sont capturées pour vous permettre de produire des rapports en fonction de vos besoins.

Logiciels et modules externes (plug-ins) tiers

Le Produit vous permet en outre de vous connecter à des logiciels, du matériel et des modules externes tiers compatibles afin d'importer des Données dans le Produit. Par conséquent, en fonction de votre configuration et des politiques de ces tiers, vos Données peuvent leur être accessibles. Dans ce cas, cet accès est soumis à leurs propres modalités et conditions et est expressément exclu de la portée de ce document.

Il en va de même des différents modules complémentaires que vous pouvez obtenir pour

compléter le Produit, lesquels ne sont pas couverts par ce document.

Accès aux données

Vos Données ne peuvent être consultées que par les administrateurs système autorisés (qui peuvent inclure votre intégrateur système) et les utilisateurs disposant des privilèges d'accès appropriés, tels que définis par vous.

Dans la mesure où vous déployez le Produit dans un environnement local, aucune Donnée ne sera mise à la disposition de Genetec, à l'exception de GUS et SAM, lorsqu'elle est activée.

Dans la mesure où vous déployez le produit dans notre environnement cloud, vos Données seront traitées dans nos centres de données de la manière décrite dans ce document. Un nombre limité de nos employés auront accès à vos Données pour nous permettre de vous procurer le service.

Dans la mesure où Genetec vous procure du support en ce qui concerne le Produit, notre équipe d'assistance

n'aura accès qu'aux informations que vous nous soumettez dans le cadre de votre demande d'assistance ou auxquelles vous décidez de nous accorder l'accès via le Produit. Ainsi, dans certains cas, nous pouvons vous demander de partager des informations supplémentaires avec nous pour être en mesure de répondre à votre demande d'assistance. Sauf indication contraire dans ce document, les employés de Genetec n'auront pas accès à vos Données.

Propriété des données

Vous demeurerez toujours le propriétaire de vos Données. Vous êtes entièrement responsable du contenu de vos Données, ce qui inclut l'obtention de tous les droits, consentements, autorisations et autres approbations de tous les tiers concernés qui peuvent être nécessaires pour que vous puissiez mettre vos Données à notre disposition dans le cadre de votre utilisation du Produit, et pour que nous traitions vos Données conformément aux modalités de notre politique de confidentialité et de ce document.

La dernière mise à jour de ce document date du 4 décembre 2019. La dernière version de ce document peut être consultée à www.genetec.com/fr/legal/pps-sc. Nous vous invitons à vous abonner aux notifications légales dans notre [Centre d'abonnement par courriel](#) pour, entre autres, être informé de tout changement majeur apporté à ce document.