MAKE THE
WORLD SEE

Milestone Systems

Guide relatif au respect de la vie privée dans le cadre du RGPD

milestone

Version history

Version du document	Release	Commentaires
Version 4	2022 R1	Les mises à jour de cette version incluent : • Chiffrement des communications entre tous les serveurs et clients ajouté à Comment XProtect réduit l'impact sur les intérêts ou les droits fondamentaux et les libertés des personnes concernées sur la page 32. • Recommandations pour activer le chiffrement pour toutes les communications entre tous les serveurs et clients ajoutées à Garantir la protection des données par défaut sur la page 44. • Recommandations pour activer le chiffrement de toutes les communications entre tous les serveurs et clients ajoutées à Protéger les données stockées et transmises sur la page 47. • XProtect Rapid REVIEW ajouté à Composants et périphériques qui n'ont pas le label européen de protection des données à caractère personnel sur la page 57. • Recommandations supprimées de Mesures de protection supplémentaires sur la page 61 car Milestone XProtect VMS prend maintenant en charge le chiffrement de la communication entre tous les serveurs et clients. • Ajout d'informations sur les sources de données en conséquence d'un IdP externe à Données personnelles de l'environnement sur la page 67. • Ajout d'informations à Données personnelles du système sur la page 67 sur la façon dont l'IdP consigne les données et la suppression des données personnelles dans tous les journaux de débogage du VMS.

Version du document	Release	Commentaires

		• Mise à jour de Données authentification et d'autorisation sur la page 69:
		  • Prise en charge du RGPD pour les utilisateurs standard
		  • Recommandations concernant l'IdP externe
		  • Chiffrement de jetons, ne nécessitant donc plus de protections supplémentaires

Version 3	2021 R2	Les mises à jour de cette version incluent : • Protection contre l'utilisation d'un VPN en mode segmentation ajoutée à Mesures de protection supplémentaires sur la page 61.
Version 2	2021 R1	Les mises à jour de cette version incluent : • L'utilisateur basique est désormais couvert par le label transeuropéen pour la protection des données à caractère personnel (Appendice : Le système Milestone XProtect VMS et le RGPD sur la page 57) et (Appendice : Traitement des données dans l'environnement Milestone XProtect VMS sur la page 67). • Recommandations ajoutées à Utilisation des arrières-plans géographiques dans XProtect Smart Client sur la page 60. • Collecte de données décrite dans Intégrations des partenaires enregistrés sur la page 61. • Historique d'authentification décrit dans Données personnelles du système sur la page 67.
Version 1	2020 R3	Il s'agit de la première publication du présent document.

Table des matières

Copyright, marques et exclusions

Marques

XProtect est une marque déposée de Milestone Systems A/S.

Microsoft et Windows sont des marques déposées de Microsoft Corporation. App Store est une marque de service d'Apple Inc. Android est une marque de Google Inc.

Toutes les autres marques citées dans ce document sont des marques déposées de leurs propriétaires respectifs.

Exonération de responsabilité

Ce manuel est un document d'information générale et il a été réalisé avec le plus grand soin.

L'utilisateur assume tous les risques découlant de l'utilisation de ces informations. Aucun élément de ce manuel ne peut constituer une garantie d'aucune sorte, implicite ou explicite.

Milestone Systems A/S se réserve le droit d’effectuer des modifications sans préavis.

Les noms de personnes et d’institutions utilisés dans les exemples de ce document sont fictifs. Toute ressemblance avec des institutions ou des personnes réelles, existantes ou ayant existé, est purement fortuite et involontaire.

Ce produit peut utiliser des logiciels tiers pour lesquels des dispositions spécifiques peuvent s’appliquer. Dans ce cas, vous pouvez trouver plus d’informations dans le fichier 3rd_party_software_terms_and_conditions.txt situé dans le dossier d’installation de votre système Milestone.

Respect du RGPD et Milestone XProtect VMS

Le 25 mai 2018, le règlement général sur la protection des données (RGPD) est entré en vigueur. L'objectif de ce règlement fournit aux personnes plus de contrôle sur la collecte, le traitement et le partage de leurs données à caractère personnel.

Le RGPD fournit une structure pour les entreprises qui explicite leurs rôles et responsabilités et donne aux personnes la possibilité de contrôler l'utilisation des données à caractère personnel les concernant.

Ce document vous apporte un aperçu des exigences et explique comment travailler dans le respect du RGPD avec le système de gestion vidéo (VMS) XProtect.

Voir Appendice : Le système Milestone XProtect VMS et le RGPD sur la page 57 pour de plus amples informations sur comment un système Milestone XProtect VMS peut être encore plus conforme au RGPD.

Exonération de responsabilité : Les informations et recommandations du présent document sont données telles quelles. Le suivi de ce document ne garantie pas que votre système sera conforme au RGPD.

Le Milestone XProtect VMS nécessite une configuration. Toute configuration ou modification des paramètres doit respecter les lois en matière de protection des données de l'U.E. Même si la Appendice : Le système Milestone XProtect VMS et le RGPD sur la page 57 et la Mesures de protection supplémentaires sur la page 61 fournissent des informations sur comment démarrer une configuration conforme, vous devez vous référez aux lois concernant la protection des données de l'U.E. pour une configuration du système plus aboutie.

Définition du RGPD

Le Règlement général sur la protection des données (RGPD) contiennent un ensemble de règles qui régissent les données à caractère personnel sous toutes leurs formes détenues par une institution. Le RGPS octroie à toute personne le droit de propriété sur les données à caractère personne la concernant et, pour ce qui est des institutions, il présente leurs obligations à toutes les étapes du traitement et de la conservation des données. Le RGPD y parvient en attribuant un nombre de droits aux personnes concernées et en octroyant les obligations correspondantes aux institutions qui traitent les données à caractère personnel.

Le RGPD harmonise les lois concernant la confidentialité des données au sein de l'U.E., et s'ajoute aux règlements de CCTV et de vidéosurveillance nationaux existants.

> Le RGPD est un règlement de l'U.E., néanmoins il peut affecter d'autres pays du monde. Il s'applique au traitement de données à caractère personnel effectué par un responsable ou un sous-traitant au sein de l'Union européenne, que le traitement ait lieu ou non en son sein.
> Il s'applique au traitement de données à caractère personnel par un responsable ou un sous-traitant qui n'est pas établi au sein de l'Union européenne mais où les activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées au sein de l'Union européenne ou la surveillance de leur comportement si leur comportement ont lieu au sein de l'Union européenne.
> En outre, d'autres pays du monde appliquent des règlements en matière de protection de la vie privée similaires, basés sur les principes de base du RGPD.

Le RGPD est appliqué par les autorités nationales.

Sa violation génère de lourdes amendes :

- Jusqu'à 4 % du revenu annuel à l'échelle mondiale de l'entreprise
- Jusqu'à 20 millions d'euros par incident

Partie responsable de l'exécution du système de gestion vidéo XProtect en conformité avec le GDPR

Le propriétaire du VMS est responsable du bon respect des règles du RGPD, dont :

- Les installations actuelles et les utilisation appliquée
- Les processus organisationnels et ancienneté
- Notification en cas de violation de données et rapport aux autorités

Le RGPD ne s'applique pas à des produits spécifiques, mais à l'ensemble du produit, les données qu'il traite. L'utilisation du produit et des données ont une incidence sur la conformité du RGPD.

Le RGPD a des répercussions directes sur les installateurs, les intégrateurs de système et les utilisateurs de technologies de vidéosurveillance.

Le propriétaire du VMS constitue le responsable du traitement (voir Responsable du traitement sur la page 15).

Le responsable du traitement peut sous-traiter des parties ou l'intégralité des opérations du VMS à un sous-traitant de données, tel qu'une entreprise de sécurité. Dans ce cas, le responsable du traitement et le sous-traitant de données doivent mettre en place un *Accord de traitement des données*. L'*Accord de traitement des données* indique quelles sont les données traitées, comment elles sont traitées et leur durée de rétention (voir Sous-traitant de données sur la page 24 et Appendice : Accord de traitement des données sur la page 57).

Prérequis de conformité des installations de vidéosurveillance au RGPD

Le RGPD s'applique aux sous-traitant et aux responsables du traitement au sein de l'Union européenne, quel que soit l'endroit où est traité la vidéo.

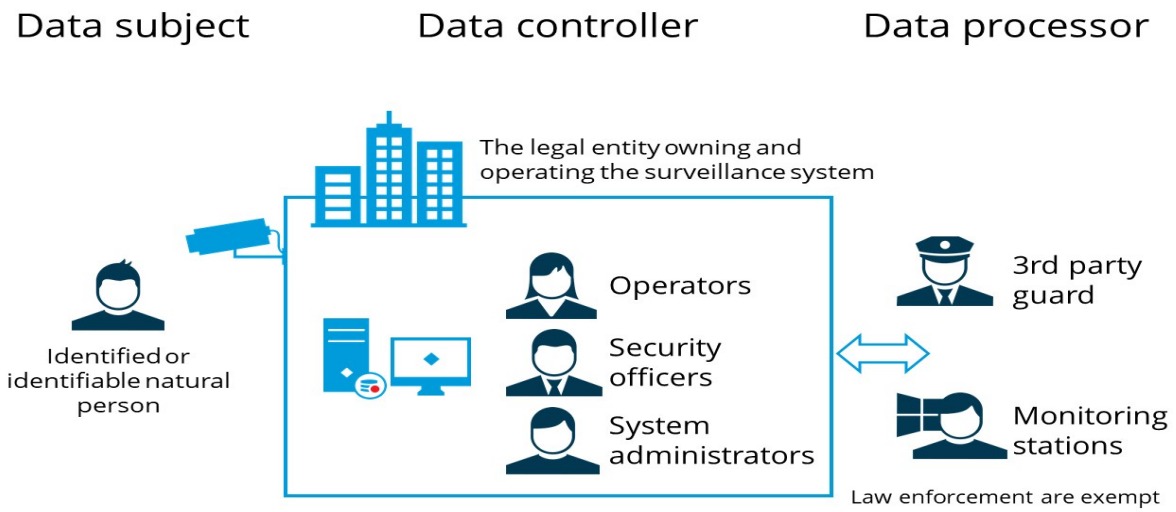
De plus, le RGPD protège la vie privée de toute personne résidant au sein de la zone géographique de l'Union européenne, couvre tous les types de vidéosurveillance au sein de l'Union européenne et protège les citoyens de tous les pays, qui résident au sein de l'Union européenne (article 3, RGPD).

Pour de plus amples informations sur le RGPD et notamment son implication dans la vidéosurveillance, voir Appendice : Conformité au RGPD sur la page 29.

Parties prenantes principales du RGPD en matière de vidéosurveillance

Trois types de parties prenantes dans le cas du RGPD et de la vidéosurveillance. Cette section définit chaque partie prenante et décrit leurs responsabilités respectives par rapport au RGPD.

- Personne concernée sur la page 10
- Responsable du traitement sur la page 15
- Sous-traitant de données sur la page 24



Personne concernée

Une personne concernée constitue toute personne dont les données à caractère personnel sont collectées, conservées et traitées.

Les personnes concernées sont les objets vus dans une vidéosurveillance, que ce soit intentionnel ou accidentel.

Les personnes concernées sont également toute personne enregistrée impliquée dans l'exécution du VMS, par exemple, les opérateurs et les gardes tiers désignés.

Le principal objectif du RGPD est de protéger les données à caractère personnel des personnes concernées.

Droits des personnes concernées

Les articles 12 à 23 du RGPD portent sur les droits des personnes concernées.

- Section 1 : Transparence et modalité
    - Article 12 : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée
- Section 2 : Informations et accès aux données à caractère personnel
    - Article 13 : Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée
    - Article 14 : Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée
    - Article 15 : Droit d'accès de la personne concernée (voir Droit d'accès sur la page 37)
- Section 3 : Rectification et effacement
    - Article 16 : Droit de rectification
    - Article 17 : Droit à l'oubli (droit à l'effacement) (voir Droit à l'oubli (droit à l'effacement) sur la page 38)
    - Article 18 : Droit à la limitation du traitement (voir Droit à la limitation du traitement sur la page 40)
    - Article 19 : Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement
    - Article 20 : Droit à la portabilité des données
- Section 4 : Droit d'opposition et décision individuelle automatisée
    - Article 21 : Droit d'opposition
    - Article 22 : Décision individuelle automatisée, y compris le profilage
- Section 5 : Limitations
    - Article 23 : Limitations

Parmi ces derniers, les droits les plus pertinents concernant la vidéosurveillance sont :

Le droit à l'information (Articles 12 à 14 et 34, RGPD)	L'article 12 traite de la transparence et des modalités, tandis que les articles 13 et 14 abordent les informations et l'accès aux données à caractère personnel. Ces articles accordent à la personne concernée le droit d'informations sur ses données à caractère personnel collectées et leur durée de rétention. Dans le cas du VMS, voir Appendice : Avis sur place sur la page 51. Larticle 34 accorde à la personne concernée le droit d'être informé en cas de violation des données si cette dernière peut représenter un risque élevé pour les droits et les libertés de la personne concernée.

Le droit d'accès (article 15, RGPD)	Ce droit accorde à la personne concernée la possibilité d'accéder à ses données à caractère personnel qui sont traitées, par exemple, les enregistrements vidéo de la personne concernée. La personne concernée a le droit de demander à une entreprise des informations sur quelles données à caractère personnel (le concernant) sont traitées et les raisons de ce traitement.
Droit à l'effacement (« droit à l'oubli ») (Article 17, RGPD)	Ce droit accorde à la personne concernée la possibilité de demander la suppression de ses données. Dans le cas d'un VMS, la suppression sur demande des personnes concernées est exceptionnelle en raison des raisons du responsable du traitement et des durées de rétention. (Voir Appendice : Politique de vidéosurveillance sur la page 52 et *Suppression partielle des enregistrements vidéo* dans Appendice : Le système Milestone XProtect VMS et le RGPD sur la page 57).
Le droit d'opposition (Article 21, RGPD)	Ce droit accorde à la personne concernée la possibilité de s'opposer au traitement de leur données à caractère personnel. Dans le cas d'un VMS, d'autres intérêts, telles que les intérêts légitimes (détection des fraudes, santé et sécurité, les obligations légales (comptabilité, blanchissement d'argent) ou même l'entrée en vigueur de contrats (contrats d'emploi) peuvent annuler les intérêts et droits de la personne concernée. Dans tous les cas, le traitement doit être entièrement transparent afin que la personne concernée puisse être informée et s'y opposer. Si la personne concernée s'oppose, le responsable du traitement doit examiner l'opposition. Dans le cas contraire, il pourrait être soumis à une amende.

Demande formulée par la personne concernée

Votre entreprise doit avoir un processus de traitement des demandes des personnes concernées, par exemple celle d'exercer son droit de demande d'accès. Ces demandes doivent être traitées dans les meilleurs délais. Conformément à l'article 12 (3) du RGPD, il est entendu "sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande." Il est recommandé d'avoir recours à un modèle de *Demande formulée par la personne concernée* pour enregistrer les demandes car elles peuvent être critiques dans l'application du RGPD avec des autorités nationales chargées de la protection des données. Pour un modèle d'exemple d'une demande de personne concernée, voir le modèle *Milestone Demande de personne concernée*.

La politique de la vidéosurveillance décrit la demande formulée par la personne concernée (voir Appendice : Politique de vidéosurveillance sur la page 52).

Défintion des données à caractère personnel

Afin d'être conforme au RGPD, vous devez avoir connaissance de la définition des données à caractère personnel et limiter la collecte des données au strictement nécessaire.

Conformément au règlement, les données à caractère personnel sont toute information se rapportant à une personne physique identifiée ou identifiable.

Une personne identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel que :

- Un nom
- Un numéro d'identification
- Données de localisation
- Un identifiant en ligne, par exemple une adresse IP ou un identificateur de cookies
- Des données d'utilisateur
- Des images vidéo
- Un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne

Les données à caractères personnel sont toute type d'information pouvant, directement ou indirectement, être utilisée pour identifier une personne physique (personne concernée). Il s'agit des données pouvant être utilisées pour identifier les objets vus de la vidéosurveillance, que les données soient collectées volontairement ou non.

Les données à caractère personnel protégées par le RGPD sont:

- Les données traitées par le produit informatique ou le service basée sur l'informatique (par exemple, nom et adresse d'une personne, image vidéo, informations de paiements, renseignements médicaux).
- Données qui sont involontairement produites lors de l'utilisation du produit ou service (par exemple, les données d'utilisation, les fichiers journaux, les données de statistiques, les données d'autorisation, les données de configuration). Ces données peuvent être des données à caractère personnel des utilisateurs du services, des données à caractère personnel des personnes exécutant le produit ou service (cela peut inclure le personnel du fournisseur du service et le personnel des utilisateurs du produit ou service) ou des données de configuration liée à la vie privée (voir Responsable du traitement sur la page 15).

Les données personnelles constituent toute information liée à une personne physique identifiée ou identifiable ou une personne concernée, par exemple :

• Nom complet	• Plaque d'immatriculation

• Adresse postale • Adresse e-mail • Numéro de téléphone • Données de localisation • Identité numérique	• Numéro du permis d'un conducteur • Numéros de carte bancaire • Informations identifiables, images, etc., telles que des enregistrements vidéo et des images statiques • Activités des utilisateurs, telles que celles figurant dans les fichiers journaux

Ces données ne sont pas forcément liée de manière directe uniquement à l'objet. Une donnée à caractère personnel peut également constituer un quasi-identificateur. Les quasi-identificateurs sont des éléments d'informations qui ne sont pas en soi des identifiants uniques, mais qui sont suffisamment corrélés à une information, ce qui permet de les utiliser avec d'autres quasi-identifiants pour créer un identifiant unique. Les quasi-identifiants sont particulièrement importants lorsqu'il s'agit de catégories spéciales de données à caractère personnel.

Les catégories spéciales de données incluent des données révélant l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l’appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle, par exemple :

• Antécédents médicaux • Données biométriques (dont les photos, vidéos et empreintes) • Casier judiciaire • Origine raciale ou ethnique	• Données génétiques • Opinions politiques et engagements • Convictions religieuses ou philosophiques • Orientation sexuelle et vie sexuelle

Ci-dessous les données à caractère personnel pouvant potentiellement être collectées par un système de vidéosurveillance :

Types de descriptions de données à caractère personnel conservées par XProtect qui relèvent du RGPD

Les données à caractères personnel sont toute type d'information pouvant, directement ou indirectement, être utilisée pour identifier une personne physique (personne concernée). Il peut s'agir de flux de vidéosurveillance, d'une seule image ou d'une séquence vidéo mêlée à d'autres informations d'emplacement des caméras et/ou des cartes à couche, d'une intégration de contrôle d'accès qui identifie une carte d'accès personnelle et qui l'unit à un emplacement spécifique, ou des données de la reconnaissance de plaques d'immatriculation (LPR) avec ou sans données d'emplacement.

Les catégories de vidéo à caractère personnel spéciales consistent en de la vidéosurveillance près des hôpitaux (liées à des informations médicales), des prisons (condamnation pénale), des activités politiques (appartenance syndicale), des activités religieuses ou des images qui révèlent l'orientation sexuelle (par exemple, des bars gays).

Les données à caractère personnel concernent également à l'activité des données d'utilisateurs (opérateur, superviseur et administrateur) et à la journalisation des activités. Cela inclut les journaux d'utilisateur personnels XProtect Smart Client, dont les horodatages de connexion et déconnexion et la journalisation des activités des flux vidéo, de l'audio et des métadonnées consultés, ainsi que la lecture et l'exportation d'enregistrements.

Voir Risques associés à l'utilisation d'un VMS sur la page 55 pour vous assurer de n'enfreindre aucun droit personnel.

Responsable du traitement

Dans ce cas de la vidéosurveillance, est entendu comme responsable du traitement toute personne possédant et exécutant des systèmes de vidéosurveillance. Le responsable du traitement est l'entité légale qui collecte, traite et partage des données des personnes concernées.

Responsabilités du responsable du traitements

Le responsable du traitement se doit de respecter les principes de protection des données ainsi que certaines obligations spécifiques. Le responsable du traitement doit mettre en place les mesures techniques et organisationnelles adéquates pour garantir et pouvoir démontrer que le traitement est conforme au RGPD. Cela inclut également :

- L'application et le maintien de politiques et procédures de sécurité de l'information pour protéger les données à caractère personnel. Ces politiques et processus doivent être approuvés au niveau le plus élevé au sein de l'institution et donc obligatoires pour les membres du personnel.
- Le maintien d'une vue d'ensemble des enregistrements des données à caractère personnel et des flux de traitement, par exemple via un registre des activités de traitement (Article 30, RGPD) et une liste des systèmes et archives qui traitent ces données à caractère personnel (le système XProtect VMS et d'autres systèmes qui retiennent des données à caractère personnel, tels que les dossiers du personnel, les accords de traitement des données, etc., y compris les informations sur comment et où les données à caractère personnel sont traités. Pour un modèle d'exemple d'un registre des activités de traitement, voir le modèle *Milestone Registre des activités de traitement*.
- La mise en place de mécanismes qui exécutent les politiques et processus internes, dont les procédures des réclamations, pour assurer l'efficacité de ces politiques dans la pratique. Cela inclut la création de campagne de sensibilisation sur la protection des données ainsi que des formations et instructions pour le personnel. Une formation de sensibilisation est disponible sur https://www.milestonesys.com/solutions/services/learning-and-performance/.
- La définition d'une politique de vidéosurveillance (voir Appendice : Politique de vidéosurveillance sur la page 52). La politique doit renvoyer aux lois nationales concernant la vidéosurveillance.
- La mise en œuvre d'analyses d'impact sur la protection des données, en particulier pour les opérations de traitement des données pouvant présenter des risques spécifiques sur les droits et libertés des personnes concernées, par exemple, du fait de leur nature, de leur portée ou de leur finalité (voir Appendice : Analyse d’impact relative à la protection des données sur la page 54).
- La garantie de la transparence de ces mesures adoptées pour les personnes concernées et le public en général. Les exigences en matière de transparence contribuent à l'obligation de rendre compte des responsables du traitement des données (par exemple, la publication des politiques de confidentialité sur internet, la transparence concernant les procédures de réclamations internes et la publication de rapports annuels).
- La publication de la notification du droit d'être informé au public (voir Appendice : Avis sur place sur la page 51). Cette notification informe les personnes concernées des finalités de la surveillance, de qui conserve les données collectées les concernant (responsable du traitement) et des politiques de rétention.
- L'assignation des responsabilités concernant la protection des données aux personnes qui sont directement responsables du bon respect des lois de protection des données de leur institution. En particulier, la désignation d'un délégué à la protection des données (DPD).

Délégué à la protection des données (DPD)

Chaque institution doit avoir un DPD désigné ou au moins une personne désignée responsable de la confidentialité.

Avant tout, les projets d'installation ou de mise à jour d'un système de vidéosurveillance doivent être communiqués au DPD.

Le DPD doit être consulté dans tous les cas et dans les plus brefs délais dans tous les cas liés à la protection des données à caractère personnel qui sont traités lorsque le service est fourni ou utilisé.

Le DPD doit être impliqué à toutes les étapes du processus décisionnel.

Les responsabilités du DPD incluent :

- Participer à la définition des finalités de la vidéosurveillance de l'entreprise, par exemple, la prévention de la criminalité, la détection de la fraude, la vérification de la qualité du produit ou de la santé et la sécurité du public, entre autres.
- Commenter le projet de politique de vidéosurveillance de l'institution, y compris ses annexes, (voir Appendice : Politique de vidéosurveillance sur la page 52), corriger les erreurs et proposer des améliorations
- Aider dans les communications avec les autorités nationales ou régionales de protection des données
- Réviser les accords avec les parties tierces lors du partage de données. Autrement dit, mettre à jour et gérer l'*accord du traitement des données* (voir Appendice : Accord de traitement des données sur la page 57)
- Élaborer des rapports de conformité et mener des audits pour obtenir une certification des parties tierces qui approuvent les mesures internes adoptées pour garantir que la conformité gère, protège et sécurise de manière efficace les données à caractère personnel
- Conserver et s'assurer que le registre des activités de traitement et les analyses d'impact de la protection des données (voir Appendice : Analyse d'impact relative à la protection des données sur la page 54) sont mises à jour à chaque changement important concernant la protection des données sur le VMS. Pour un modèle d'exemple d'un registre des activités de traitement, voir le modèle *Milestone Registre des activités de traitement*.

Rôles du responsable du traitement

La section ci-dessous décrit les responsabilités des responsables du traitement :

- Responsable de la sécurité (superviseur du VMS) sur la page 18
- Administrateur du système VMS sur la page 20
- Opérateur du VMS sur la page 20

Responsable de la sécurité (superviseur du VMS)

Les responsables de la sécurité ou superviseurs sont responsables de la mise en place d'un environnement conforme au RGPD. Les responsables de la sécurité doivent :

- Définir les autorisations utilisateur (voir Gestion des autorisations utilisateur sur la page 18)
- Mettre en place des formations de sensibilisation du personnel (voir Formation à la protection des données sur la page 19)
- Contacter le Délégué de la protection des données (DPD) en cas de suspicion de non-conformité au RGPD, par exemple, dans le cas d'une violation de données de matériels vidéo (voir Appendice : Conformité au RGPD sur la page 29)
- Appliquer et maintenir un haut niveau de sécurité globale. Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.

Gestion des autorisations utilisateur

Personnes autorisées à accéder au VMS

Les institutions doivent :

- Limiter l'accès des utilisateurs à un petit nombre de personnes clairement identifiées, sur la base du besoin de savoir.
- Maintenir des journaux d'activité de l'accès et des activités des utilisateurs.

Les autorisations d'accès doivent être limitées à un petit nombre d'individus clairement identifiés en cas de nécessité absolue. Assurez-vous que les utilisateurs autorisés peuvent accéder uniquement aux données auxquelles se réfèrent leurs autorisations d'accès. Des politiques de contrôle d'accès doivent être définies en suivant le principe du « moindre privilège » : les utilisateurs doivent avoir accès uniquement aux informations strictement nécessaires à l'exécution de leurs tâches.

En cas de partage d'un ordinateur, Milestone recommande que les opérateurs du VMS ne partagent pas leur compte de connexion à Windows. Chaque opérateur doit avoir un compte individuel.

En outre, les opérateurs du VMS ne doivent pas sélectionner l'option « Se souvenir de mon mot de passe » lorsqu'ils se connectent au système VMS.

Seul le responsable de la sécurité, l'administrateur du système ou les autres membres du personnel désignés expressément par le responsable de la sécurité doivent être habilités à accorder, modifier ou supprimer des autorisations d'accès de toutes les personnes. L'octroi, la modification et la suppression des autorisations d'accès doivent toujours se faire dans le respect des critères définis par la politique de vidéosurveillance (voir Appendice : Politique de vidéosurveillance sur la page 52).

Les personnes qui disposent d'autorisations d'accès doivent en tout temps être des individus clairement identifiables. Par exemple, aucun identifiant ou mot de passe générique ou courant ne doit être attribué à une entreprise de sécurité externalisée, qui emploie plusieurs personnes pour travailler pour l'institution.

La politique de vidéosurveillance doit spécifier et documenter clairement l'architecture technique du système de vidéosurveillance, qui a accès aux séquences de vidéosurveillance, la raison de cet accès et la nature précise des autorisations d'accès. Vous devez spécifier, plus particulièrement, qui dispose des autorisations pour :

• Visionner ou accéder à la vidéo en temps réel • Commander les caméras à balayage horizontal, vertical et zoom (PTZ) • Voir ou accéder à la vidéo enregistrée	• Exporter des enregistrements et des pistes de vérification • Supprimer ou effacer des périphériques (caméras) et supprimer les enregistrements • Modifier toute donnée après la configuration d'origine

En outre, vous devez vous assurer que ces permissions sont uniquement accordées pour les accès nécessaires aux fonctionnalités du VMS suivantes :

• Gérer le VMS • Créer/modifier/consulter/supprimer des signets • Créer/modifier/consulter/supprimer des protections des preuves • Enlever les masques de confidentialité • Exporter à des chemins définis (par exemple, exporter uniquement au format XProtect avec cryptage vers un lecteur partagé)	• Lire les journaux d'activité • Débuter/terminer un enregistrement • Créer/modifier/supprimer/activer/verrouiller/libérer les préréglages PTZ • Créer/modifier/supprimer/démarrer/arrêter les schémas de patrouille PTZ • L'audio, les métadonnées, les permissions E/S et des événements

Formation à la protection des données

L'ensemble du personnel ayant des autorisations d'accès, y compris le personnel extérieur qui effectue les opérations CCTV ou la maintenance du système journalières, doit recevoir une formation sur la protection des données et doit avoir connaissance des dispositions du RGPD dans la mesure où elles concernent leurs tâches.

La formation doit faire particulièrement attention au besoin d'empêcher la divulgation de la vidéosurveillance à quiconque ne constituant pas une personne autorisée.

La formation du personnel est essentielle est doit inclure :

- La cybersécurité
- L'exportation de données du VMS

Une formation doit être tenue lors de l'installation d'un nouveau système, lorsque des modifications importantes ont lieu sur le système, lorsqu'une nouvelle personne rejoint l'institution, ainsi qu'à intervalles réguliers par la suite. En ce qui concerne les systèmes existants, une formation initiale doit avoir lieu lors de la période de transition ainsi qu'à intervalles réguliers par la suite.

Pour de plus amples informations sur le RGPD de l'opérateur du VMS, voir le Milestone Guide de confidentialité du RGPD pour les opérateurs du VMS et la Milestone formation en ligne sur le RGPD pour les opérateurs du VMS.

Administrateur du système VMS

Les administrateurs de système sont responsables de la configuration d'un environnement de système conforme au RGPD. Les administrateurs de système sont en charge, entre autres, de :

- Appliquer et maintenir un haut niveau de sécurité globale. Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.
- Appliquer une politique de mot de passe sécurisé
- Mener des audits de sécurité
- S'assurer que les périphériques enregistrent selon les finalités définies, par exemple, sur événement, sur mouvement, de manière permanente, etc.
- S'assurer que la durée de rétention des enregistrements et des journaux d'activité est configuré conformément aux lois locales et aux finalités définies du VMS
- Garantir la gestion des utilisateurs (ajouter et supprimer des utilisateurs)
- S'assurer que les caméras suivent les lois sur la vie privée et qu'elles ne filment pas de zones qui ne doivent pas être enregistrées en appliquant des masques de confidentialité sur les zones concernées
- Contacter le Délégué de la protection des données (DPD) en cas de suspicion de non-conformité au RGPD, par exemple, dans le cas d'une violation de données de matériels vidéo (voir Appendice : Conformité au RGPD sur la page 29)

Opérateur du VMS

Les opérateurs du VMS doivent suivre les processus et les instructions de travail lorsqu'ils accèdent aux données dans le système, par exemple, lorsqu'ils visionnent de la vidéo ou qu'ils exportent de la vidéo, entre autres.

Afin d'être conformes au RGPD, les opérateurs doivent avoir :

- Une compréhension globale du RGPD et des règles en matière d'exportation des données
- Une formation sur le RGPD

  Les opérateurs doivent suivre une formation adéquate sur le système de vidéosurveillance pour s'assurer que la vie privée et d'autres droits fondamentaux des personnes concernées filmées par les caméras ne sont pas enfreints. Ils doivent avoir connaissance du contenu des politiques de vidéosurveillance (par exemple, les procédures écrites des preuves vidéo), savoir qui contacter en cas de doute (supérieur hiérarchique, tel que le Délégué du traitement des données), entre autres (voir Responsable de la sécurité (superviseur du VMS) sur la page 18).

  Pour de plus amples informations sur le RGPD de l'opérateur du VMS, voir le Milestone Guide de confidentialité du RGPD pour les opérateurs du VMS et la Milestone formation en ligne sur le RGPD pour les opérateurs du VMS.

Gestion des données exportées

L'exportation a lieu en cas d'incident qui requiert le partage de preuves avec les autorités. Si vous disposez des autorisations utilisateur pour exporter les preuves, vous êtes également responsable de leur gestion. Il s'agit d'une action particulièrement sensible en raison des consentements et du fait que les données partent du système de surveillance. La plupart du temps, il s'agit d'un incident qui implique une activité criminelle. La preuve peut contenir des informations privées sensibles. Lorsque vous les exportez, elle est généralement conservée sur un stockage amovible (clé USB, disque optique, etc.).

Si la donnée termine dans de mauvaises mains, la confidentialité de la vie privée des personnes concernées présentes dans la preuve pourrait être perdue.

Vous devez compter sur un processus clair pour l'exportation de preuves, qui couvre :

- Qui peut exporter la preuve ?
- Où la preuve est-elle conservée en attendant son transfert vers les autorités ?
- Les personnes ayant accès
- Le ou les formats à utiliser
- Le cryptage doit-il être appliqué (hautement recommandé) ?
- Quand la preuve est-elle détruite ?

Les responsables du traitement doivent prendre de mesures techniques et organisationnelles pour protéger les données qui ne sont plus du ressort du Milestone XProtect VMS. Ces mesures peuvent être :

- Limiter la permission d'exporter des vidéos et des journaux d'activité à un personnel spécifique uniquement
- Considérer le cryptage des données avant ou après l'exportation
- Appliquer des masques de confidentialité avant l'exportation de donnée vidéo, si besoin
- Protéger physiquement les médias amovibles contenant des données à caractère personnel

- Établir des politiques qui assurent que les données à caractère personnel sont supprimées des médias conformément à la durée de rétention
- Maintenir un registre des médias amovibles : qui a exporté quelle donnée vers le média ? À qui a-t-elle été envoyée et à quelle fin ? Le destinataire est-il informé de détruire le média ou de le retourner une fois la finalité atteinte ? Etc.
- Utiliser les politiques de groupe de Windows pour désactiver les ports USB ou l'accès aux médias sur les PC des clients
- Surveiller les journaux d'activité à la recherche d'événements d'exportation non autorisés
- Engager les employés sur la politique de protection des données
- Effacer les médias ou les détruire physiquement si l'effacement n'est pas possible (par exemple, les DVD)

Voir la Milestone formation au RGPD pour les opérateurs du VMS pour de plus amples informations sur la gestion des exportations de données.

Gestion des données exportées dans les notifications et courriers électroniques

Outre les exportations, les données peuvent également être extraites du VMS par le biais de pièces-joints aux notifications. Les notifications sont des courriers électroniques envoyés à une adresse électronique spécifique. Lors de la création d'une notification, l'administrateur peut choisir d'inclure un ensemble de captures d'écran ou un AVI d'une séquence. Étant donné que les captures d'écran et les séquences AVI jointes aux notifications partent du VMS, elles se retrouvent hors du contrôle du VMS concernant l'accès utilisateur et la conservation. Il est recommandé de ne pas joindre d'images ou de séquences AVI aux notifications par courrier électroniques. Si les pièces-jointes sont nécessaires, vous devez au moins vous assurer de la mise en place de procédures et contrôles organisationnels de la part des destinataires des courriers électroniques et s'informer sur leur gestion.

Vous devez compter sur un processus clair, qui couvre :

- L’endroit où les données sont stockées

  Assurez-vous que les serveurs qui envoient et reçoivent des courriers électroniques sont sous le contrôle de l'institution du responsable du traitement ou sous-traitant des données de la vidéosurveillance. En particulier, les destinataires ne doivent pas posséder de messageries électroniques sur des messageries gratuites, telles que Gmail ou Hotmail, entre autres.
- Les personnes ayant accès
- Le ou les formats à utiliser

- L'application du cryptage SMTP

  Remarque : Utilisez un serveur de messagerie SMTP/SMTPS. Vous devez crypter la connexion entre le VMS et les serveurs de messagerie externalisés, ainsi qu'entre les serveurs SMTP d'envoi et de réception pour recevoir le label transeuropéen pour la protection des données. Une connexion non-cryptée et non-sécurisée enfreint le label européen de protection des données à caractère personnel et provoque la non-conformité au label européen de protection des données à caractère personnel.

- Délai de destruction de la preuve

  Milestone recommande d'aligner la durée de rétention des données vidéo des messageries électroniques entrantes et sortantes sur la durée de rétention de la base de données des médias ou sur la durée de rétention des alarmes qui peuvent être déclenchées par les mêmes événements que ceux ayant causé la notification.

  La durée de rétention des messageries électroniques doit avoir une limite raisonnable pour la finalité du processus de notification.

  Milestone recommande d'utiliser uniquement les messages électroniques du responsable du traitement ou du sous-traitant des données et de configurer la suppression automatique des courriers électroniques une fois atteint la durée de rétention.

  Les responsables du traitement/sous-traitants des données doivent s'assurer que ces messageries électroniques ne sont pas automatiquement archivées par le système de message électronique.

Violation de données à caractère personnel

Le RGPD définit une « violation de données personnelles » comme étant « une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière. »

Dans le cas d'une violation des données, le DPD doit décider de notifier ou non l'Autorité de protection des données et les personnes concernées impliquées, conformément aux articles 33 et 34 du RGPD.

Conformément à l'article 33 (1) du RGPD :

> *En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.*

Si cela est jugé nécessaire, le responsable doit publier une notification de violation des données 72 au plus tard après avoir en avoir pris connaissance (voir Violation de données à caractère personnel sur la page 23). Pour un modèle d'exemple d'une notification de violation des données, voir le modèle *Milestone Notification de*

violation des données. Les personnes concernées doivent également être notifiées si la violation des données à caractère personnel « est susceptible de provoquer un risque élevé pour les droits et libertés des personnes concernées. »

Les sous-traitant de données qui font face à une violation des données à caractère personnel doivent notifier le responsable du traitement, mais autrement, ils n'ont aucune autre obligation de notification ou rapport conformément au RGPD.

Pour de plus amples informations sur les autres responsabilités du DPD, voir Responsable du traitement sur la page 15.

Sous-traitant de données

Si une entreprise sous-traite toutes ou une parties de ses activités de vidéosurveillance à un tiers (un traitement de données), elle demeure responsable du respect du RGPD en tant que contrôleur de données. Par exemple, les gardes de la sécurité en charge de la surveillance vidéo en direct dans la zone de réception d'une institution travaillant pour une entreprise privée avec laquelle l'institution sous-traite la tâche de la surveillance en direct. Dans ce cas, l'institution doit s'assure que les gardes de la sécurité réalisent leurs activités conformément au RGPD.

Pour être conformes au RGPD, les responsables du traitement tiers (à l'exception de l'application des lois) doivent :

- Respecter les mêmes exigences que l'opérateur (voir Opérateur du VMS sur la page 20)
- Singer et respecter un *Accord de traitement des données* (voir Appendice : Accord de traitement des données sur la page 57).

Résumé

Le RGPD est une règlement qui gouverne déjà la gestion des données, y compris les données vidéo, des institutions.

Au minimum, chaque institution qui traite des données à caractère personnel doit désigner une ou plusieurs personnes responsables de garantir une gestion des données à caractère personnel conforme au RGPD et aux politiques de l'entreprise (le nombre de heures de main d'œuvre affectées variera en fonction de la taille de l'institution et de la quantité de données à caractère personnel collectées et traitées). En outre, pour certaines institutions, le RGPD exigera la désignation d'un délégué à la protection des données pour exécuter ces tâches.

Des changements auront également lieu au niveau du processus administratif. Conformément au RGPD, les institutions doivent posséder un *Rapport des activités de traitement des données* détaillé et précis. Pour un modèle d'exemple d'un registre des activités de traitement, voir le modèle *Milestone Registre des activités de traitement*. Un éventail d'informations doit être enregistré, dont, entre autres :

- À quelle catégorie de personnes les données à caractère personnel appartiennent-elles (par exemple, les clientes, employés, visiteurs des magasins, etc.)
- À quelles fins les données à caractère personne sont-elles utilisées
- Si les données à caractère personnel vont être transférées (à d'autres entreprises et/ou en dehors de l'U.E.)
- La durée de rétention des données à caractère personnel
- Les mesures prises par l'institution par rapport à chaque activité du traitement des données afin de garantir la conformité au RGPD

Ces informations sont importantes concernant la conservation de la vidéosurveillance et elles sont définies dans la politique de la vidéosurveillance (voir Appendice : Politique de vidéosurveillance sur la page 52).

Les institutions ont l'obligation d'expliquer l'emplacement des caméras vidéo ainsi que ce qu'elles filment et à quelle fin. Dans le cas de la de vidéosurveillance, une signalisation appropriée dans et autour de la zone où est utilisée la vidéosurveillance doit être utilisées pour fournir ces informations.

Le responsable du traitement peut avoir l'obligation de mener une analyse d'impact sur la protection des données (voir Appendice : Analyse d'impact relative à la protection des données sur la page 54) lors de la configuration d'une caméra dans un lieu public. Une analyse d'impact doit inclure :

- Une description systématique des opérations de traitement prévues et les finalités de ce traitement
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités (cela peut nécessiter une aide extérieure)
- Une évaluation des risques pour les droits et libertés des personnes concernées
- Les mesures envisagées pour faire face aux risques, y compris les garanties et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et le bon respect du RGPD (compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées)

Un des éléments principaux du RGPD est que les personnes sous surveillance doivent être entièrement informées des données conservées les concernant ainsi que de leur utilisation. Le droit à l'information informe les personnes concernées : des finalités de la surveillance, de qui conserve les données collectées les concernant (responsable du traitement / sous-traitant de données) et des politiques de rétention. Pour un modèle d'exemple d'une notification d'avis sur place, voir le modèle *Milestone Avis sur place*.

Les institutions qui conservent de la vidéo ont des responsabilités claires concernant la conservation de données à caractère personnel et doivent mettre en place des mesures fortes pour empêcher tout accès non autorisé. En d'autres termes, il est important de définir, par écrit, qui a accès aux caméras et aux enregistrements.

Les institutions doivent également mettre en place une procédure pour les cas où une personne concernée choisit d'exercer son droit d'accès aux données à caractère personnel ou demande leur suppression. Cela leur permettra de rester dans la fenêtre d'un mois au cours de laquelle elles doivent respecter ces demandes conformément au RGPD. Lors d'une requête, il est raisonnable d'attendre le demandeur que le demandeur fournisse les informations nécessaires à la localisation des données, par exemple, une période de temps approximative et un emplacement où a été capturée la vidéo. Autrement dit, la personne concernée doit fournir la preuve de leur identité avec des papiers d'identité officiels et l'institution doit enregistrer les enregistrements dévoilés ou fournis à la personne concernée. De plus, les autres personnes figurant sur la vidéo doivent être masquées par le biais d'outils tiers.

Les institutions doivent utiliser des mesures fortes pour empêcher tout accès non autorisé aux données à caractère personnel conservées. Les tactiques utilisées par chaque institution seront spécifiques aux problèmes qu'elles affrontent. Cependant, dans toutes les instances, les institutions doivent employer des contrôles de sécurité robustes, rester à jour avec les meilleures pratiques de cybersécurité et garantir qu'elles travaillent avec des partenaires de confiance, qui fournissent du matériel et des logiciels sécurisés ainsi qu'un suivi rigoureux.

Gestion des données à caractère personnel

La gestion des données à caractère personnel implique les principes suivants :

- Accès : Avoir connaissance des informations à caractère personnel conservées dans vos fichiers et sur vos ordinateurs.
- Minimisation : Conserver uniquement le nécessaire pour votre entreprise.
- Protection : Protéger les informations conservées.
- Suppression : Effacer ce qui n'est plus nécessaire.
- Réponse : Rapporter immédiatement les failles de sécurité actuelles ou suspectées.

Pour plus d'informations

- Pour la version complète du *Règlement général sur la protection des données*
- Pour de plus amples informations sur le RGPD de l'opérateur du VMS, voir le Milestone Guide de confidentialité du RGPD pour les opérateurs du VMS et la Milestone formation en ligne sur le RGPD pour les opérateurs du VMS.
- Pour rester à jour et en savoir plus sur les développement du RGPD, rendez-vous sur le site Web de la Commission européenne sur la protection des données
- Pour un guide du RGPD qui aide les institutions à respecter ses prérequis, voir le Guide du Bureau du commissaire à l'information du Règlement général sur la protection des données du R.U.
- Pour une liste des principaux éléments du RGPD, voir *Principaux éléments du Règlement général sur la protection des données*
- Pour des recommandations des institutions et organismes européens sur la conception et l'exécution des systèmes de vidéosurveillance, voir les *lignes directrices sur le Contrôleur européen de la protection des données (CEPD)*
- Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.
- Pour plus d'informations sur comment les composants du Milestone XProtect VMS intéragissent, voir le document Milestone qui décrit l'architecture du système.

Milestone Modèles du RGPD

- Modèle *Avis sur place Milestone*.
- Modèle *Rapport sur les activités de traitement Milestone*.
- *Modèle Milestone Politique de la vidéosurveillance*.

> Vous devez obéir aux exigences du RGPD pour la configuration et le développement de la politique de la vidéosurveillance. Veuillez remarquer que la collecte d'audio et de métadonnées n'est pas prise en charge par le label transeuropéen pour la protection des données (EuroPriSe).

- *Milestone Modèle Accord de traitement des données*
- *Modèle d'une Demande d'une personne concernée Milestone*.

> Veuillez remarquer qu'il s'agit uniquement d'un exemple. Aucune demande officielle de demande d'une personne concernée n'existe.

- *Modèle Notification d'une violation de données Milestone*.

Appendices

Pour de plus amples informations, voir les sections suivantes :

Appendice : Conformité au RGPD

Cette section présente un aperçu des réglementations du RGPD concernant la vidéosurveillance. Elle définit le RGPD et décrit son impact sur l'utilisation de la vidéosurveillance dans les section suivantes :

- Existe-t-il une base légale justifiant la collecte des données ? sur la page 29
- Droits des personnes sur la page 35
- Protection des données dès la conception sur la page 41
- Responsabilité sur la page 48
- Liste récapitulative pour la garantie de l'intégrité et de la confidentialité sur la page 50

Existe-t-il une base légale justifiant la collecte des données ?

Le RGPD exige que toutes les institutions s'appuient sur une base légale valide pour collecter et traiter des données à caractère personnel.

La vidéosurveillance effectuée sur la base d'un consentement ou d'intérêts vitaux peut être possible dans des situations exceptionnelles, telles que dans le secteur de la santé si une personne doit être surveillée en permanence.

Il est exigé de tenir un registre des activités de traitement dans un *Registre des activités de traitement* (Article 30, RGPD). Pour un modèle d'exemple d'un registre des activités de traitement, voir le modèle *Milestone Registre des activités de traitement*.

Vérifier la légitimité du traitement des données vidéo et des données des utilisateurs conformément aux niveaux de réglementation suivants :

1. Réglementation pour la protection des données à caractère général (Article 6, RGPD)

   Notamment l'article 6 (1)(b) du RGPD :

   > *Le traitement est nécessaire à l'exécution d'un **contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.*

   Et l'article 6 (1)(e)(f) du RGPD :

   > *Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, **notamment lorsque la personne concernée est un enfant**.*

2. Application de la Directive (UE) 2016/680 ou droit national basé sur cette directive

   Respect du droit national basé sur la l'application de la Directive (UE) 2016/680 pour établir une base légale pour vérifier la légitimité du traitement.

3. Droit national

   Respect du droit national, par exemple, la Section 4 de la loi fédérale sur la protection des données (BDSG), même si cette disposition ne s'applique pas à la vidéosurveillance menée par les entreprises.

Avant de mettre en place de la vidéosurveillance, évaluez les avantages potentiels ainsi que l'impact relatif à la protection des données et autres droits fondamentaux et les intérêts légitimes de ces derniers dans la zone couverte.

Lorsque vous décidez d'avoir recours à la vidéosurveillance, documentez les fins du système vidéo, les informations collectées, pour quoi elles seront utilisées, par qui, pour combien de temps et fournissez les preuves à l'appui adéquates, telles que des données statistiques sur le nombre d'accidents de la sécurité qui se sont produits, ainsi que des preuves de l'efficacité passée des caméras pour prévenir, empêcher, enquêter ou poursuivre en justice ces accidents.

L'étendue de l'évaluation varie en fonction de la taille du système proposé et son impact sur la protection des données et autres intérêts légitimes ou sur les droits fondamentaux.

Traitement basé sur une obligation légale ou une mission d'intérêt public

Quand la base juridique des obligations légales s'applique-t-elle ? En résumé, lorsque vous êtes obligé de traiter des données à caractère personnel pour respecter la loi. L'article 6 (3) du RGPD déclare que l'obligation juridique doit être définie par le droit de l'UE ou le droit de l'État membre.

Cela ne signifie pas qu'une obligation juridique doit exiger de manière expresse l'activité de traitement en question. Le fait est que votre finalité générale doit être de respecter une obligation juridique ayant une base suffisamment claire provenant du droit commun ou de la loi écrite. Par exemple, une ordonnance de tribunal peut vous demander de traiter des données à caractère personnel pour une fin spécifique, ce qui constitue une obligation juridique.

En général, les institutions publiques utilisent la vidéosurveillance pour exécuter des tâches d'intérêt public. Veuillez noter que la mise en balance des intérêts ne constitue pas une base légale pour les autorités publiques dans l'exécution de ces tâches.

Pour les institutions publiques, la vidéosurveillance est uniquement légitime si elle est nécessaire à l'exécution d'une tâche d'intérêt public. Lorsque vous exécutez une tâche d'intérêt public, vous devez mener une appréciation de la proportionnalité (voir Mise en balance des intérêts/appréciation de la proportionnalité sur la page 31). Le responsable du traitement doit prendre en compte les principes de minimisation des données (par exemple, le masquage de confidentialité), limitation de la conservation (la durée de rétention) et de limitation des finalités (article 5 (1), RGPD).

Mise en balance des intérêts/appréciation de la proportionnalité

En général, les organismes privées exécute un VMS aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (article 6 (1)(f), RGPD). Une mise en balance des intérêts est donc nécessaire pour vérifier la légitimité du traitement. Le responsable du traitement a besoin d'identifier et d'évaluer ses intérêts en comparaison aux intérêts ou droits fondamentaux et libertés des personnes concernées, qui requièrent la protection de leurs données à caractère personnel.

En général, le traitement des données sur l'historique des audits et des alarmes peut se baser sur des intérêts légitimes du responsable du traitement (article 6 (1)(f), RGPD). Il en va de même pour les données de gestion des utilisateurs (données du compte, identifiant d'authentification, données d'autorisation, données de configuration) si l'utilisateur est un employé d'une entreprise de sécurité.

Dès le début, vous devez être honnête et ouvert avec les personnes concernant votre utilisation de leurs données à caractère personnel. Lors de votre analyse, répondez les questions suivantes :

- Quels sont les avantages de l'utilisation de la vidéosurveillance ? Ces bénéfices l'emportent-ils sur les effets négatifs ?
- La finalité du système est-elle clairement précisée, explicite et légitime ? Existe-t-il une légitimation de la vidéosurveillance ?
- Le besoin de l'utilisation de la vidéosurveillance est-il clairement démontré ? S'agit-il d'un outil efficace dans l'atteinte de ses objectifs poursuivis ? Existe-t-il des alternatives plus discrètes ?

En outre, le responsable du traitement peut utiliser les données à caractère personnel pour une nouvelle finalité uniquement si celle-ci est compatible avec l'objectif initial, s'il obtient le consentement ou s'il s'appuie sur une base juridique claire.

Intérêts caractéristiques du responsable du traitement

Habituellement, le responsable du traitement :

- Exerce son droit de déterminer qui peut être se voir autoriser ou renier l'accès aux données
- Protège des intérêts légitimes à des fins bien définies

Dans le cadre des relations de travail, le responsable du traitement doit être informé que le traitement des données à caractères personnel des employés (données vidéo et données des utilisateurs) dans le cadre des relations de travail peuvent être soumises à des règles plus spécifiques du droit des États membres (Article 88, RGPD), par exemple Section 26 BDSG (Allemage).

Intérêts caractéristiques et droits des personnes concernées

Les personnes concernées ont le droit à :

- Aucune surveillance à long terme
- Aucune surveillance dans des situations intimes
- Une durée de rétention brève
- Des protections adéquates sur le traitement portant sur des catégories particulières de données à caractère personnel (article 9, RGPD)

Comment XProtect réduit l'impact sur les intérêts ou les droits fondamentaux et les libertés des personnes concernées

Milestone XProtect réduit l'impact sur les intérêts et les droits fondamentaux et libertés des personnes concernées grâce à :

- La protection des données à caractère personnel avec :
  - Le contrôle d'accès basé sur les rôles
    - Supervision uniquement sur les masques de confidentialité amovibles
    - Journalisation des accès
  - Cryptage des enregistrements
  - Chiffrement de toutes les communications entre les serveurs et les clients XProtect VMS
  - Conservation de la vidéo automatique (suppression automatique)
  - Masquage de confidentialité
  - Exportation de la vidéo sécurisée et vérifiable
- Cybersécurité
  - Durcissement du système. Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.
  - Rapport et correction des vulnérabilités connues. Pour plus d'informations, voir Rapport et correction des vulnérabilités connues.
- Éducation et sensibilisation
  - Programmes de certification pour nos partenaires
  - Programmes de certification sur les produits de nos partenaires (voir Milestone Programme partenaire technologique et Milestone Marketplace)
  - Milestone Formation en ligne sur le RGPD pour les opérateurs de VMS

Transferts et divulgations

Le RGPD définit trois grandes règles concernant les transferts en fonctions de si les enregistrements sont transférés vers :

- Un destinataire au sein de l'institution ou vers une autre institution

  Dans ce cas, le RGPD prévoit que les enregistrements peuvent faire l'objet d'un transfert à des tiers au sein de l'institution ou vers une autre institution si ce transfert est nécessaire à l'exécution légitime de missions relevant de la compétence du destinataire.

- Des destinataires à l'intérieur de l'Union européenne

  Dans ce cas (transfert en dehors des institutions mais à l'intérieur de l'Union européenne), ce transfert est possible s'il est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou si le destinataire démontre la nécessité du transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes des personnes dont les images sont transférées.

- Ou vers l'extérieur de l'Union européenne

  Dans ce cas, le transfert en dehors de l'Union européenne est possible : (1) s'il a pour seul objectif de permettre l'exécution de la mission de l'institution et (ii) moyennant le respect de conditions supplémentaires visant principalement à garantir la protection adéquate des données à l'étranger.

Résumé

Assurez-vous que votre utilisation des données ne viole aucune loi.

Vous devez utiliser les données à caractère personnel de manière équitable. En d'autres termes, vous ne devez pas traiter les données de manière préjudiciable, inattendue ou pouvant nuire aux personnes concernées.

Vous pouvez utiliser les données à caractère personnel pour une nouvelle finalité uniquement si celle-ci est compatible avec votre objectif initial, si vous obtenez un consentement ou si vous vous appuyez sur une base juridique claire.

Dans les cas pouvant constituer un risque élevé d'empiéter sur la vie privée, vous devez mener une analyse d'impact officielle (voir Appendice : Analyse d'impact relative à la protection des données sur la page 54).

Mener une analyse d'impact

Avant d'installer et de mettre un place des systèmes de vidéosurveillance, vous devez mener une *analyse d'impact relative à la protection des données* et de la vie privée.

L'objectif d'une analyse de l'impact des opérations de traitement est de déterminer l'impact du système proposé sur la protection de la vie privée et d'autres droits fondamentaux des individus et d'identifier des mesures pour diminuer ou éviter des effets négatifs.

Quels doivent-être les efforts déployés dans l'analyse d'impact ? Tout dépend des circonstances. Un système de vidéosurveillance présentant un risque élevé d'empiéter sur la vie privée justifie d'un plus grand investissement qu'un système de vidéosurveillance avec un impact limité sur la vie privée, tel qu'un système CCTV statique conventionnel.

Conformément à l'article 35 (7) du RGPD, l'analyse doit au moins contenir :

- Une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités

- Une évaluation des risques pour les droits et libertés des personnes concernées conformément à l'article 35 (1) du RGPD :

  Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées

Quoi qu'il en soit et dans tous les cas, vous devez évaluer et justifier la nécessité de recourir à de la vidéosurveillance, comment placer les caméras, sélectionner et configurer les systèmes et comment mettre en place les mesures de protection des données requises. Pour plus d'informations sur la sécurité de vos installations XProtect VMS, voir le guide de durcissement et le guide des certificats.

Droits des personnes

L'un des principaux objectifs du RGPD est d'offrir aux personnes une plus grande protection et un ensemble de droits gouvernant leurs données à caractère personnel.

Les dispositions du règlement définissent des exigences très spécifiques, le tout décrétant qu'il incombe aux parties qui traitent ou stockent des données à caractère personnel de les protéger.

Le RGPD octroie aux personnes le droit de savoir quand leurs données à caractère personnel sont collectées (au moment de la collecte) et comment elles sont utilisées. Par exemple, dans le cas de la vidéosurveillance, il s'agit d'une signalisation appropriée dans et autour de la zone où est utilisée la vidéosurveillance.

Les articles12 à 23 du RGPD portent sur les droits des personnes concernées.

- Section 1 : Transparence et modalité
  - Article 12 : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée
- Section 2 : Informations et accès aux données à caractère personnel
  - Article 13 : Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée
  - Article 14 : Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée
  - Article 15 : Droit d'accès de la personne concernée (voir Droit d'accès sur la page 37)

- Section 3 : Rectification et effacement
  - Article 16 : Droit de rectification
  - Article 17 : Droit à l'oubli (droit à l'effacement) (voir Droit à l'oubli (droit à l'effacement) sur la page 38)
  - Article 18 : Droit à la limitation du traitement (voir Droit à la limitation du traitement sur la page 40)
  - Article 19 : Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement
  - Article 20 : Droit à la portabilité des données
- Section 4 : Droit d'opposition et décision individuelle automatisée
  - Article 21 : Droit d'opposition
  - Article 22 : Décision individuelle automatisée, y compris le profilage
- Section 5 : Limitations
  - Article 23 : Limitations

Parmi ces derniers, les droits les plus pertinents concernant la vidéosurveillance sont :

Le droit à l'information (Articles 12 à 14 et 34, RGPD)	L'article 12 traite de la transparence et des modalités, tandis que les articles 13 et 14 abordent les informations et l'accès aux données à caractère personnel. Ces articles accordent à la personne concernée le droit d'informations sur ses données à caractère personnel collectées et leur durée de rétention. Dans le cas du VMS, voir Appendice : Avis sur place sur la page 51. Larticle 34 accorde à la personne concernée le droit d'être informé en cas de violation des données si cette dernière peut représenter un risque élevé pour les droits et les libertés de la personne concernée.
Le droit d'accès (article 15, RGPD)	Ce droit accorde à la personne concernée la possibilité d'accéder à ses données à caractère personnel qui sont traitées, par exemple, les enregistrements vidéo de la personne concernée. La personne concernée a le droit de demander à une entreprise des informations sur quelles données à caractère personnel (le concernant) sont traitées et les raisons de ce traitement.
Droit à l'effacement (« droit à l'oubli »)	Ce droit accorde à la personne concernée la possibilité de demander la suppression de ses données. Dans le cas d'un VMS, la suppression sur demande des personnes concernées est exceptionnelle en raison des raisons du responsable du traitement et

(Article 17, RGPD)	des durées de rétention. (Voir Appendice : Politique de vidéosurveillance sur la page 52 et *Suppression partielle des enregistrements vidéo* dans Appendice : Le système Milestone XProtect VMS et le RGPD sur la page 57).
Le droit d'opposition (Article 21, RGPD)	Ce droit accorde à la personne concernée la possibilité de s'opposer au traitement de leur données à caractère personnel. Dans le cas d'un VMS, d'autres intérêts, telles que les intérêts légitimes (détection des fraudes, santé et sécurité, les obligations légales (comptabilité, blanchissement d'argent) ou même l'entrée en vigueur de contrats (contrats d'emploi) peuvent annuler les intérêts et droits de la personne concernée. Dans tous les cas, le traitement doit être entièrement transparent afin que la personne concernée puisse être informée et s'y opposer. Si la personne concernée s'oppose, le responsable du traitement doit examiner l'opposition. Dans le cas contraire, il pourrait être soumis à une amende.

Trois droits sont particulièrement pertinents pour la conformité des systèmes VMS au RGPD : le droit à l'information, le droit d'accès et le droit à l'effacement.

Droit d'accès

L'article 15 du RGPD confère aux personnes concernées le contrôle sur leurs données à caractère personnel, y compris le droit d'accéder à leurs données. Un élément particulièrement important est le droit des personnes concernées d'obtenir une copie de leurs données et que les personnes tierces sont masquées (via des outils tiers).

Sur demande, les institutions doivent fournir à la personne concernée toutes les données à caractère personnel la concernant, y compris la vidéo collectée par un système de vidéosurveillance.

Assurez-vous d'établir les procédures et politiques officielles pour la gestion des demandes du droit d'accès, décrites dans *Registre des transferts et divulgations* .

Transferts et divulgations

Le RGPD définit trois grandes règles concernant les transferts en fonctions de si les enregistrements sont transférés vers :

- Un destinataire au sein de l'institution ou vers une autre institution

  Dans ce cas, le RGPD prévoit que les enregistrements peuvent faire l'objet d'un transfert à des tiers au sein de l'institution ou vers une autre institution si ce transfert est nécessaire à l'exécution légitime de missions relevant de la compétence du destinataire.

- Des destinataires à l'intérieur de l'Union européenne

  Dans ce cas (transfert en dehors des institutions mais à l'intérieur de l'Union européenne), ce transfert est possible s'il est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public ou relevant de l'exercice de l'autorité publique, ou si le destinataire démontre la nécessité du transfert et s'il n'existe aucune raison de penser que ce transfert pourrait porter atteinte aux intérêts légitimes des personnes dont les images sont transférées.

- Ou vers l'extérieur de l'Union européenne

  Dans ce cas, le transfert en dehors de l'Union européenne est possible : (1) s'il a pour seul objectif de permettre l'exécution de la mission de l'institution et (ii) moyennant le respect de conditions supplémentaires visant principalement à garantir la protection adéquate des données à l'étranger.

Registre des transferts et divulgations

Les institutions doivent maintenir un registre, dans la mesure du possible, au format électronique, des transferts et divulgations. Chaque transfert vers un tiers doit y être inscrit. (toute personne au sein de l'institution vers qui un transfert a lieu par ceux ayant accès aux enregistrements en premier lieu est également considérée comme un tiers. En général, cela inclut tout transfert en dehors de l'unité de sécurité.) En outre, le registre doit contenir toutes les instances dans lesquelles des tiers ont eu accès aux enregistrements ou lorsque le contenu des enregistrements a été divulgué de quelque façon que ce soit à des tiers et ce, même si la copie de l'enregistrement de la vidéosurveillance n'a pas été transférée.

Le registre doit au moins contenir ce qui suit :

- La date des enregistrements
- La partie requérante (nom, titre et institution)
- Le nom et le titre de la personne qui autorise le transfert
- Une brève description du contenu des enregistrements
- Le motif de la demande et le motif de l'accord
- Si une copie de l'enregistrement a été transférée, l'enregistrement a été montré ou si des informations orales ont été données

Droit à l'oubli (droit à l'effacement)

L'article 17 du RGPD confère aux personnes concernées le contrôle sur leurs données à caractère personnel, y compris le droit d'obtenir l'effacement de leurs données à caractère personnel si elles ne sont plus nécessaires au regard des finalités du système.

Conformément à l'article 17 (1)(c) du RGPD, le responsable du traitement doit répondre aux objections des personnes concernées. Étant donné la difficulté d'effacer d'une vidéo une personne concernée spécifique, les responsables du traitement doivent limiter le plus possible la durée de rétention de la vidéo conformément aux finalités documentées du système.

Procédure

Consultez la durée de rétention de toutes les caméras et assurez-vous de la configurer conformément aux finalités documentées du système.

Le droit d'être oublié s'applique peu à la vidéosurveillance étant donné que la durée de rétention est en général courte et que d'autres bases juridiques annule les intérêts techniques et juridiques « raisonnables », telles que l'obligation juridique (loi sur l'emploi), les intérêts d'ordre public (prévention de la criminalité, santé et sécurité publiques), les intérêts d'ordre vital (données critiques et de la santé, environnements dangereux; intérêts légitimes (détection des fraudes, emploi, développement de produit) ou l'entrée en vigueur de contrats (emploi, souscriptions et licences). Un exemple d'un intérêt légitime est que les enregistrements de la vidéosurveillance doivent constituer une source de preuve de confiance à tout moment, c'est pourquoi le VMS protège essentiellement les preuves vidéo contre la falsification et assure leur authentification, ce qui rend le droit à l'oubli secondaire.

En général, il existe deux raisons pour lesquelles les personnes concernées s'opposent au stockage des enregistrements vidéo :

- Les intérêts du responsable du traitement de stocker les données sont annulés par les intérêts ou les droits fondamentaux et libertés de la personne concernée, qui requiert la protection de ses données à caractère personnel (article 17 (1)(c), RGPD)
- Les données à caractère personnel ont fait l'objet d'un traitement illicite, par exemple, la surveillance d'une crèche ou de vestiaires (article 17 (1)(d), RGPD)

Chaque demande doit donc être examinée minutieusement.

Durée de rétention des enregistrements

Le principe général est que les enregistrements ne doivent pas être retenus plus longtemps que nécessaire aux finalités pour lesquelles ils ont été menés. Il faut également considéré le caractère nécessaire de l'enregistrement en premier lieu et si la surveillance en direct sans enregistrement serait suffisante.

Si une institution opte pour l'enregistrement, elle doit spécifier la durée de rétention des enregistrements. Les enregistrements doivent être effacés une fois cette période écoulée. Milestone XProtect VMS automatise ce processus de suppression en effaçant automatiquement les enregistrements plus anciens que la durée de rétention.

Lorsque les fichiers qui contiennent des données de vidéo enregistrée sont supprimés par le VMS, ces fichiers et leur contenu ne sont pas effacés des blocs de données du système de stockage, mais simplement marqués comme étant libres dans le système de fichiers, ce qui permet l'écriture des autres fichiers à cet emplacement sur le système de stockage. Jusqu'à ce que les blocs de données ne soient écrasés avec de nouvelles données, les anciennes données vidéo supprimées peuvent être restaurées, autorisant ainsi l'accès à des enregistrements plus anciens que la durée de rétention configurée.

C'est pour cette raison qu'il est recommandé de ne pas sur-dimensionner le système de stockage car le risque s'élève en cas de surcharge de la taille.

Par exemple, si le système de stockage affecté est deux fois plus grand que la quantité de données vidéo stockées pour la durée de rétention configurée, par exemple sept jours, les blocs de données supprimés qui contiennent d'anciennes données vidéo supprimées peuvent rester dans le système de stockage durant sept jours supplémentaires avant qu'ils ne soient écrasés.

Pour mieux réduire le risque d'accès aux anciennes données vidéos qui ont été supprimées, et pour des questions de sécurité en général, il est recommandé d'activer le cryptage des bases de données multimédia car outre la restauration des fichiers supprimés, cela requiert également l'interruption du cryptage.

Que les données vidéo aient été cryptées ou non, une fois que les disques du système de stockage ne sont plus utilisables, il est important de nettoyer ou procéder à la destruction physique des disques durs qui ont été utilisés pour stocker les bases de données multimédia avant de vous en débarrasser (par exemple, par déchiquetage ou par un autre moyen similaire).

Pour plus d'informations sur comment configurer cette installation dans Milestone XProtect, voir la section Stockage et archive (explications) dans le manuel de l'administrateur pour un VMS XProtect.

Si la vidéosurveillance est en place pour une question de sécurité et qu'un incident de la sécurité a lieu et qu'il est déterminé que les enregistrements sont nécessaires à l'enquête de l'incident ou utilisés comme preuve, l'enregistrement concerné peut être conservé au-delà de la durée de rétention normale et aussi longtemps que nécessaire. Ils doivent, bien évidemment, être supprimés par la suite.

Durée de rétention à des fins de sécurité typiques : d'une semaine à un mois

Lorsque les caméras sont installés pour des questions de sécurité, le délai suffisant pour que le personnel de la sécurité décide de conserver un enregistrement plus longtemps pour enquêter sur un incident de sécurité ou pour l'utiliser comme preuve, est d'une semaine à un mois.

Exemple de législation locale : conformément à la loi allemande sur la protection des données et à la plupart des documentations sur la protection des données, cette durée de rétention varie de 48 à 72 heures à titre de référence pour le contrôle d'accès et l'enquête d'infractions pénales.

État membre ou territoire de pays tiers : 48 heures

Lorsque la surveillance couvre des zones extérieures de bâtiments du territoire (généralement, près des zones d'entrée et de sortie) d'un État membre (ou d'un pays tiers) et qu'il n'est pas possible d'éviter l'enregistrement de passagers ou de voitures par les caméras, il est recommander de réduire la durée de rétention à 48 heures ou bien de tenir compte le plus possible des préoccupations locales.

Droit à la limitation du traitement

En référence à l'article 18 (1) du RGPD, la personne concernée a le droit d'obtenir la limitation du traitement. Dans un scénario de VMS basique, la personne concernée peut prétendre que le traitement VMS est illicite, par exemple, si la personne concernée ignore qu'un espace public est soumis à une vidéosurveillance comportant des masques de confidentialité. Il est recommandé d'utiliser un modèle de *demande formulée par la personne concernée* pour enregistrer la réclamation (voir Demande formulée par la personne concernée sur la page 12). Pour un modèle d'exemple d'une demande de personne concernée, voir le modèle *Milestone Demande de personne concernée*.

La réclamation doit être traitée dans un délai raisonnable, plus vite que celui de la durée de rétention afin d'éviter la rétention automatique ou la suppression d'une preuve du VMS dans le processus de la réclamation. Il est généralement recommandé de solliciter l'aide d'un avocat concernant la restriction du traitement. Un moyen de répondre à ladite demande est de permettre à l'administrateur du VMS de limiter les superviseurs ou opérateurs du VMS par le biais de rôles pour que ces derniers aient uniquement la possibilité de lire les enregistrements dans un cours laps de temps après l'enregistrement, comme quatre heures ou un jour (voir Procédure sur la page 41 : « Restreindre l'accès des opérateurs à la vidéo enregistrée, soit complètement, uniquement à la vidéo enregistrée au cours des dernières heures ou seulement avec une double autorisation »). Les limites de la lecture s'appliquent également à la protection des preuves. Si de plus amples limitations du traitement sont requises, il est recommandé de mener une analyse d'impact commercial ainsi qu'une analyse d'impact sur la protection des données (voir Mener une analyse d'impact sur la page 34) dans le cadre de la gestion de la réclamation.

Protection des données dès la conception

Le RGPD décrète que la protection des données doit être une priorité tout au long de la conception et de la mise en service du système. L'approche adoptée par rapport à la protection des données se doit d'être préventive et non réactive. Les risques doivent être anticipés et l'objectif doit être d'éviter les événements avant qu'ils n'aient lieu.

Les institutions doivent examiner et enregistrer avec soin le processus de conception des systèmes afin de respecter les objectifs stipulés.

Un soin particulier doit être porté à ne pas collecter les données à caractère personnel des personnes qui ne relèvent pas du domaine du système (par exemple, les zones publiques contiguës).

Une attention particulière doit être portée à qui a besoin de voir quelles informations (par exemple, en direct/enregistrée, délai, résolution) et qui peut accéder à quelles fonctionnalités (par exemple, la recherche).

Procédure

- Documenter la résolution des différents points de la scène des caméras
- Documenter la durée de rétention voulue
- Considérer l'application d'un masquage de confidentialité (permanent ou amovible)
- Considérer la configuration de permissions de voir des vidéos en direct et enregistrées
- Considérer restreindre l'accès à l'exportation d'enregistrements et à la suppression des masques de confidentialité
- Vérifier régulièrement les rôles et responsabilités des opérateurs, enquêteurs, administrateurs du système et autres, ainsi que leur accès au système
- Considérer restreindre l'accès aux groupes chargés d'enquêter sur les caméras qui ont été spécifiquement positionnées pour capturer l'identité (par exemple, le visage des personnes qui entrent dans une boutique)

- Considérer restreindre l'accès des opérateurs à la vidéo enregistrée, soit complètement, uniquement à la vidéo enregistrée au cours des dernières heures ou seulement avec une double autorisation
- Limiter le nombre d'utilisateurs qui ont un rôle d'administateur

Prérequis pour la protection des données dès la conception

Minimisation des données	Vous devez vous assurer que les données à caractère personnel que vous traitez sont : • adéquates : suffisantes au regard de la finalité spécifiée • pertinentes : elles ont un lien rationnel avec ladite finalité • limitées au nécessaire : vous ne retenez pas plus de ce dont vous avez besion pour cette finalité.
Exactitude	De manière générale, pour les données à caractère personnel : • Vous devez prendre toutes les mesures justifiées pour garantir que les données à caractère personnel que vous détenez ne sont pas incorrectes ou trompeuses. • Vous pourriez avoir besoin de mettre à jour les données à caractère personnel, bien que cela dépende de votre utilisation. • Si vous découvrez que les données à caractère personnel sont incorrectes ou trompeuses, vous devez prendre les mesures justifiées pour les corriger ou les effacer au plus vite. • Vous devez prendre en considération les défis liés aux données à caractère personnel.
Limite de la durée de stockage	• Vous ne devez pas conserver les données à caractère personnel plus longtemps que nécessaire. • Vous devez estimer et être en mesure de justifier, la durée de rétention des données à caractère personnel. Celle-ci varie en fonction des finalités de la rétention des données. • Vous avez besoin d'une politique qui fait état des durées de rétention standard dans la mesure du possible pour respecter les exigences documentées. • Vous devez également vérifier à intervalles réguliers les données que vous détenez et les effacer ou les rendre anonymes lorsque vous n'en avez plus besoin.

	• Vous devez prendre en considération les défis liés à votre rétention des données. Les personnes concernées ont un droit à l'effacement si vous n'avez plus besoin de leurs données. • Vous pouvez conserver les données à caractère personnel uniquement si vous les conserver à des fins d'archivage d'intérêt public, de recherche scientifique ou historique ou à des fins de statistiques.

Protection des données dès la conception et protection des données par défaut

Conformément au RGPD, lorsqu'il traite lesdites données, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données stipulés dans le RGPD. Le RGPD s'y réfère comme la protection des données dès la conception.

Dans le cas d'une caméra, un bon exemple de protection des données dès la conception serait une fonctionnalité qui permet numériquement à l'utilisateur de restreindre la capture des images d'un périmètre donné, empêchant ainsi la caméra de capturer toute image en dehors de ce périmètre qui serait en temps normal capturée.

Le VMS XProtect prend en charge le masquage de la confidentialité de deux façons : les masques permanents qui ne peuvent pas être supprimés, et les masques amovibles qui (avec les autorisations appropriées) peuvent être retirés pour révéler l'image figurant derrière le masque.

Le responsable du traitement doit également mettre en œuvre des mesures techniques et organisationnelle, qui, par défaut, garantissent un traitement des données à caractère personnel en question le moins indiscret possible. Le RGPD s'y réfère comme protection des données par défaut. Dans le cas d'une caméra, un exemple pertinent de la protection des données par défaut peut être l'utilisation d'un masque de confidentialité pour garder privées les zones sensibles au sein de la vue de la caméra.

Exemple d'une fonctionnalité de XProtect qui prend en charge l'approche de la protection des données par défaut

Milestone développe régulièrement son portfolio de produits, et la protection des données par défaut constitue un critère-clé d'évaluation pour le bon respect de XProtect au RGPD. Pour plus d'informations, voir le guide sur le cycle de développement sécurisé sur Milestone. Ce guide représente une partie intégrante de la protection des données par défaut en appliquant des principes, tels que la « défense en profondeur », le « moindre privilège », en évitant moins de paramètres de sécurité par défaut et en arrêtant des fonctionnalités peu utilisées par défaut.

Garantir la protection des données par défaut

- Prendre en compte la résolution de différents points dans le champ de la caméra et documenter ces paramètres

  La qualité des images varie selon les finalités. Lorsque l'identification n'est pas nécessaire, la résolution de la caméra et d'autres facteurs ajustables doivent être choisis pour garantir qu'aucune image de visages reconnaissables ne soit capturée.

- Crypter vos enregistrements

  Milestone vous recommande de sécuriser vos enregistrements en activant au moins Cryptage faible dans l'option stockage et archives de vos serveurs d'enregistrement. Milestone utilise l'algorithme AES-256 pour le cryptage. Si vous sélectionnez Cryptage faible, seule une partie de l'enregistrement sera cryptée. Si vous sélectionnez Cryptage complte, l'intégralité de l'enregistrement sera crypté.

- Sécuriser le réseau

  Milestone vous recommande de sélectionner les caméras qui prennent en charge HTTPS. Il est recommandé de configurer les caméras sur des VLAN séparés et d'utiliser HTTPS pour la communication entre votre caméra et le serveur d'enregistrement et entre les clients et le serveur d'enregistrement.

  Il est recommandé d'activer le chiffrement pour toutes les communications entre tous les serveurs et clients. Pour plus d'informations sur la sécurité de vos installations XProtect VMS, voir le guide de durcissement et le guide des certificats.

  Il est recommandé de placer XProtect Smart Client et XProtect Smart Wall sur le même VLAN que celui des serveurs.

  Si vous utilisez Smart Client ou Smart Wall depuis un lieu éloigné, utilisez un VPN crypté ou similaire.

- Activer et documenter la durée de rétention voulue

  Conformément à l'article 17 (1)(a) du RGPD, les enregistrements ne doivent pas être retenus plus longtemps que nécessaire aux finalités pour lesquelles ils ont été menés. Milestone vous recommande de configurer la durée de rétention en conséquence. Cette action automatise alors la suppression de la vidéo.

- Sécuriser les exports

  Milestone vous recommande d'autoriser l'accès aux fonctionnalités d'exportation uniquement à un certain ensemble d'utilisateurs qui ont besoin de cette permission.

  Milestone recommande également de modifier le profil Smart Client de manière à autoriser les exportations uniquement au format XProtect avec le cryptage activé. Les exportations au format AVI et JPEG ne doivent pas être autorisées car elles ne peuvent pas être sécurisées. Cela rend l'exportation de toute preuve protégée par un mot de passe, cryptée et requérant une signature numérique, assurant ainsi que la pièce judiciaire est authentique, infalsifiable et vue uniquement par le destinataire autorisé.

- Activer le masquage de confidentialité (permanent ou amovible)

  Utilisez le masquage de confidentialité pour éviter la surveillance de zones non pertinentes à la cible de votre surveillance.

- Restreindre les autorisations d'accès via des rôles

  Appliquer le principe du moindre privilège (PoLP).

  Milestone recommande d'autoriser l'accès aux fonctionnalités uniquement à un ensemble d'utilisateurs sélectionné qui ont besoin de cette permission. Par défaut, seul l'administrateur du système peut accéder au système et aux tâches de performance. Aucun nouveau rôle et utilisateur créé n'a accès à aucune fonctionnalité tant qu'il n'est pas volontairement configuré par un administrateur.

  Configurez des permissions pour toutes les fonctionnalités, y compris le visionnage de la vidéo en direct et des enregistrements, l'écoute de l'audio, l'accès au métadonnées, le contrôle des caméras PTZ, l'accès et la configuration de Smart Wall, le levage des masques de confidentialité, le travail avec les exportations, l'enregistrement de captures d'écran, etc.

  Restreignez l'accès des opérateurs à la vidéo enregistrée, à l'audio et aux métadonnées, soit complètement, à la vidéo uniquement ou soit aux métadonnées enregistrées au cours des dernières heures ou moins.

  Analysez et vérifiez régulièrement les rôles et responsabilités des opérateurs, enquêteurs, administrateurs du système et autres, ainsi que leur accès au système. Le principe du moindre privilège s'applique-t-il encore ?

- Restreindre les permissions des administrateurs

  Milestone vous recommande de limiter le nombre d'utilisateurs qui ont un rôle d'administrateur.

Configurer le système de vidéosurveillance

Le principe fondamental commun à toutes les recommandations contenues dans cette section est qu'il faut réduire le plus possible sur le respect de la vie privée et sur les autres droits fondamentaux et intérêts légitimes des personnes surveillées.

Emplacement des caméras et angles de vue

Les caméras doivent être placées de façon à filmer le moins possible des endroits inutiles pour l’objectif recherché.

En règle générale, lorsqu’un système de vidéosurveillance est installé dans le but de protéger les actifs (biens ou informations) de l’institution ou la sécurité de son personnel et de ses visiteurs, l’institution doit limiter la surveillance

- à des endroits soigneusement sélectionnés contenant des informations sensibles, des articles de valeur ou d'autre bien nécessitant une protection accrue pour une raison spécifique,
- aux points d'entrée et de sortie des bâtiments (y compris les issues de secours ainsi que les murs et clôtures entourant le bâtiment ou le terrain); et
- points d'entrée et de sortie à l'intérieur du bâtiment reliant différentes zones soumises à des autorisations d'accès différents et séparés par des portes verrouillées et un autre mécanisme de contrôle d'accès.

Nombre de caméras

Le nombre de caméras à installer dépend de la taille des bâtiments et des besoins de sécurité, qui dépendent eux-mêmes de différents facteurs. Lenombre et le type de caméras qui conviennent à une institution peuvent être tout à fait disproportionnés pour une autre institution. Cependant, toutes choses égales par ailleurs, le nombre de caméras est un bon indicateur de la complexité et de la taille d'un système de surveillance et peut indiquer des risques accrus pour le respect de la vie privée et d'autres droits fondamentaux. L'augmentation du nombre de caméras augmente également le risque que ces caméras ne soient pas utilisées efficacement et que cela provoque une surcharge d'informations. Le Contrôleur européen de la protection des données (CEPD) recommande donc de limiter le nombre de caméras au strict nécessaire pour réaliser les objectifs du système. La politique de vidéosurveillance doit préciser le nombre de caméras.

Horaires de surveillance

Les horaires d'enregistrement des caméras doivent être déterminés de façon à couvrir le moins possible de moments où l'enregistrement ne présente aucun intérêt pour l'objectif recherché. Si l'objectif de la vidéosurveillance est la sécurité, le système doit si possible enregistrer uniquement aux heures présentant une probabilité accrue de problèmes de sécurité.

Résolution et qualité d'image

Il convient d'opter pour une résolution et une qualité d'image adéquates. La qualité d'image requise varie en fonction de l'objectif poursuivi. Par exemple, si l'identification de personnes est essentielle, il convient de prendre en considération la résolution des caméras, les paramètres de compression des systèmes numériques, l'emplacement, l'éclairage et d'autres facteurs et de les définir ou de les modifier de façon à obtenir des images de qualité suffisante pour permettre la reconnaissance des visages. Lorsque l'identification n'est pas nécessaire, la résolution des caméras et les autres paramètres modifiables doivent être choisis de façon à ne pas enregistrer d'images faciales reconnaissables.

Personnes autorisées à accéder au VMS

Les autorisations d'accès doivent être limitées à un petit nombre d'individus clairement identifiés en cas de nécessité absolue. Les politiques d'accès du VMS doivent être définies en suivant le principe du « moindre privilège » : les utilisateurs ont accès uniquement aux informations strictement nécessaires pour l'exécution de leurs tâches.

Seul le responsable du traitement, l'administrateur système ou les autres membres du personnel désignés expressément par le responsable du traitement à cette fin doivent être habilités à accorder, modifier ou supprimer les autorisations d'accès de toutes les personnes. L'octroi, la modification et la suppression de autorisations d'accès doivent toujours se faire dans le respect des critères définis par la politique de vidéosurveillance de l'institution.

Les personnes qui disposent d'autorisations d'accès doivent en tout temps être des individus clairement identifiables.

La politique de vidéosurveillance doit clairement spécifier et documenter qui a accès aux enregistrements de vidéosurveillance et/ou à l'architecture technique, par exemple les serveurs du VMS, du système de vidéosurveillance, la raison de cet accès et la nature précise des autorisations d'accès. Vous devez spécifier, plus particulièrement, qui dispose des autorisations pour

- Visionner de la vidéo/écouter de l'audio en temps réel
- Commander les caméras à balayage horizontal, vertical et zoom (PTZ)
- Visionner les enregistrements
- Exporter, ou
- Supprimer un enregistrement

Vous devez également configurer l'accès aux fonctionnalités du VMS suivantes :

- Les signets
- Le verrouillages des preuves
- Enlever les masques de confidentialité
- Exporter
- Déclencher des événements
- Débuter/terminer un enregistrement
- Créer/modifier/supprimer/activer/verrouiller/libérer les préréglages PTZ
- Créer/modifier/supprimer/démarrer/arrêter les schémas de patrouille PTZ
- La recherche avancée
- L'audio, les métadonnées, les permissions E/S et des événements

Protéger les données stockées et transmises

Avant tout, il y a lieu d'effectuer une analyse interne des risques de sécurité afin de déterminer les mesures de sécurité nécessaires pour protéger le système de vidéosurveillance, y compris les données à caractère personnel qu'il traite.

Dans tous les cas, des mesures doivent être prises pour garantir la sécurité en matière de

- Transmission
- Stockage (par exemple, dans des bases de données informatiques)
- Accès (par exemple, accès aux systèmes informatiques et aux locaux)

La transmission doit passer par des canaux de communication sécurisés et protégés contre l'interception, par exemple en procédant comme suit :

- Chiffrer la base de données médias dans le Recording Server et chiffrer toutes les communications entre les serveurs et les clients. Pour plus d'informations sur la sécurité de vos installations XProtect VMS, voir le guide de durcissement et le guide des certificats.
- Connecter la caméra HTTPS au Recording Server
- Utiliser un VPN pour Smart Client ou Management Client connectés via Internet

La protection contre l'interception est particulièrement importante en cas d'utilisation d'un système de transmission sans fil ou de transfert de séquences via Internet. Dans de tels cas, les données doivent être cryptées pendant leur transmission ou bénéficier d'une protection équivalente.

Le cryptage ou d'autres moyens techniques offrant une protection équivalente doivent également être envisagés dans d'autres cas, au niveau du stockage, si l'analyse interne des risques de sécurité le justifie. Cela peut être, par exemple, dans le cas de séquences particulièrement sensibles. L'activation du cryptage de la base de données multimédia le permet.

Tous les locaux servant au stockage ou au visionnage de séquences de vidéosurveillance doivent être sécurisés. L'accès physique à la salle de contrôle et à la salle de serveur où sont situés les serveurs du VMS doit être protégé. Aucune partie tierce (par exemple, personnel d'entretien ou de maintenance) ne doit pouvoir accéder à ces locaux sans surveillance.

L'emplacement des moniteurs doit être défini de façon à ce que les images ne soient pas visibles pour le personnel non autorisé. S'ils doivent être placés près de la réception, les moniteurs doivent être orientés de façon à ce que seul le personnel de sécurité puisse les consulter.

Le XProtect VMS enregistre par défaut les informations de base, mais nous vous recommandons d'activer la journalisation des accès utilisateur dans le Management Client pour le journal d'activité.

Ce système d'archivage numérique doit être mise en place pour permettre, en cas d'audit, de déterminer à tout moment qui a accédé au système, où et quand. Le système d'archivage doit être en mesure d'identifier qui a visionné, supprimé ou exporté n'importe quelle donée de vidéosurveillance (cela nécessite d'activer la journalisation de l'accès des utilisateurs).

Pour plus d'informations, voir le manuel de l'administrateur pour VMS XProtect.

À cet égard comme ailleurs, il convient d'accorder une attention particulière aux rôles et aux pouvoirs essentiels des administrateurs du système et à la nécessité de compenser ces pouvoirs par des mesures de contrôle et de protection suffisantes.

Responsabilité

L'article 5 (2) du RGPD indique que :

Le responsable doit être responsable de la conformité avec le paragraphe 1 (« responsabilité ») et pouvoir en apporter la preuve.

Les principes concernant le traitement des données à caractère personnel sont : la régularité, l'équité et la transparence, la limitation des finalités, la minimisation des données, la précision, la limitation de la conservation, l'intégrité et la confidentialité.

Le principe de responsabilité vous exige d'assumer la responsabilité de votre traitement des données à caractère personnel.

Plus concrètement, l'article 30 du RGPD indique que :

Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité.

Ce registre comporte toutes les informations suivantes :

a. le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données

b. les finalités du traitement

c. une description des catégories de personnes concernées et des catégories de données à caractère personnel

d. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des institutions internationales

e. le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49 (1), les documents attestant de l'existence de garanties appropriées

f. dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données

g. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32 (1).

La responsabilité constitue l'un des principes de la protection des données. Vous devez assumer la responsabilité du bon respect du RGPD et pouvoir en apporter la preuve.

Vous devez prendre les mesures techniques et organisationnelles adéquates pour assurer le bon respect du principe de responsabilité.

Vous pouvez, et dans certains cas, devez, prendre plusieurs mesures, dont :

- L'adoption et la mise en œuvre des politiques en matière de protection des données
- L'adoption d'une approche de « protection des données dès la conception et protection des données par défaut » (pour plus d'informations, voir Protection des données dès la conception sur la page 41)
- La mise en place de contrats écrits avec les institutions qui traitent les données à caractère personnel en votre nom
- Le maintien d'une documentation de vos activités de traitement
- La mise en œuvre des mesures de sécurité adéquates

- L'enregistrement et, si nécessaire, le rapport des violations de données à caractère personnel
- L'exécution d'analyse d'impact sur la protection des données pour l'utilisation des données à caractère personnel qui peut provoquer un risque élevé pour les intérêts des personnes concernées.
- La désignation d'un délégué à la protection des données
- L'adhésion aux codes de conduite concernés et l'inscription aux systèmes de certification

Utilisation d'un modèle de rapport des activités de traitement pour identifier et repérer les problèmes liés aux obligations de rendre compte. Pour un modèle d'exemple d'un registre des activités de traitement, voir le modèle *Milestone Registre des activités de traitement*.

Les obligations de rendre compte sont continues. Vous devez vérifier et, si nécessaire, mettre à jour les mesures mises en œuvre.

La mise en place d'un cadre de gestion de la protection de la vie privée peut vous aider dans l'intégration de mesures de transparence et créer une culture de protection au sein de votre institution.

La transparence peut vous aider à établir un lien de confiance avec les personnes concernées et diminuer les mesures répressives du RGPD.

Liste récapitulative pour la garantie de l'intégrité et de la confidentialité

Conformément au RGPD, les institutions doivent avoir des politiques et des procédures exhaustives qui garantissent que les données à caractère personnel demeurent sous son contrôle. De plus, toute violations de données à caractère personnel doit être reportés dans un délai de 72 heures aux autorités de contrôle compétentes désignées par le gouvernement du pays.

Prendre toutes les mesures techniques et organisationnelles nécessaires à la protection des données à caractère personnel.

Procédure

- Vérifier les politiques de sécurité concernant le contrôle des mots de passe et l'usage des comptes.
- Configurer des exigences de complexité pour les mots de passe de tous les groupes de domaines. Configurer des exigences plus strictes pour les comptes administratifs au niveau du domaine.
- Mettre en place les processus pour contrôler les statuts de protection et détecter les failles.
- Assurer que les utilisateurs ne partagent pas leurs comptes, que ce soit en partageant leurs mots de passe ou en omettant de se déconnecter/connecter à la fin/au début de leur quart.
- Maintenir une politique et une procédure documentées qui régissent les actions à prendre en cas de fuite de violation de données.
- Vous devez vous assurer d'avoir mis en place les mesures de sécurité adéquates pour la protection des données à caractère personnel que vous détenez.

- Un principe clé du RGPD est le « principe de sécurité ». En d'autres termes, vous traitez les données à caractère personnel de manière sécurisée par le biais de « mesures techniques et organisationnelles adéquates ».
- Pour ce faire, vous devez prendre en compte des éléments, tels que les analyses de risques, les politiques organisationnelles et les mesures physiques et techniques.
- Vous devez également prendre en compte des exigences supplémentaires concernant la sécurité de votre traitement. Cela s'applique également aux sous-traitants de données.
- Vous pouvez prendre en compte l'état de la technique et les coûts de la mise en œuvre lorsque vous décidez des mesures à prendre. Dans tous les cas, ces dernières doivent être adéquates pour vos circonstances et le risque impliqué par votre traitement.
- S'il y a lieu, vous devez considérer l'utilisation de mesures, telles que la pseudonymisation (par exemple, par le biais d'une protection avec un masque flou) et le cryptage.
- Vos mesures doivent garantir la « confidentialité, l'intégrité et la disponibilité » de vos systèmes et services ainsi que les données à caractère personnel qu'ils traitent.
- Les mesures doivent également vous permettre de restaurer l'accès aux données à caractère personnel et leur disponibilité dans les meilleurs délais possible lorsqu'un incident physique ou technique survient.
- Vous devez également garantir d'avoir les processus adéquats en place pour tester l'efficacité de vos mesures et procéder à toute amélioration requise.

Appendice : Avis sur place

Les avis affichés sur place doivent inclure un pictogramme (par exemple le pictogramme ISO ou le pictogramme utilisé habituellement à l'endroit où se situe le bâtiment). Le pictogramme doit également être compréhensible pour les enfants. Vous trouverez un exemple sur la page des symboles graphiques ISO (https://www.iso.org/obp/ui/#search/grs/). Cet avis doit :

- Identifier le responsable du traitement
- Spécifer la finalité de la surveillance :
    - Pour que les organismes de droit public puissent exécuter leurs tâches
    - Pour exercer le droit de déterminer qui peut avoir ou non l'accès
    - Pour protéger des intérêts légitimes à des fins bien définies
- Indiquer clairement si les images sont enregistrées
- Fournir des informations de contact et un lien vers la politique de vidéosurveillance disponible en ligne
- Si la surveillance s'étend à n'importe quel endroit en dehors du bâtiment, l'avis doit le préciser clairement

Le personnel de sécurité et l'équipe de réception doit avoir reçu une formation relative aux aspects de protection des données de la vidéosurveillance et être en mesure de distribuer immédiatement des copies de l'avis détaillé en matière de protection des données (voir Appendice : Politique de vidéosurveillance sur la page 52), sur simple demande. Ces employés doivent également pouvoir donner aux membres du public le nom de la personne à contacter pour toute question supplémentaire ou pour avoir accès aux données les concernant.

Ces avis doivent être placés aux endroits opportuns et avoir un format suffisant pour que les personnes concernées puissent les remarquer avant de pénétrer dans la zone surveillée et qu'elles puissent les lire sans difficulté. Cela ne signifie pas pour autant qu'il faille afficher un avis à côté de chaque caméra.

Les affiches situées à l'intérieur du bâtiment doivent être dans la ou les langue(s) généralement comprises par les membres du personnel et les visiteurs les plus fréquents. Les avis situés à l'extérieur des bâtiments (si la surveillance couvre des espaces extérieurs) doivent également être affichés dans la ou les langue(s) locale(s).

Pour un modèle d'exemple d'une notification d'avis sur place, voir le modèle *Milestone Avis sur place*.

Appendice : Politique de vidéosurveillance

La politique de vidéosurveillance poursuit plusieurs objectifs et répond aux besoins suivants :

- L'adoption de ce document sera souvent nécessaire pour compléter et spécifier la base juridique, et donc pour établir la légitimité de la vidéosurveillance (voir l'article 5 du RGPD).
- Le fait de mettre les bonnes pratiques par écrit et de réfléchir aux mesures supplémentaires à prendre permettra probablement d'améliorer les procédures et de garantir une meilleure conformité.
- L'adoption d'une politique et sa publication contribueront aussi au respect de l'obligation, imposée par le RGPD, de communiquer au public les informations nécessaires pour garantir un traitement équitable.
- La politique définit un ensemble de règles permettant de mesurer la conformité (par exemple lors d'un audit).
- En renforçant leur transparence et en apportant la preuve de leurs efforts de conformité, les institutions inspirent la confiance de leurs employés et des parties tierces et contribuent à faciliter les consultations avec les parties prenantes.

La politique de vidéosurveillance doit :

- Présenter une vue d'ensemble du système de vidéosurveillance et décrire ses finalités
- Décrire l'utilisation du système, l'usage qui est fait des données à caractère personnel et les mesures de protection des données mises en place
- Confirmer expressément le respect du RGPD
- Décrire les mesures de mises en œuvre éventuellement nécessaires

Les institutions doivent publier leurs politiques de vidéosurveillance sur leur intranet et leurs sites internet. Si le document de base contient des informations confidentielles, une version non confidentielle doit être rendue publique.

Pour pouvoir servir correctement d'avis en matière de protection des données, votre politique de vidéosurveillance doit contenir les informations suivantes dans un langage et un format facilement lisibles :

- L'identité du responsable du traitement (par exemple, l'institution, la direction générale, la direction et l'unité)
- Une description succincte de la couverture du système de vidéosurveillance (par exemple, entrées et sorties, salles informatiques, salles d'archive)
- La base juridique de la vidéosurveillance, par exemple, l'article 6 (1)(f) du RGPD
- Les données collectées et la finalité de la vidéosurveillance (toutes les restrictions en matière d'utilisation autorisée doivent également être précisées clairement)
- Les personnes qui ont accès aux séquences de vidéosurveillance et celles à qui les images sont susceptibles d'être divulguées
- La façon dont les informations sont protégées et sauvegardées
- La durée de conservation des données
- La procédure à suivre par les personnes concernées pour vérifier, modifier ou supprimer leurs informations (avec des coordonnées permettant d'obtenir de plus amples informations et des informations sur la façon de lancer un recours en interne)

Par ailleurs, la politique de vidéosurveillance doit également fournir des références vers :

- Les rapports d'audit de l'institution
- les rapports de l'analyse d'impact de l'institution

Pour un modèle d'exemple d'une politique de vidéosurveillance, voir le modèle *Milestone Politique de vidéosurveillance*.

Exonération de responsabilité : Le modèle de la politique de vidéosurveillance doit être vérifié par le responsable du traitement. Il est responsable de la conformité de ce modèle au RGPD.

Remarque : La collecte d'audio et de métadonnées n'est pas couverte par le label européen de protection des données à caractère personnel. Une configuration VMS qui collecte de l'audio et des métadonnées n'est pas habilité à utiliser le profil de produit certifié EuroPriSe. Un responsable du traitement des données ou un sous-traitant de données qui dévient de ces exigences ne peut prétendre utiliser un produit qui protège les données et qui est conforme au RGPD.

Appendice : Analyse d'impact relative à la protection des données

Conformément à l'article 35 du RGPD, une *analyse d'impact relative à la protection des données* est nécessaire si la surveillance

est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

Le responsable du traitement doit consulter l'autorité de contrôle préalablement au traitement lorsqu'une *analyse d'impact relative à la protection des données* effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque (Consultation préalable, article 36 du RGPD).

Créer et respecter une *Analyse d'impact relative à la protection des données*, avis aux personnes concernées. Ce document :

- Décrit les fins de la surveillance
- Est conservé par le responsable du traitement
- Définit les politiques de conservation

Une *analyse d'impact relative à la protection des données* doit être mise en place avant l'installation et la mise en œuvre des systèmes de vidéosurveillance dès qu'elle ajoute de la valeur aux démarches de l'institution pour respecter ses obligations. L'objectif de l'*analyse de l'impact des opérations de traitement* est de déterminer l'impact du système proposé sur la protection de la vie privée et d'autres droits fondamentaux des individus et d'identifier des mesures pour diminuer ou éviter des effets négatifs.

Conformément à l'article 35 (7) du RGPD, l'analyse doit au moins contenir :

- Une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités
- Une évaluation des risques pour les droits et libertés des personnes concernées conformément à l'article 35 (1) du RGPD :

  Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées

L'effort nécessaire pour investir dans une *analyse d'impact relative à la protection des données* varie en fonction des circonstances. Un système de vidéosurveillance comportant des risques élevés ou soulevant des questions complexes ou nouvelles, justifie de plus grands efforts qu'un système ayant un impact limité sur la protection de la vie privée et d'autres droits fondamentaux des individus, tels qu'un système CCTV statique conventionnel exécuté à des fins de sécurité habituelles.

Quoi qu'il en soit et dans tous les cas, qu'il s'agisse ou non d'une *analyse d'impact relative à la protection des données* protocolaire, les institutions doivent évaluer et justifier la nécessité de recourir à de la vidéosurveillance, comment placer, sélectionner et configurer leurs systèmes et comment mettre en place des mesures de protection des données.

En outre, il se peut qu'une institution propose un système non conventionnel. Dans ce cas, l'institution doit évaluer soigneusement les différences prévues par rapport aux recommandations énoncées, en discuter avec leur responsable de la protection des données et les autres parties prenantes puis documenter son évaluation par écrit, que ce soit dans une *analyse d'impact relative à la protection des données* protocolaire ou autre. Les analyses du système menée par l'organisatoin doivent également aborder la légalité de la personnalisation du système.

Enfin, en raison de leur complexité, nouveauté, spécificité ou risque inhérent, il est vivement recommandé de mener une *analyse d'impact relative à la protection des données* dans les cas suivants :

- Surveillance vidéo à des fins autres que la sécurité (y compris à des fins d'enquête)
- Vidéosurveillance des espaces publics
- Surveillance des employés
- Surveillance des territoires d'un État membre et dans des pays tiers
- Catégories de données spéciales
- Zones sous un plus grand respect de leur vie privée
- Vidéosurveillance de haute technologie et/ou intelligente
- Systèmes interconnectés
- Enregistrement audio

L'*analyse d'impact relative à la protection des données* peut être effectuée en interne ou par un prestataire indépendant. L'analyse doit être menée dès le début du projet. En fonction des résultats de l'*analyse d'impact relative à la protection des données* une institution peut décider de :

- S'abstenir ou modifier la surveillance planifiée et/ou
- Mettre en place des mesures de protection supplémentaires

Risques associés à l'utilisation d'un VMS

Lorsque vous effectuez l'*analyse d'impact relative à la protection des données*, vous devez prendre en compte les risques inhérents à l'utilisation d'un VMS.

L'*analyse d'impact relative à la protection des données* doit être soigneusement documentée. Par principe, un rapport de l'*analyse d'impact relative à la protection des données* doit préciser clairement les risques pour la vie privée et/ou pour les autres droits fondamentaux qui ont été identifiés par l'institution, ainsi que les mesures de protection supplémentaires proposées. Il est nécessaire de prendre en compte les risques suivants qui enfreignent les droits individuels :

- Entreprise/employeur qui utilise des flux vidéo, alarmes ou journaux d'activité :
    - Surveiller les heures de travail des employés sur le site évalué, comme les heures d'arrivée et de départ
    - Surveiller l'efficacité des employés en surveillant où ils passent leur temps, le nombre de temps passé à la machine à café, aux toilettes, combien de temps ils travaillent à leurs différentes tâches
    - Surveiller ce que les employés regardent sur leurs ordinateurs
    - Surveiller si les employés respectent les exigences en matière de travail et de sécurité, comme sur les sites de construction
    - Montrer des enregistrements vidéo d'employés à d'autres employés ou responsables pour intimider l'employé ou menacer d'autres employés de faire de même
    - Vérifier si les agents et opérateurs de la sécurité exécutent bien leurs tâches, par exemple, en vérifiant s'ils utilisent activement les clients, sélectionnent des caméras, effectuent des relectures, etc.
- Entreprise/propriétaire/opérateur/gardes qui utilisent des flux vidéo pour :
    - Partager des enregistrements vidéo de personnes (employés de l'entreprise ou public en général) dans des situations embarrassantes ou sensibles sur les réseaux sociaux
    - Utiliser des caméras PTZ pour faire un zoom avant sur des personnes et obtenir d'eux et à leur insu des enregistrements de près intimes/inappropriés
- Entreprise/propriétaire/opérateur/gardes
    - Exporter de la vidéo ou autoriser l'accès à de la vidéo enregistrée sans discernement à quiconque demande

Sources supplémentaires pour identifier un risque :

- Le *Guide de durcissement Milestone* fournit la structure de gestion des cyberrisques, qui décrit les six étapes recommandées pour la classification, sélection, mise en place, évaluation, autorisation et surveillance des risques. Le *Milestone guide de durcissement* fournit une série de risques techniques ainsi que les mises en place recommandées pour les diminuer. Ceux-ci incluent, sans se limiter, la protection de la confidentialité du VMS dans le contexte de risques d'une série d'atteintes à la protection des données et d'accès non-autorisés dus à des failles dans la configuration technique, la conception et les opérations de maintenance. Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.

- Le (présent) *guide relatif au respect de la vie privée Milestone* fournit des recommandation sur le traitement des risques opérationnels non-techniques, y compris le traitement des droits et demandes des personnes concernées, les rôles et les responsabilités d'un VMS, des modèles pour un avertissement immédiat, les politiques en matière de vidéosurveillance et les *accords de traitement des données*.
- La formation en ligne sur la confidentialité de la vie privée des utilisateurs finaux de Milestone offre une formation de sensibilisation pour les opérations du VMS et les superviseurs sur comment traiter, dans les opérations du quotidien, les risques concernant la protection de la vie privée liés au VMS. Pour de plus amples informations, voir le Milestone site Web de certification du RGPD.

Appendice : Accord de traitement des données

Le contrôleur de données doit définir un *Accord de traitement des données* avec toute personne tierce avec laquelle il partage des données de vidéosurveillance, hormis le partage de multimédia de vidéosurveillance avec les autorités.

Si une entreprise sous-traite toutes ou une parties de ses activités de vidéosurveillance à un tiers (un traitement de données), elle demeure responsable du respect du RGPD en tant que contrôleur de données. Par exemple, les gardes de la sécurité en charge de la surveillance vidéo en direct dans la zone de réception d'une institution travaillant pour une entreprise privée avec laquelle l'institution sous-traite la tâche de la surveillance en direct. Dans ce cas, l'institution doit s'assure que les gardes de la sécurité réalisent leurs activités conformément aux prévisions du RGPD.

Pour un modèle d'exemple d'un accord de traitement des données, voir le modèle *Milestone Accord de traitement des données*.

Exonération de responsabilité : Le modèle de l'*Accord de traitement des données* doit être vérifié par le contrôleur de données. Il est responsable de la conformité de ce modèle au RGPD.

Appendice : Le système Milestone XProtect VMS et le RGPD

Remarque : Cette description décrit les exigences et limitations pour un produit conforme au label européen de protection des données à caractère personnel (EuroPriSe). Un responsable du traitement des données ou un sous-traitant de données qui dévient de ces exigences ne peut prétendre utiliser un produit qui protège les données et qui est conforme au RGPD.

Composants et périphériques qui n'ont pas le label européen de protection des données à caractère personnel

Les composants suivants n'ont pas le label européen de protection des données à caractère personnel :

- Les modules d'extension disponibles sur Milestone Marketplace
- Serveur XProtect Mobile (désactivé par défaut)
- Client XProtect Mobile
- XProtect Web Client
- XProtect Access (désactivé par défaut)
- XProtect LPR (désactivé par défaut)
- XProtect Transact (désactivé par défaut)
- Milestone Interconnect
- XProtect DLNA Server
- Milestone Open Network Bridge (sécurise l'intégration vidéo du privé vers le public)
- XProtect Rapid REVIEW
- Modules d’extension XProtect Event Server
- Traitement des données audio (désactivé par défaut)
- Traitement des métadonnées (désactivé par défaut)
- Traitement des données des périphériques d'entrée vers les périphériques de sortie (désactivé par défaut)
- XProtect BYOL tel que fourni via https://aws.amazon.com/marketplace/pp/B089DKW36G

Pour une installation de Milestone XProtect VMS ayant le label européen de protection des données à caractère personnel, ces composants ne doivent pas être installés.

En outre, le produit standard n'effectue pas la reconnaissance faciale, l'analyse des comportements, le suivi automatique ou la reconnaissance de personnes dans le flux en direct ou dans les médias enregistrés. Ces fonctionnalités ne sont pas non plus conforme au label européen de protection des données à caractère personnel.

En d'autres termes, dans le programme d'installation, quand vous installez le XProtect VMS, n'utilisez pas l'option **Ordinateur seul** car il installera automatiquement le Mobile Server.

Installez plutôt le système XProtect VMS avec l'option **Distribuée** ou **Personnalisée**. Ces options n'installe pas le Mobile Server.

Une fois XProtect VMS installé, la page de téléchargements du Management Server répertoriera les composants supplémentaires du DLNA Server et du Mobile Server. N'installez pas ces serveurs.

Guide de mise à niveau

Pour une mise à niveau vers une installation de Milestone XProtect VMS version 2018 R2 ou une version plus récente, les anciens fichiers journaux doivent être effacés manuellement afin que l'installation soit conforme au RGPD.

Une fois XProtect VMS mis à niveau, il est possible de supprimer les anciens fichiers journaux par le biais des informations et outils décrits dans l'article Base de connaissance.

Sécuriser le réseau pour l'authentification et la transmission de données

Dans la mesure du possible, concevez une infrastructure du réseau qui utilise un réseau physique ou une segmentation VLAN.

Milestone vous recommande de sélectionner les caméras qui prennent en charge HTTPS. Il est recommandé de configurer les caméras sur des VLAN séparés et d'utiliser HTTPS pour la communication entre votre caméra et le serveur d'enregistrement et entre les clients et le serveur d'enregistrement.

Il est recommandé de placer XProtect Smart Client et XProtect Smart Wall sur le même VLAN que celui des serveurs.

Si vous utilisez Smart Client ou Smart Wall depuis un lieu éloigné, utilisez un VPN crypté ou similaire.

Activer le cryptage de toutes les communications. Pour plus d'informations sur la sécurité de vos installations XProtect VMS, voir le guide de durcissement et le guide des certificats.

> Remarque : Un transport des données vidéo non-crypté et non-sécurisé enfreint le label européen de protection des données à caractère personnel et provoque la non-conformité au label européen de protection des données à caractère personnel.

Masquage des personnes pour l'accès

Conformément à l'article 15 du RGPD, la personne concernée a le droit d'accéder à ses données à caractère personnel qui sont traitées, par exemple, les enregistrements vidéo de la personne concernée.

La personne concernée a le droit de demander à une entreprise des informations sur quelles données à caractère personnel (le concernant) sont traitées et les raisons de ce traitement.

Étant donné que XProtect VMS ne prend pas en charge l'identification automatique des personnes, vous devez mettre en place des mesures supplémentaires pour protéger les droits des personnes. Dans le cas du VMS, voir Appendice : Avis sur place sur la page 51.

En outre, XProtect VMS ne prend pas en charge le masquage des personnes qui accompagnent la personne exerçant son droit d'accès.

Différentes solutions de partenaires techniques de Milestone proposant un floutage dynamique de toutes les personnes ou de personnes tierces sont disponibles sur Milestone Marketplace. Il est également possible d'ajouter le floutage à des images seules ou à des flux vidéo manuellement ou de façon assistée après l'exportation. Certaines entreprises proposent le floutage en tant que service (par exemple, FACIT Data Systems).

Suppression partielle des enregistrements vidéo

Conformément à l'article 17 du RGPD, la personne concernée a le droit d'obtenir l'effacement de données à caractère personnel la concernant. Dans le cas du VMS, ce droit n'est pas souvent respecté en raison de la satisfaction des intérêts légitimes (détection de fraude, santé et sécurité) ou d'autre finalités commerciales indiquées dans la politique de la vidéosurveillance (voir Droit à l'oubli (droit à l'effacement) sur la page 38 et Appendice : Politique de vidéosurveillance sur la page 52). Les politiques en matière de vidéosurveillance définissent la rétention automatique (7 jours par défaut) pour assurer la suppression automatique des images, ce qui permet un juste équilibre des droits des personnes concernées quant aux finalités commerciales raisonnables.

Si la personne concernée demande l'effacement des données la concernant, il est recommandé que le responsable du traitement utilise une *Demande de la personne concernée* pour documenter la demande (voir Demande formulée par la personne concernée sur la page 12). Pour un modèle d'exemple d'une demande de personne concernée, voir le modèle *Milestone Demande de personne concernée*.

Vous devez supprimer tous les enregistrements de la ou les caméra(s) en question.

Pour conserver tous les autres enregistrements qui ne doivent pas être supprimés, exportez toutes les données et maintenez-les protégées. Vous ne pouvez pas restaurer ces données dans le VMS.

Toute exportation doit être cryptée et soumise à la signature numérique. Elle ne doit également exclure les intervalles de temps spécifiés de la ou les caméra(s) spécifiées en question. Autrement dit, exportez les données correspondant jusqu'à l'heure/la date et exportez-les après l'heure/la date. Cela peut entraîner des sauvegardes de plusieurs périodes.

Le Smart Client – Player peut ensuite être utilisé pour consulter les données.

Il est recommandé que le responsable du traitement sollicite l'aide d'un avocat, qu'il effectue une évaluation de l'incidence sur les entreprises et une analyse d'impact sur la vie privée (voir Mener une analyse d'impact sur la page 34) avant d'exécuter le droit d'être oublié de la personne concerné étant donné que la suppression peut provoquer de nouveaux risques de l'entreprise qui pourraient faire basculer la balance des intérêts et introduire des risques pouvant affecter la protection de la confidentialité d'autres personnes concernées.

Utilisation des arrières-plans géographiques dans XProtect Smart Client

XProtect Smart Client prend en charge l'utilisation d'arrières-plans géographiques. Ces arrières-plans affichent les arrières-plans des plans.

Vous risquez d'enfreindre le RGPD lorsque vous utilisez l'un des services de carte suivants, et vous ne serez plus conforme au RGPD dans la certification EuroPriSe :

- Bing Maps
- Google Maps
- Milestone Map Service

Ces services ne fournissent pas de protections adéquates concernant le traitement de données à caractère personnel au sein des États-Unis. Le client devient (conjointement) le responsable du traitement des données d'utilisateur.

Consultez les mises à jour de la Commission européenne concernant l'arrêt Schrems II sur le site Web officiel.

Comme alternative, il est recommandé de configurer le service **OpenStreetMap** privé pour l'arrière-plan géographique.

Intégrations des partenaires enregistrés

Lorsqu'une licence est activée, Milestone collecte des données pour chaque intégration. Le XProtect VMS recueille des données sur les modules d'extension et les fabricants des modules d'extension ainsi que sur les modules d'extension et intégrations utilisées par le client.

Les données collectées pour chaque installation sont :

- Le nom de l'intégration
- Le fabricant de l'intégration
- La version de l'intégration
- Le type de l'intégration (autonome Smart Client, Management Client, Event Server) et le nombre d'instances de chaque type (c'est-à-dire le nombre de clients exécutant le module d'extension)

Les développeurs de module d'extension ne doivent jamais utiliser de noms personnels lorsqu'ils enregistrent leur produit. Ils voient uniquement utiliser le nom de l'entreprise.

Les données sont traitées uniquement par Milestone si le fabricant du module d'extension figure sur Marketplace et qu'il a approuvé le traitement des données à des fins d'amélioration de Milestone XProtect Corporate (et non à des fins commerciales ou d'étude de marché). Si le module d'extension n'est pas enregistré, les données sont immédiatement supprimées. La base légale du traitement est l'article 6 (1)(f) du RGPD, qui indique les intérêts légitimes de Milestone et des utilisateurs du VMS.

Mesures de protection supplémentaires

Pour vous assurer que la configuration Milestone XProtect VMS est conforme au RGPD, consultez cette liste qui fournit des protections supplémentaires à prendre en compte lors de la configuration du système.

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
Les caméras PTZ et le masquage de confidentialité ne fonctionnent pas ensemble. Les masques	Le renforcement du respect de la vie privée peut être contourné.	Milestone vous recommande de procéder à l'une des solutions suivantes :

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
ne suivent pas les mouvements des caméras PTZ.		• Vous ne devriez pas utiliser la fonctionnalité de masquage de confidentialité intégrée dans XProtect sur les caméras PTZ car le masque est statique pra rapport aux pixels décodés de l'image et non par rapport à la direction ou l'emplacement du la caméra PTZ. • Désactiver les fonctionnalités PTZ lorsque vous utilisez les masques. • Acheter des caméras PTZ qui prennent en charge le masquage de confidentialité dynamique (ainsi, les zones sélectionnées sont toujours masquées, quel que soit l'emplacement et le zoom de la caméra).
L'utilisation d'un microphone ou d'un périphériques de métadonnées peut empiéter sur la vie privée des personnes. (Dans XProtect Corporate, ces paramètres sont désactivés par défaut.)	L'utilisation du microphone peut facilement enfreindre les dispositions du RGPD.	Avant d'activer les microphones et les périphériques de métadonnées, vous devez vous assurer d'avoir une finalité clairement justifiée pour la collecte des données. Voir Existe-t-il une base légale justifiant la collecte des données ? sur la page 29

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
	Remarque : L'utilisation du microphone et des périphériques de métadonnées n'est pas couverte par le label européen de protection des données à caractère personnel. Son utilisation enfreindrait le label EuroPriSe.	
Les opérateurs et les administrateurs peuvent exporter ou copier des données vidéo, des archives vidéo, des sauvegardes de la configuration et des journaux d'activité vers des disques durs locaux ou vers des médias amovibles, comme des CD, des DVD, des clés USB, etc.	Les données à caractère personnel ne sont plus du ressort de XProtect VMS. Les données ne sont plus protégées par les mécanismes de contrôle d'accès du XProtect VMS et elles ne peuvent pas être effacées par XProtect VMS une fois atteinte la durée de rétention. Cela provoque le risque d'une conservation des données plus longue que celle autorisée, une utilisation autre que les finalités indiquées et la violation de la confidentialité des données.	Les responsables du traitement doivent prendre de mesures techniques et organisationnelles pour protéger les données qui ne sont plus du ressort du XProtect VMS. Voir Gestion des données exportées sur la page 21 pour consulter les possibles mesures à prendre.
Les données des journaux d'activité et les autres données à caractère personnel ne sont pas	Le plus important est la divulgation des données sensibles du journal d'activité à des utilisateurs non-autorisés. Voir Protéger les données	Procédez de la manière suivante :

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
cryptés par le produit avant leur conservation dans les bases de données SQL. Les administrateurs des bases de données peuvent accéder aux données des journaux d'activité en utilisant les clients de la bases de données. XProtect Corporate ne peut pas contrôler ou enregistrer cet accès.	stockées et transmises sur la page 47. Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.	• Mettez en place d'un concept de rôles adéquate pour l'administration de la base de données. • Limitez l'accès à la base de données uniquement aux personnes autorisées. • Si possible, activez le cryptage de la base de données via des mécanismes de base de données.
Le produit met en place une fonctionnalité de sauvegarde. Cette fonctionnalité sauvegarde la configuration du VMS mais pas de la base de données des journaux d'activité.	La destruction physique du support de données qui possède la base de données des journaux d'activité peut empêcher le responsable du traitement de respecter ses obligations lorsqu'aucune sauvegarde des journaux d'activité n'existe.	Envisager de créer des sauvegarde de la base de données des journaux d'activité. Si le responsable du traitement décide de créer des sauvegardes de la base de données des journaux d'activités, il devrait également établir un processus pour supprimer les sauvegardes une fois atteinte la durée de rétention et le protéger contre un accès non-autorisé (par exemple, le cryptage de la sauvegarde, le blocage des multimédias de la sauvegarde, etc.). Pour plus d'informations, voir le manuel de l'administrateur pour VMS XProtect.
Utiliser un VPN en mode segmentation pourrait dévoiler l'adresse IP des	Lorsque la segmentation de tunnel est activée, les utilisateurs contournent le niveau de sécurité de la passerelle qui	Procédez de la manière suivante :

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
utilisateurs XProtect VMS.	est peut-être installée dans l'infrastructure de réseau.	• Utiliser une connexion VPN sécurisée (un VPN est sécurisé par défaut, mais certains anciens protocoles VPN ne chiffrent pas les données échangées entre le serveur et le client) • Toujours utiliser la tunnellisation complète • Utiliser les protocoles d'authentification compatibles les plus élevés (le cas échéant) • Utiliser Active Directory pour authentifier les utilisateurs de VPN Pour plus d'informations sur comment sécuriser vos installations de XProtect VMS contre les cyberattaques, voir le guide de durcissement.
Le produit permet la configuration des durées de rétention des journaux d'activité, des données vidéo, des alarmes et d'autres données à caractère personnel.	La configuration de durée de rétention sur des périodes trop longues peut enfreindre les exigences du RGPD en matière de limite de conservation (article 5 (1)(e) et article 17 du RGPD).	Les durées de rétention doivent s'adapter aux finalités du traitement (voir Droit à l'oubli (droit à l'effacement) sur la page 38).
Les administrateurs peuvent configurer les destinataires des courriers électroniques	Une faute de frappe peut provoquer une violation de données lorsqu'une partie tierce reçoit des courriers électroniques comportant des données vidéo ou des alarmes du	Informer le responsable du traitement de ce risque. Milestone recommande d'établir un processus organisationnel, tel

Problème	Impact négatif sur la confidentialité	Conseil pour le responsable du traitement
qui peuvent recevoir des extraits vidéo ou des images du VMS lorsque certains événements surviennent. Il est impossible de configurer une liste blanche des domaines autorisés pour ces destinataires de courriers électroniques.	système.	que le principe des « quatre yeux » qui réduit le risque de failles lors de la saisie des adresses électroniques.
Les notifications sont des courriers électroniques envoyés à une adresse électronique spécifique. Lors de la création d'une notification, l'administrateur peut choisir d'inclure un ensemble de captures d'écran ou un AVI d'une séquence.	Étant donné que les captures d'écran et les séquences AVI jointes aux notifications partent du VMS, elles se retrouvent hors du contrôle du VMS concernant l'accès utilisateur et la conservation.	Étant donné que les courriers électroniques et leur contenu se retrouvent hors du contrôle de l'accès utilisateur et de la conservation du VMS, il est recommandé de ne pas attacher d'images ou de séquences AVI aux notifications de courriers électroniques. Si le client a besoin de cette fonctionnalité, il doit au moins s'assurer de la mise en place de procédures et contrôles organisationnels de la part des destinataires des courriers électroniques et s'informer sur leur gestion. Voir Gestion des données exportées dans les notifications et courriers électroniques sur la page 22.

Appendice : Traitement des données dans l'environnement Milestone XProtect VMS

Le *Document sur l'architecture du système Milestone* décrit les composants du système et comment ils interagissent entre eux et avec les composants du système de l'environnement. Pour chaque cas d'utilisation du produit, vous trouverez un diagramme illustrant les flux de communication entre les composants qui sont impliqués dans les cas d'utilisation. Ces diagrammes offre une vue d'ensemble des données transférées. Pour plus d'informations sur comment les composants du Milestone XProtect VMS intéragissent, voir le document Milestone qui décrit l'architecture du système.

Cette section répertorie les processus d'installation de XProtect par défaut des données personnelles et des données d'authentification et de configuration applicables pour les paramètres de confidentialité et de sécurité.

Données personnelles du VMS

Le type de données principal sont les données vidéo des caméras vidéo. Ces données sont stockées par le service Recording Server. Les données vidéo peuvent être diffusées en direct ou en mode relecture dans le XProtect Smart Client. L'autre partie des données sont les données de base des utilisateurs VMS qui sont stockées dans la base de données SQL.

Données personnelles de l'environnement

Les données personnelles sur les utilisateurs de VMS proviennent de l'environnement dans deux circonstances :

- À partir de l'environnement Windows où Active Direct (AD) est utilisé pour l'authentification des utilisateurs et en tant que source pour les appartenances à des groupes. Le service Milestone XProtect Management Server interroge l'AD via le protocole LDAP pour recueillir les informations des utilisateurs qui se connectent au système.
- À partir des services external IDP tiers, où les utilisateurs standard sont gérés dans ce service.

Données personnelles du système

Ces données personnelles incluent toute sorte de données nécessaires pour sécuriser, configurer, exécuter, maintenir ou prendre en charge le système. Elles incluent :

- Données de journaux

  Les systèmes informatiques enregistrent habituellement les données des utilisateurs et du système dans des fichiers de journal d'activité et de débogage en vue d'aider à l'exécution et la maintenance des systèmes. XProtect Corporate procède également ainsi. Le VMS consigne les informations sur les actions des utilisateurs et les sauvegarde dans la base de données Log Server (SQL). Ce journal d'activité permet de mieux comprendre l'implication des actions et du comportement du système antérieurs et de suivre tout abus d'utilisation du système. Les journaux de débogage permettent d'identifier les défauts et failles du système. Les données de débogage ne contiennent pas de données personnelles.

  Les entrées de journal peuvent révéler des informations détaillées sur l'utilisation du système de la part des opérateurs et des administrateurs, et peuvent servir à surveiller le comportement et la peformance des employés.

- Journalisation de l'authentification

  Le serveur d'autorisation Duende OAuth et Identity Provider (IDP) créent des fichiers de journal d'activité. Ces fichiers sont sauvegardés dans la base de données Log Server (SQL), et tous les journaux de débogage ont vu les données personnelles et les marqueurs d'identité supprimés. Ces journaux d'activité sont visibles à partir du XProtect Management Client.

Données authentification et d'autorisation

- Authentification des utilisateurs dans le VMS

  Il existe trois options pour authentifier les utilisateurs VMS de XProtect Management Client et XProtect Smart Client. Vous pouvez utiliser les mécanismes de connexion de Windows, l'authentification native du VMS, ou bien utiliser un external IDP.

  Dans l'environnement Windows Active Directory, vous pouvez choisir d'utiliser le mécanisme de connexion intégré de Windows. L'authentification avec la connexion Windows se base par défaut sur le protocole Kerberos. Il s'agit de l'option la plus sécurisée. Il est possible que Kerberos ne soit pas pris en charge par les contrôleurs de domaines d'anciens environnements. Dans ce cas, la connexion Windows retombe automatiquement vers le protocole NT LAN Manager (NTLMv2), qui est connu pour être moins sécurisé que Kerberos.

  Dans les environnements dépourvus du contrôleur de domaines Windows, vous pouvez utiliser la méthode d'authentification native de XProtect, qui est l'authentification de base avec un identifiant et un mot de passe utilisateur par rapport au Identity Provider local ou à Windows pour l'authentification des groupes de travail, si cette option est disponible.

  Vous pouvez également utiliser un external IDP. Un external IDP est une application et un service externes dans lesquels vous pouvez stocker et gérer les informations sur l'identité des utilisateurs, et fournir des services d'authentification utilisateur à d'autres systèmes. Vous pouvez associer un external IDP au XProtect VMS.

  > Pour garantir la protection des données, n'utilisez pas d'IdP tiers depuis Internet. Si vous utilisez un external IDP, il doit être localement installé et géré par la même organisation ou enteprise que celle qui exécute le VMS.

  ll existe trois types d'identifiants d'authentification :

  - Les jetons de connexion de Windows (les jetons de Kerberos ou du NTLM)
  - Les identifiants d'authentification basique
  - Windows pour l'authentification des groupes de travail

  Une fois l'authentification réussie, l'utilisateur est connecté au VMS et une session utilisateur est créée par le service Management Server, où a lieu la connexion. Le client peut maintenant accéder aux fonctionnalités du service Management Server dans le contexte de cette session utilisateur. Lorsque l'utilisateur souhaite accéder aux fonctionnalités dans le service Recording Server, le XProtect Smart Client a besoin d'une session utilisateur ainsi que ce service du serveur.

- Autorisation utilisateur dans le service Recording Server

  Étant donné que la session utilisateur entre le XProtect Smart Client / XProtect Management Client et le service Management Server ne peut pas être réutilisée pour accéder au Recording Server, le Recording Server doit également autoriser l'utilisateur. Pour autoriser le service Recording Server, le service Management Server fournit au client un jeton d'autorisation, qu'il doit présenter au service Recording Server. Dans le même temps, le service Management Server envoie le jeton d'autorisation à tous les services Recording Server de l'installation VMS. Ces derniers peuvent, à leur tour, être utilisés pour autoriser les utilisateurs par la suite.

  XProtect VMS utilise un simple GUID, tel qu'un jeton d'authentification, que le client envoie au service Recording Server. Les GUID sont créés et gérés par le service Management Server, qui renouvelle ces jetons après une période donnée. Le GUID est simplement un identifiant pour l'utilisateur dans la base de données SQL Server.

- Données d'autorisation

  Les données d'autorisation pour les utilisateurs VMS sont stockées dans la base de données SQL dans un SQL Server. Au temps de démarrage, les services Management Server et Recording Server extraient les données d'autorisation concernées, y compris les jetons d'authentification pour tous les utilisateurs de la base de données SQL afin d'être prêts lors des prochains accès utilisateurs aux serveurs. Lors qu'un administrateur modifie les permissions, les rôles ou toute autre chose qui affecte l'autorisation utilisateur, cette mise à jour est stockée par le service Management Server dans la base de données SQL sur le SQL Server et propagée activement à tous les service Recording Server. Les services Recording Server stockent les données d'autorisation utilisateur et tous les jetons d'authentification localement et peut, par conséquent, authentifier immédiatement les utilisateurs client qui présentent leur jeton d'authentification.

- Données de configuration

  Outre les données des vues, qui sont configurées par le XProtect Smart Client, toutes les données de configuration du système VMS sont configurées via le XProtect Management Client du VMS et stockées dans la base de données SQL. Il existe différents types de données de configuration :

  - Paramètres d'utilisateurs et préférences
  - Autorisations d'utilisateurs
  - Configuration du serveur
  - Paramètres du système
  - Configuration des caméras et périphériques

  Bien que les données de configuration peuvent ne pas contenir de données personnelles, elles peuvent néanmoins affecter la manière dont le VMS traite les données personnelles. À titre d'évaluation seulement, les informations d'autorisation et les paramètres de sécurité et de confidentialité parmi les données de configuration répertoriées ci-dessus sont importantes.

helpfeedback@milestone.dk

À propos de Milestone

Milestone Systems est un fournisseur leader de l'édition de logiciels de gestion de vidéo sur plate-forme ouverte : une technologie qui permet au monde de découvrir comment garantir la sécurité, protéger les actifs et augmenter l'efficacité commerciale. Milestone Systems permet une communauté de plate-forme ouverte qui alimente la collaboration et l'innovation par le développement et l'utilisation de la technologie de la vidéo en réseau, avec des solutions fiables et évolutives qui ont fait leurs preuves sur plus de 150 000 sites à travers le monde. Fondée en 1998, Milestone Systems opère en tant que société autonome du Canon Group. Pour plus d'informations, rendez-vous à l'adresse https://www.milestonesys.com/.