RECOMMANDATIONS SUR LA VIDÉOSURVEILLANCE

FGS
Forum Genevois de la Sécurité

www.fgsonline.ch

JUIN 2016

TABLE DES MATIÈRES

FORUM GENEVOIS DE LA SÉCURITÉ

Le Forum Genevois de la Sécurité (ci-après FGS ou forum) est une association destinée aux professionnels des métiers de la sécurité, dont les objectifs sont de favoriser:

> la **convergence** entre les différentes spécialités de la sûreté, de la sécurité incendie, de la sécurité au travail et de la sécurité de l'information, afin de partager des bonnes pratiques, harmoniser les méthodes et le vocabulaire, et

> la **communication** entre spécialistes mais aussi et surtout des départements sécurité vers toutes les parties prenantes que sont les utilisateurs, les décideurs ou encore les partenaires externes comme les autorités.

Afin de rendre ce document vivant, nous vous invitons à envoyer vos remarques, constatations ou axes de développement futurs par courriel à l'adresse suivante: cctv@fgsonline.ch

Les recommandations sont disponibles au format PDF sur les sites internet suivants:

> **www.fgsonline.ch**
Site du Forum Genevois de la Sécurité

> **www.ge.ch/ppdt**
Site du préposé cantonal à la protection des données et à la transparence

GROUPE DE TRAVAIL VIDÉOSURVEILLANCE

L'idée de créer un document portant sur les bonnes pratiques de la vidéosurveillance est née en 2011, suite à une formation approfondie dans le domaine de la vidéosurveillance forensique, et a trouvé un écho favorable au sein du comité du Forum Genevois de la Sécurité (ci-après: FGS).

Le FGS a mis sur pied un comité de pilotage et lui a donné pour mission d'élaborer un guide sur le sujet afin d'aider les organisations à investir dans des systèmes performants, adaptés à leurs besoins, en accord avec la loi et utilisant des formats et pratiques exploitables par la Justice. Le comité de pilotage, constitué d'Yves-Alain Hirschi (président du groupe de travail), Arnaud Ducrot et Pierre-Antoine Gämperlé, a défini la stratégie nécessaire à l'atteinte des objectifs fixé, à savoir remettre une version finalisée des recommandations en 2015.

Le comité de pilotage s'est entouré de professionnels (voir ci-après "crédits") en fonction des thématiques abordées afin de définir la structure du document et d'en rédiger les contextes, procédures et fiches (légales et techniques) qui sont à disposition.

> Crédits

BRACONE Piero
Directeur / Associé, Jomos Romandie SA

CABESSA Jean-Marc
Ingénieur sécurité

DUBOIS Isabelle
Expert en protection des données, AD HOC Résolution

DUCROT Arnaud
CTO, Protectas SA
Président du comité FGS

GÄMPERLE Pierre-Antoine
Chef de secteur commercial & conduite, Securitas SA
Membre du comité FGS

HIRSCHI Yves-Alain
Deputy CIO, État-major Police Genève
Membre du comité FGS

JAGGI Jean-Paul
Chef d'entreprise, ETAVIS TSA SA

MALLERET Jacques
Inspecteur du travail, OCIRT

MARTINEZ Juan-Carlos
Ingénieur sécurité, Office des bâtiments

MODIFICATIONS DANS LA VERSION 2016

La version des recommandations sur la vidéosurveillance de juin 2016 propose une mise à jour du glossaire et une refonte de la "procédure technique extraction" intégrant les notions issue du Code de procédure pénale suisse (CPP RS 312.0) comme suit:

> actualisation du schéma avec ajout de la demande de préservation de séquence;
> création de la fiche technique "demande de préservation";
> actualisation de la fiche technique "demande d'extraction";
> actualisation de la fiche technique "communication des extractions";
> création de la fiche technique "traçabilité".

PRÉAMBULE

La vidéosurveillance est un outil qui s'inscrit dans un concept global de sécurité.

Notamment par l'enregistrement de données filmées, elle constitue une atteinte sérieuse à la sphère privée. Vu la difficulté de recueillir le consentement des personnes concernées, sa mise en œuvre doit répondre à des exigences strictes.

Par conséquent, avant toute installation de système de vidéosurveillance, on doit se demander quels risques on veut couvrir (déprédations, atteintes à la propriété ou à l'intégrité physique, sauvegarde de preuves, contrôle d'accès, ..) par le raisonnement suivant:

> quel(s) objectif(s) on vise (opérationnel ou enquête – les deux ?),
> s'il(s) pourrai(en)t être atteint(s) par une mesure moins intrusive,
> quelle(s) autre(s) mesure(s) est (sont) prise(s) en parallèle.

Pour rappel, une stratégie de sécurité efficace comporte trois composantes:

> technique (vidéosurveillance, alarme anti-intrusion, système électronique de contrôle d'accès, …),
> organisationnelle (concept de sécurité, procédure d'utilisation des systèmes, …),
> humaine (visionnement des enregistrements, intervention sur alarme, rondes, …).

Enfin, le besoin ultime pourrait être la collecte de moyens de preuves à fournir à la Justice.
Il s'agira donc de s'assurer également que ceux-ci soient probants.

C'est sur ces bases que nos recommandations ont été élaborées.

DEMARCHE

Après avoir traversé le "préambule", qui fournit les bases de la réflexion, une "marche à suivre" permet d'obtenir une vision plus précise du projet. Par la suite, deux contextes sont proposés:

Le contexte légal permet de valider une installation en place ou un futur projet dans le respect des obligations légales, notamment en matière de protection des données. Il est enrichi de fiches légales permettant d'obtenir des informations plus détaillées sur les points abordés.

Le contexte technique détaille six procédures clés d'un système de vidéosurveillance: prise de vue, transmission, stockage, exploitation, extraction et maintenance. Chaque procédure est enrichie de fiches techniques permettant d'obtenir des informations détaillées.

L'annexe contient une conclusion, une liste de contacts utiles (préposé fédéral et préposés cantonaux à la protection des données et à la transparence) ainsi que des liens internet régulièrement mis à jour.

MARCHE À SUIVRE

Cette marche à suivre, non exhaustive, permet de guider les organisations dans leur démarche de déploiement d'un système de vidéosurveillance:

> Préambule

- ❏ Définir les objectifs visés
- ❏ Définir la stratégie de sécurité efficace
- ❏ Définir le contexte légal
- ❏ Définir le contexte budgétaire
- ❏ Définir le contexte technique

> Définition des responsabilités légales

- ❏ Définir le maître du fichier
- ❏ Définir le(s) responsable(s) de l'exploitation et de la maintenance du système

> Définition des besoins en termes de prise de vue

- ❏ Établir un plan des vues ou champs de vision souhaités (surface surveillée)
- ❏ Définir le type de caméra (fixe / PTZ, analogique / numérique, sans / avec son, noir et blanc / couleur / thermique, …) avec son boîtier (chauffage, anti-vandale) et son type de fixation (anti-arrachement)
- ❏ Définir le type d'objectif (angle de vue, sensibilité, …)
- ❏ Définir les besoins en éclairage (naturel, d'appoint, infrarouge, …)
- ❏ Prendre en compte les éléments naturels (soleil, contrejour, intempéries, climat)

> Définition des besoins en termes de transmission des données

- ❏ Définir les besoins du réseau informatique (bande passante, redondance, filaire ou non, PoE, …)
- ❏ Définir le niveau de sécurisation (QOS, SLA, DVR / NVR, réseau, lecture, relecture, exportation, …)
- ❏ Établir des procédures de transmissions de données (vidéo, photo, main courante ou journal de bord, ...)

> Définition des besoins en termes de stockage

- ❏ Définir le type d'enregistrement (pré / post, sur événement, …)
- ❏ Définir le type de stockage et archivage (RAID, nb de jours, résolution, compression, …)
- ❏ Définir les supports (DVR, NVR, NAS, NAS dédié, SAN, …)
- ❏ Définir la sécurisation physique des équipements de stockage (contre le vol ou a détérioration en cas de cambriolage par exemple)

> Définition des besoins en termes d'exploitation

- ❏ Définir le type de visualisation (opérationnel / enquête, …)
- ❏ Définir les besoins en analyse d'image en direct (aide à l'engagement)
- ❏ Définir les besoins en analyse d'image en différé (sur enregistrement)

> Définition des besoins en termes d'extraction

- ❏ Établir le champ documentaires relatifs aux extractions (demande, rapport, remise, …)
- ❏ Définir le cadre relatifs des extractions (qui peut demander quoi, comment, …)
- ❏ Définir les procédures et guides pour la réalisation des extractions
- ❏ Etablir le type d'extraction à disposition (natif, tiff, jpg, par courriel, type de support, …)

> Définition des besoins en termes de maintenance

- ❏ Définir le niveau de qualité de service (QOS, SLA, réparation, maintenance) dans le contrat
- ❏ Définir le type de maintenance souhaitée (préventive ou corrective)

CONTEXTE LÉGAL

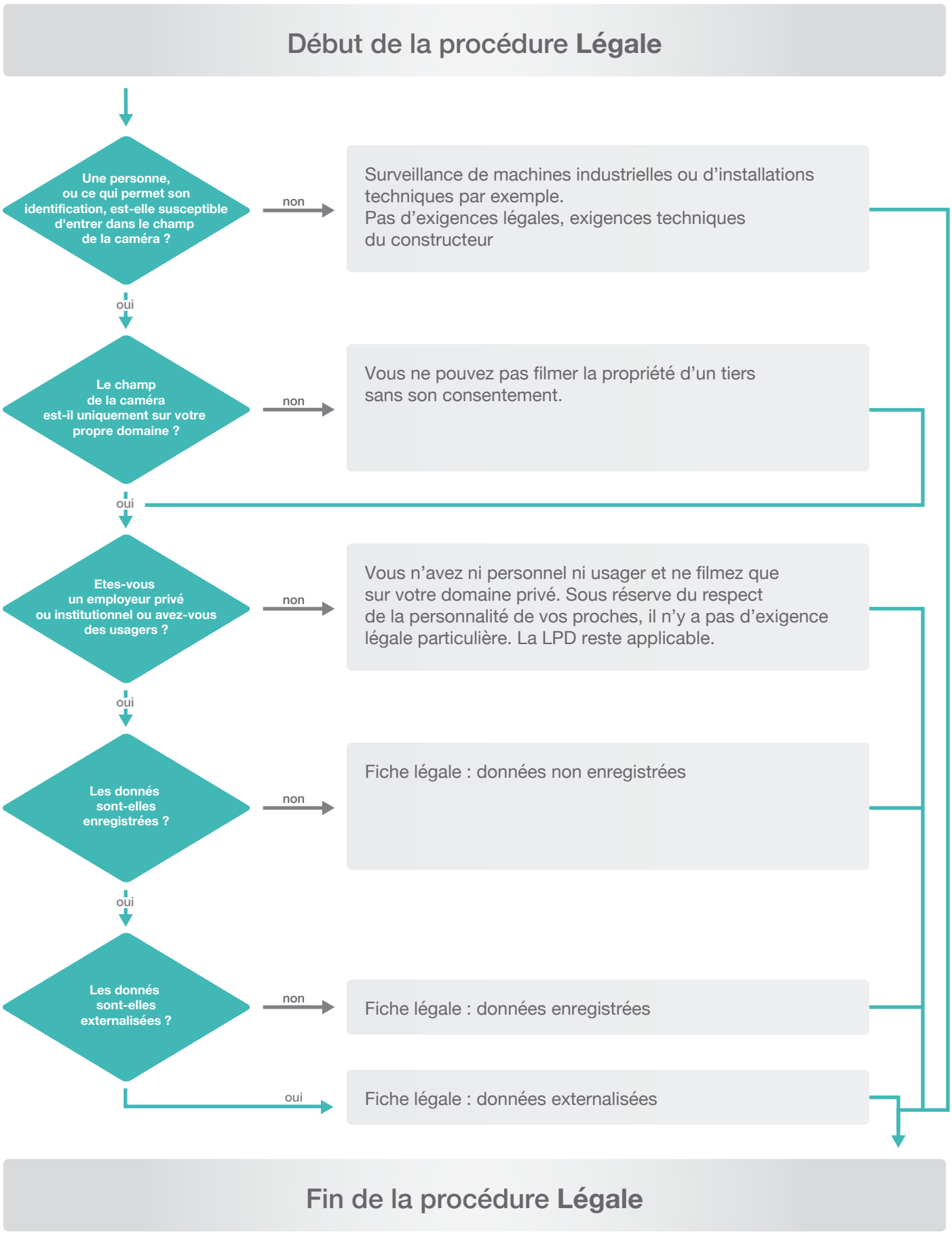
Tout organisme, qu'il soit privé ou public, doit respecter la législation lors de la mise en place d'un système de vidéosurveillance.

S'appliquent essentiellement, dans ce contexte:

> la loi fédérale sur la protection des données (LPD / RS 235.1);
> la loi cantonale sur l'information du public, l'accès aux documents et la protection des données (LIPAD / rsGE A 2 08)
> la loi fédérale sur le travail (LTr / RS 822.11)
> les ordonnances fédérales relative à la sur le travail (OLT 1 à 5 / RS 822.111 à 822.115)

Les conditions-cadres étant les mêmes en droit fédéral et en droit cantonal, la procédure présentée ci-après peut être suivie par tout organisme.

PROCÉDURE LÉGALE



FICHE LÉGALE DONNÉES NON ENREGISTRÉES

LES DONNÉES NE SONT PAS ENREGISTRÉES

> Les caméras doivent être signalées de manière adéquate au public et au personnel.
> Le champ de la caméra doit être limité au périmètre nécessaire à la surveillance.
> Le personnel doit être hors champ ou, à défaut, non identifiable.
> L'objectif de la vidéosurveillance doit être clairement annoncé aux travailleurs ; sauf exception, une surveillance systématique du comportement des travailleurs à leur poste de travail est interdite.
> Le visionnement des données, en direct, doit être limité à un cercle restreint de personnes dûment autorisées ; s'agissant des institutions publiques, la liste à jour de ces personnes doit être communiquée au préposé cantonal.

SOURCES:

> http://www.ge.ch/legislation /
A 2 08, LIPAD, art. 42
> https://www.admin.ch/gov/fr/accueil/droit-federal/recueil-systematique.html
RS 220, CO (Code des obligations), art. 328 et 328bis
> http://www.edoeb.admin.ch/themen/00794/00800/00911/index.html?lang=fr
Préposé fédéral, explications sur la vidéosurveillance sur le lieu de travail
> http://www.edoeb.admin.ch/dokumentation/00445/00507/00603/index.html?lang=fr
Préposé fédéral, vidéosurveillance de l'espace privé, effectuée par des particuliers
> http://www.edoeb.admin.ch/themen/00794/00800/01765/index.html?lang=fr
Préposé fédéral, vidéosurveillance de l'espace public, effectuée par des particuliers
> http://www.admin.ch/ch/f/rs/8/822.113.fr.pdf
art. 26 de l'ordonnance 3 relative à la LTr (loi sur le travail)
> http://www.seco.admin.ch,
commentaires de l'art. 26 OLT 3 (Ordonnance relative à la LTr)

FICHE LÉGALE DONNÉES ENREGISTRÉES

LES DONNÉES SONT ENREGISTRÉES ET VOUS ÊTES UN EMPLOYEUR PRIVÉ OU INSTITUTIONNEL OU AVEZ DES USAGERS

> Les caméras doivent être signalées de manière adéquate au public et au personnel.
> Le champ de la caméra doit être limité au périmètre nécessaire à la surveillance.
> Le personnel doit être hors champ ou, à défaut, non identifiable.
> L'objectif de la vidéosurveillance doit être clairement annoncé aux travailleurs ; sauf exception, une surveillance systématique du comportement des travailleurs à leur poste de travail est interdite.
> Le visionnement des données ne doit intervenir qu'en cas de nécessité et être limité à un cercle restreint de personnes dûment autorisées. S'agissant des institutions publiques, la liste à jour de ces personnes doit être communiquée au préposé cantonal.
> La destruction des enregistrements doit intervenir dans les plus brefs délais (si possible après 24 heures mais au plus tard après 7 jours pour le secteur public), sauf atteinte avérée et procédure ouverte.
> La sécurité des installations et des données enregistrées doit être garantie.
> Les données enregistrées ne peuvent être communiquées qu'à des fins de preuve et uniquement aux instances hiérarchiques et aux autorités judiciaires.
> Le fichier des images enregistrées doit être déclaré au catalogue des fichiers (au préposé genevois pour les institutions publiques genevoises, au préposé fédéral pour les privés)

SOURCES:

> http://www.ge.ch/legislation/
A 2 08, LIPAD, art. 42
> https://www.admin.ch/gov/fr/accueil/droit-federal/recueil-systematique.html
RS 220, CO (Code des obligations), art. 328 et 328bis
> http://www.edoeb.admin.ch/datenschutz/00625/00729/index.html?lang=fr
(Vidéosurveillance) :
explications sur la vidéosurveillance sur le lieu de travail
vidéosurveillance de l'espace privé, effectuée par des particuliers
vidéosurveillance de l'espace public, effectuée par des particuliers
> http://www.admin.ch/ch/f/rs/8/822.113.fr.pdf
art. 26 de l'ordonnance 3 relative à la loi sur le travail
> http://www.seco.admin.ch
commentaires de l'art. 26 OLT 3 (Ordonnance relative à la LTr)
> http://www.ge.ch/ppdt/espace-citoyen/catalogue.asp
CATFICH : catalogue des fichiers

FICHE LÉGALE EXTERNALISATION DES DONNÉES ET INFORMATIQUE EN NUAGE

DÉFINITIONS

On entend par **externalisation des données** le fait de confier à un tiers, le sous-traitant, tout ou partie du traitement des données personnelles, par exemple la conservation (stockage). Si le tiers ne conserve pas les données confiées sur ses serveurs, dans un lieu géographiquement circonscrit, mais au sein d'un réseau virtuel, on parle d'**informatique en nuage**. L'environnement informatique n'est plus la propriété de l'entreprise ou de l'autorité et n'est plus géré par elle mais est loué à un ou plusieurs prestataires de services. Le nuage peut être privé ou public, voire les deux et peut être partagé par plusieurs organisations.

RISQUES ET ENJEUX

L'enjeu essentiel pour les organismes est de réduire les coûts d'infrastructure informatique, de disposer d'une plus grande capacité de stockage et de calcul via la souplesse d'utilisation que propose le système. Les risques généraux de la sous-traitance sont la perte de données, les pannes de systèmes et l'indisponibilité des données ainsi qu'un usage abusif des données. S'y ajoutent avec l'informatique en nuage : la perte de contrôle sur les données, le manque de séparation et d'isolation des données, l'accès d'autorités étrangères aux données (via eDiscovery par exemple), la captivité et le non-respect des dispositions légales. Le maître de fichier reste responsable du traitement des données personnelles, et le sous-traitant le devient dans la mesure de son contrat.

RÈGLES À RESPECTER

Pour sous-traiter le traitement de données personnelles il faut qu'une loi le prévoie ou qu'une convention soit conclue, que les données ne soient pas couvertes par un secret et que la sécurité soit garantie par le tiers (art. 10a LPD, et 35, 37, 43 al. 3 b) LIPAD). Si le traitement est effectué à l'étranger (informatique en nuage notamment) il faut encore s'assurer que toutes les conditions légales au traitement des données personnelles soient respectées. Dans le cadre de l'union européenne le niveau législatif est adéquat, mais tel n'est pas le cas d'autres pays et des garanties suffisantes concernant la sécurité des données doivent être obtenues.

Le responsable de traitement doit s'assurer que l'ensemble des lieux d'hébergement (y compris de sauvegarde) répondent aux exigences de sécurité et aux obligations légales. Il doit garder la maîtrise sur les données qu'il traite car il est notamment tenu d'accorder le droit d'accès (art. 8 LPD et 44 LIPAD) et le droit d'effacer ou de rectifier les données (art. 5 LPD et 47 LIPAD).

RECOMMANDATIONS

Sur la base d'une convention prévoyant toutes les garanties nécessaires au respect des règles légales par le sous-traitant, et permettant le contrôle de ces conditions par le maître de fichier, la conservation de données enregistrées de vidéosurveillance par un tiers est possible. La sous-traitance de ces données en dehors de Suisse ou du territoire de l'Union européenne est vivement déconseillée.

SOURCES:

> http://www.ge.ch/legislation/
A 2 08, LIPAD
> http://www.admin.ch/opc/fr/classified-compilation/19920153/index.html
RS 235.1 LPD
> http://www.edoeb.admin.ch/datenschutz/00683/00877/index.html?lang=fr
Explications du PFPDT sur l'informatique en nuage
> http://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf
Maîtriser les risques de l'infogérance
> http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/cloud-computing-les-7-etapes-cles-pour-garantir-la-confidentialite-des-donnees/
Fiche pratique de la CNIL sur le cloud computing

CONTEXTE TECHNIQUE

Une fois opérée l'analyse des besoins et objectifs de l'installation d'un système de vidéosurveillance (cf. Préambule) et la prise en compte du contexte légal, le choix du système se fera en définissant de manière préalable le type de surveillance recherché.

Pour chaque question, des commentaires sont formulés et renvoient à une fiche précisant les conditions techniques à prendre en compte pour chaque situation concrète rencontrée.

Prise de vue
Définition de la qualité de l'image, de l'endroit de la mesure et du point de focale.

Transmission
Définition des besoins relatifs au transport sécurisé des données.

Stockage
Définition des mesures organisationnelles.

Exploitation
Définition des besoins relatifs au centre d'exploitation.

Extraction
Définition des étapes clés.

Maintenance
Définition des besoins relatifs à la maintenance.

PROCÉDURE PRISE DE VUE

PRISE DE VUE

Début de la procédure **Prise de vue**

SURVEILLANCE ? — oui

Permettrait d'avoir une compréhension sommaire d'un événement afin de déclencher ou non une action.

FICHES TECHNIQUES
Surveillance
Endroit de la mesure
Profondeur de champ

non

DÉTECTION ? — oui

Permettrait de faire de la levée de doute, de différencier des individus entre eux et de comprendre leur interaction afin de déclencher ou non une action.

FICHES TECHNIQUES
Détection
Endroit de la mesure
Profondeur de champ

non

RECONNAISSANCE ? — oui

Permettrait de reconnaître un individu ou un objet pour autant qu'il ait déjà été vu auparavant.

FICHES TECHNIQUES
Reconnaissance
Endroit de la mesure
Profondeur de champ

non

IDENTIFICATION ? — oui

Permettrait d'identifier un individu ou un objet avec une grand probabilité.

FICHES TECHNIQUES
Identification
Endroit de la mesure
Profondeur de champ

Fin de la procédure **Prise de vue**

FICHE TECHNIQUE SURVEILLANCE

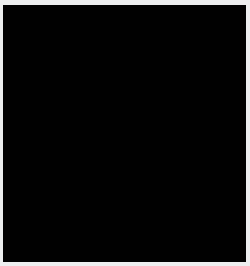
Les chiffres énoncés ci-dessous sont à prendre avec circonspection parce que de nombreuses conditions minimales, comme le rendu de couleur, la luminosité, l'angle de vue, le type de compression utilisé, la qualité de la caméra, etc., sont requises pour définir la qualité d'une image, cette dernière ne se limitant pas au nombre de pixels par mètre.

Ces fiches techniques seront développées lors de parutions ultérieures à l'aide de conseils avisés d'invités (faisant partie du troisième cercle) possédant de l'expérience ou des compétences techniques reconnues.

FICHES TECHNIQUES

SURVEILLANCE
Entre environ 1 et 30 pixels par mètre linéaire à l'endroit de la mesure (cf. fiche technique 2 : endroit de la mesure).

Exemple: (source des images: www.avigilon.com)



FICHE TECHNIQUE DÉTECTION

FICHES TECHNIQUES

DÉTECTION
Entre environ 30 et 50 pixels par mètre linéaire à l'endroit de la mesure (cf. fiche technique 2 : endroit de la mesure)..

Exemple: (source des images: www.avigilon.com)

FICHE TECHNIQUE RECONNAISSANCE

FICHES TECHNIQUES

RECONNAISSANCE
Entre environ 50 et 80 pixels par mètre linéaire à l'endroit de la mesure (cf. fiche technique 2 : endroit de la mesure).

Exemple: (source des images: www.avigilon.com)

http://www.edoeb.admin.ch/dokumentation/00445/00472/01369/index.html?lang=fr

Préposé fédéral, guide relatif aux systèmes de reconnaissance biométrique.

FICHE TECHNIQUE IDENTIFICATION

FICHES TECHNIQUES

IDENTIFICATION
Au-dessus d'environ 80 pixels par mètre linéaire à l'endroit de la mesure (cf. fiche technique 2 : endroit de la mesure).

Exemple: (source des images: www.avigilon.com)

IDENTIFICATION DE PLAQUES

Définition minimale de l'image à l'endroit de la mesure: environ 100 pixels par mètre linéaire.

IDENTIFICATION D'INDIVIDUS

Définition minimale de l'image à l'endroit de la mesure, pour une identification automatique assistée par un logiciel spécialisé : environ 80 pixels entre les pupilles.

http://www.edoeb.admin.ch/dokumentation/00445/00472/01369/index.html?lang=fr

Préposé fédéral, guide relatif aux systèmes de reconnaissance biométrique.

FICHE TECHNIQUE ENDROIT DE LA MESURE

FICHES TECHNIQUES

ENDROIT DE LA MESURE

La notion de calcul à l'endroit de la mesure peut sembler abstraite mais elle est en réalité triviale après quelques explications.

Une fois l'image capturée par le système de vidéosurveillance, il faut l'exporter sans en affecter la qualité (tiff par exemple) et l'ouvrir dans un logiciel de traitement d'image (Adobe Photoshop par exemple). À l'aide de l'outil de calcul de la longueur (règle), positionner sur « pixel », mesurer l'objet en question. Le résultat donné correspondra au nombre de pixels (dans l'exemple - 28 pixels entre les yeux) :

Exemple: (source des images: www.avigilon.com)

FICHE TECHNIQUE PROFONDEUR DE CHAMP

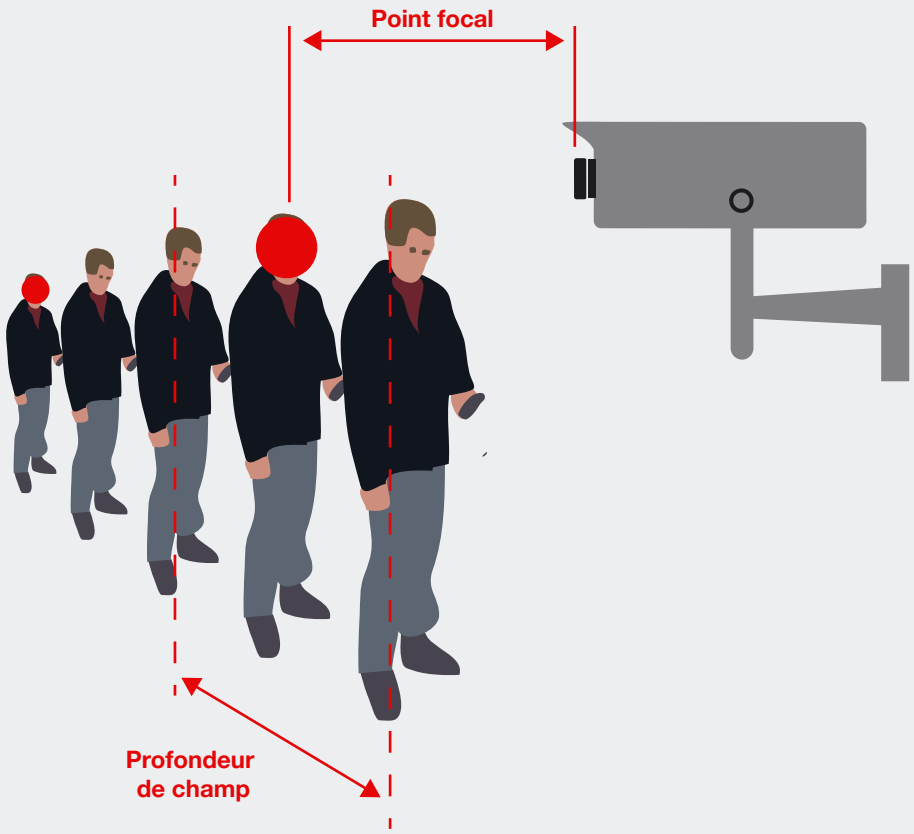
La notion de profondeur de champ peut être simplement expliquée par le schéma suivant:

Le **point de focale** permet d'avoir une zone de netteté définie (petite profondeur de champ) alors que les caméras actuelles ont une grande profondeur de champ (net partout - empiétement sur les sphères publique ou privée tierces). Un réglage pourrait permettre de restreindre la violation de ces sphères.

Les points rouges symbolisent **l'endroit de la mesure**. Si on veut identifier un individu, il faut se poser la question de sa position dans la profondeur de champ.

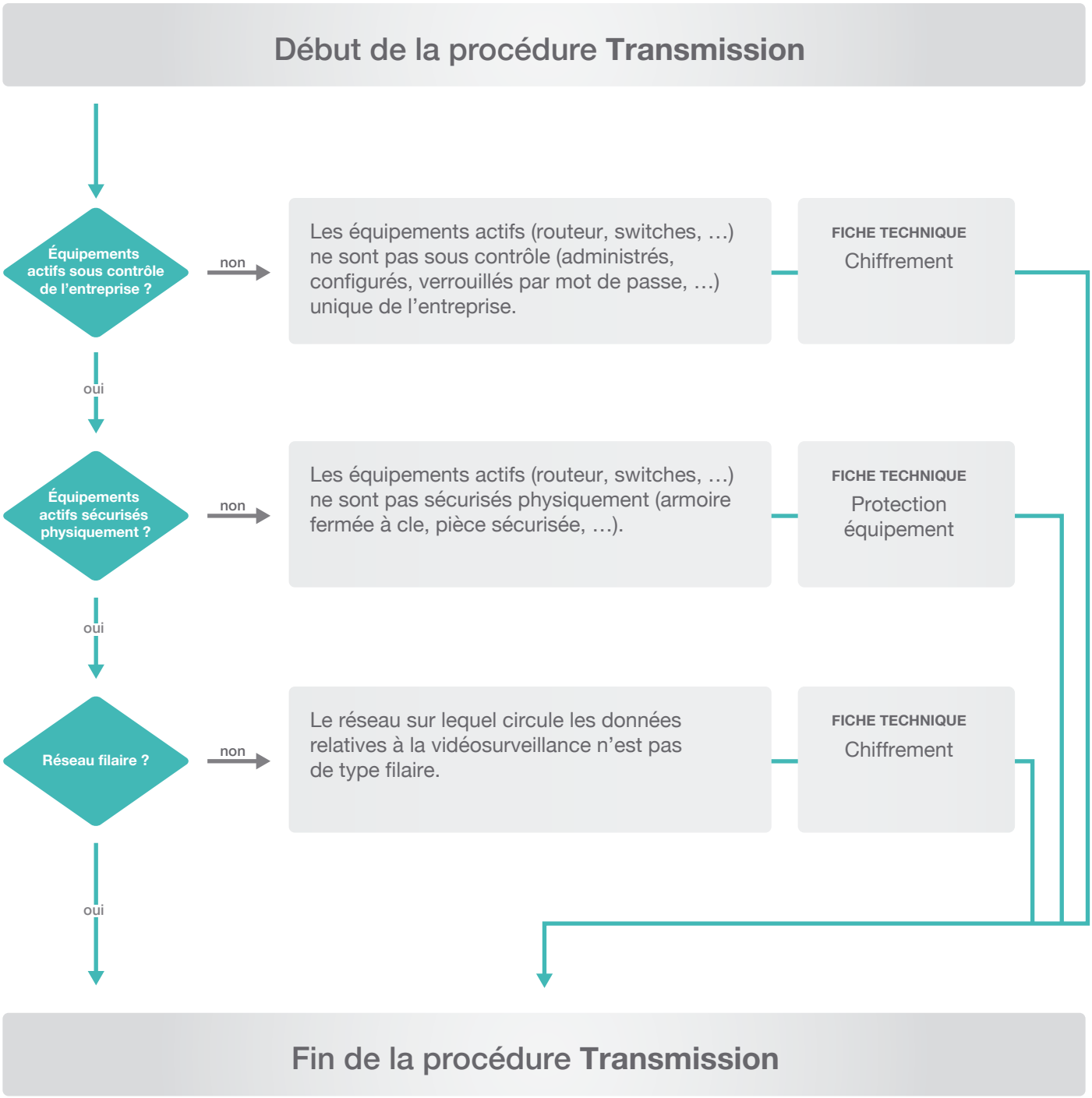
Taille de la tête - avant:

Taille de la tête - arrière:



PROCÉDURE TRANSMISSION

TRANSMISSION



FICHE TECHNIQUE CHIFFREMENT

Pour permettre d'échanger sans risque des données entre un ou plusieurs systèmes, des équipements actifs ou passifs ainsi que des protocoles ont été créés et développés. Ils assurent la sécurité au sens large (confidentialité, intégrité, authenticité) de l'information transportée.

A ce jour, nous recommandons le plus connu d'entre eux le TLS –Transport Layer Security (autrefois nommée SSL – Secure Socket Layer). Son objectif est de créer un tunnel sécurisé entre un client et un serveur (caméra et son système de stockage).

FICHE TECHNIQUE PROTECTION ÉQUIPEMENT

Afin de pouvoir acheminer les données sensibles d'un bout à l'autre des infrastructures techniques, un certain nombre d'équipements passifs (hub, câblage, …) et actifs doivent être mis en place (routeur, switch, …).

Ces éléments sont en général localisés dans des armoires ou des locaux prévus à cet effet.

L'un des risques principaux prend la forme d'un accès physique non autorisé. Si la protection n'est pas correctement déployée, un certain nombre de moyens peuvent être mis en œuvre pour accéder et voler des données (sniffing) ou prendre la main sur l'appareil afin de transmettre l'information ailleurs.

Ces éléments, actifs ou passifs, doivent être sécurisé physiquement, dans des locaux fermés (clé, badge, ...). Des moyens annexes (directs ou/et indirects) peuvent être mis en œuvre pour accentuer la sécurité comme de la surveillance vidéo ou par analyse régulière des journaux d'entrées par exemple.

FICHE TECHNIQUE CALCUL BANDE PASSANTE

Les exigences relatives à la bande passante doivent impérativement être prises en considération lors de la conception d'un système de vidéosurveillance.

Ces facteurs importants tiennent compte du nombre de caméras, la résolution d'image utilisée, le type et le rapport de compression, les fréquences d'images et la complexité des scènes.

Les produits de vidéo sur IP utilisent la bande passante réseau en fonction de leur configuration selon les critères non exhaustifs suivants:

> Nombre de caméras
> Type d'enregistrement (continu ou séquentiel - basé sur des événements)
> Nombre d'images visualisées
> Nombre d'écrans de visualisation (en fonction du nombre d'images par seconde)
> Nombre d'images par seconde (FPS : frame per seconde - IPS : image par seconde)
> Résolution d'image
> Type de compression vidéo (Motion JPEG, MPEG-4, H.264, …)
> Scène : complexité de l'image (par exemple mur gris, forêt, etc.)
> Conditions d'éclairage
> Mouvement (environnement statique - bureau - ou dynamique - gares)

Pour plus d'information, des sites professionnels peuvent être consultés, tel que:
http://www.axis.com/fr/products/video/about_networkvideo/bandwidth.htm
http://www.axis.com/fr/products/video/design_tool/ (configurateur en ligne)

PROCÉDURE STOCKAGE

Début de la procédure **Stockage**

Stockage on Edge ?

oui → Le stockage des données de vidéosurveillance (données et métadonnées) se fait sur de support localisé dans la caméra.

FICHE TECHNIQUE
On Edge

non

Stockage centralisé en interne ?

oui → Le stockage des données de vidéosurveillance (données et métadonnées) se fait sur un support localisé dans l'entreprise.

FICHE TECHNIQUE
Stockage centralisé en interne

non

Stockage externalisé DaaS ?

oui → Le stockage des données de vidéosurveillance (données et métadonnées) se fait dans le cloud.

FICHE TECHNIQUE
Stockage externalisé DaaS

FICHE LÉGALE
Externalisation des données et informatique en nuage

non

Fin de la procédure **Stockage**

FICHE TECHNIQUE CONSIDÉRATIONS RELATIVES AU STOCKAGE

Les exigences relatives au stockage (ainsi qu'à la bande passante - cf procédure transmission, calcul de la bande passante) doivent impérativement être prises en considération lors de la conception d'un système de vidéosurveillance. Ces facteurs importants peuvent être:

> Le nombre de caméras;
> Le type d'enregistrement (continu, sur événements);
> Nombre d'heures d'enregistrement quotidien par la caméra;
> Images par seconde;
> Résolution de l'image;
> Type de compression vidéo (Motion JPEG, MPEG-4, H.264, …)
> Complexité de la compression (zones identiques, conditions d'éclairage, …);
> Mouvement (environnement de bureau ou gares ferroviaires bondées);
> Durée de conservation souhaitée des données.

Exemple de calcul pour une carte SD/SDHC de 32Gb*:

Jours	Stockage / jour*(Go)	Image par seconde	Résolution de la caméra
45	0.7	15	VGA
27	1.2	30	VGA
19	1.7	10	HDTV 720p
9	3.6	30	HDTV 720p

* Les chiffres sont calculés, en fonction d'une compression de 30 % H.264, d'une détection de mouvements de 20 % et d'une scène d'agitation moyenne (www.axis.com).

FICHE TECHNIQUE ON EDGE

Type de support	Carte mémoire (SD, Micro-SD)
Capacité max	64GB
Avantage	Coûts Simplicité d'installation et mise en œuvre Aucun matériel complémentaire
Désavantage	Capacité de stockage limitée Aucune redondance Sécurité physique limitée (renforcer accès, boîtier, …) Sécurité de l'information (voir partie légale)

Le stockage Edge est une fonctionnalité des caméras et des encodeurs vidéo sur IP, permettant l'enregistrement des images sur un support de stockage (par exemple SD) embarquée dans la caméra. On y fait parfois référence sous l'appellation de "stockage local" ou "d'enregistrement embarqué".

Ce stockage décentralisé (sur chaque caméra) permet une diminution des coûts d'enregistrement (pas de serveur de stockage) et de la flexibilité de mise en œuvre pour des utilisations uniques (magasin, surveillance de chantier, surveillance mobile) ou multiples (chaîne de magasins, flotte de véhicules, …).

Cette conception de stockage décentralisé permet de palier aux problèmes lié à la faiblesse de la bande passante (limitée, intermittente ou absente) dans les utilisations suivantes:

> visionner en direct un flux vidéo dégradé (basse résolution pour comprendre l'événement) et garder les images non dégradées (haute résolution pour investigation) sur le support de stockage de la caméra;
> téléchargement des images stockées sur un serveur centralisé à la demande ou sur planification (pour une utilisation appropriée de la bande passante la nuit par exemple) ou en fonction d'un incident;
> redondance en cas d'interruption de la bande passante entre la caméra et un serveur centralisé (permet de garder les images en local).

Il faut cependant prendre en compte la faiblesse de la protection des données.
En effet, la carte mémoire de la caméra peut être accédée (vol, copie, destruction, …) si une protection (boîtier fermé à clé, inaccessibilité de caméra, autre protection active ou passive) fait défaut (cf procédure transmission - fiche technique "protection équipement").

FICHE TECHNIQUE STOCKAGE CENTRALISE EN INTERNE

Type de support	NVR, NAS, serveur de fichiers
Capacité max	Stockage flexible et illimité
Avantage	Capacité de stockage illimitée Redondance possible Vitesse de consultation Gestion centralisée
Désavantage	Coûts proportionnels à la capacité Maintenance à prévoir Connaissances spécifiques nécessaires pour la mise en œuvre

STOCKAGE BASÉ SUR SERVEUR

Le nombre de caméras, la taille d'image et le nombre d'images par seconde que peut gérer un serveur PC dépendent de l'unité centrale (UC), de la carte réseau et de la mémoire RAM (Random Access Memory) interne dont dispose le serveur. La plupart des PC possèdent entre deux et quatre disques durs, chacun pouvant contenir (environ) jusqu'à 300 Go de données. Dans une installation de petite à moyenne envergure, le PC qui exécute le logiciel de gestion vidéo est également utilisé pour l'enregistrement vidéo. On appelle cela le stockage embarqué (DAS, Direct-Attached Storage).
Avec un logiciel de gestion vidéo centralisé, par exemple, un disque dur est suffisant pour stocker les enregistrements de six à huit caméras. Avec 12 à 15 caméras ou plus, il est nécessaire d'utiliser au moins deux disques durs, afin de répartir la charge. Pour plus de 50 caméras, l'utilisation d'un deuxième serveur est recommandée.

CONFIGURATIONS SYSTÈME

Un système de petite envergure (de 1 à 30 caméras) peut être composé d'un serveur qui exécute toutes les tâches:

> gestion et configuration du réseau;
> enregistrement des vidéos en interne;
> affichage des images en directe;
> relecture des images en différé;
> possibilité de connecter un client (local ou distant) pour effectuer les mêmes opérations.

Un système de moyenne envergure (de 25 à 100 caméras) peut être composé d'un serveur dédié au stockage et l'autre dédié aux tâches suivantes:

> gestion et configuration du réseau;
> affichage des images en directe;
> relecture des images en différé;
> possibilité de connecter un client (local ou distant) pour effectuer les mêmes opérations.

Un système centralisé de grande envergure (de 50 à 1000 caméras, voire plus) peut être composé de plusieurs serveurs dédiés aux tâches particulières (gestion et configuration, stockage, visualisation en direct, relecture, …) afin d'offrir de solides performances (load balancing) et une fiabilité importante (redondance matérielle et données) dans le traitement d'une grande quantité de données. Cette configuration offre la possibilité de faire évoluer le système (maintenance, ajout d'équipements, …) sans arrêter l'ensemble du système.

FICHE TECHNIQUE STOCKAGE EXTERNALISE (DaaS - data as a service)

Type de support	Espace de stockage sur un ou plusieurs serveurs appartenant à un prestataire de services
Capacité max	Évolutive
Avantage	Pas d'investissement de matériel et personnel Maintenance assurée par le prestataire Mitigation des risques en cas de désastre
Désavantage	Coûts du service Offres disponibles limitées Sécurisation des données (voir partie légale) Nécessite une haute bande passante Étude des conditions générales

Les informations dans ce domaine étant très changeantes, il y a lieu de se référer à Internet pour toutes recherches actualisées.

PROCEDURE EXPLOITATION

EXPLOITATION

Début de la procédure **Exploitation**

Visualisation en direct ?

oui

Le système permet la visualisation en directe (live) dans un centre d'exploitation (local ou déporté) sur un ou plusieurs écrans de contrôle.

FICHE TECHNIQUE
Centre d'exploitation

non

Analyse d'images en direct ?

oui

Un système de détection automatique (VCA: video content analytics) est déployé sur l'installation (caméra ou système central) et permet l'analyse des images à la volée indépendamment de l'enregistrement (détection de franchissement, détection d'objet, …).

FICHES TECHNIQUES
Analyse automatisée d'images
Analyse d'images en direct

non

Enregistrement des images ?

oui

Les séquences sont enregistrées sur un système de stockage.

PROCÉDURE STOCKAGE

non

Analyse d'images en différé ?

oui

Un système de détection automatisé (VCA: video content analytics) est déployé sur le système central et permet d'effectuer une recherche spécifique (passage d'un véhicule rouge par exemple) sur un enregistrement sélectionné.

FICHES TECHNIQUES
Analyse automatisée d'image
Analyse d'images en différé

non

Fin de la procédure **Exploitation**

FICHE TECHNIQUE CENTRE D'EXPLOITATION

La visualisation d'images en direct (live) doit se faire sur un terminal de visualisation (écran d'ordinateur, téléviseur, tablettes, smartphone, …). Relevons que les solutions mobiles, telles que les tablettes ou les smartphones posent la problématique du transfert des données hors du territoire dans lequel elles ont été capturées, et partant, de la sécurité des données personnelles, sachant que la confidentialité, l'intégrité et la disponibilité doivent être assurées (cf. fiche légale : externalisation des données et informatique en nuages).

Afin d'optimiser la visualisation, celle-ci peut être effectuée dans un centre d'exploitation ou de surveillance (également dénommé CSU: centre de supervision urbain, RCC: remote control center, CAE: centrale d'alarme et d'engagement). Ce centre peut également assumer d'autres fonctions comme, par exemple, la gestion des alarmes et l'engagement de moyens (humains, techniques, fonctionnels, …).

Les besoins concrets du centre d'exploitation sont définis au préalable dans un cahier des charges, établi sur la base des méthodes d'évaluations des risques. Une matrice attribue un niveau de probabilité et de gravité à chaque danger répertorié (qui intègre différentes composantes comme l'architectonique, la vulnérabilité des valeurs à protéger, …), qui découle sur un traitement approprié (réduction, évitement, transfert, acceptation, …).

Ce centre d'exploitation peut être:

> **sur site:** mise en place physiquement d'une loge pour la gestion technique et organisationnelle du personnel d'exploitation, afin de pouvoir gérer les actions à entreprendre ainsi que la coordination des ressources pour les interventions. Le personnel peut être celui de l'entreprise, insourcé ou outsourcé;
> **décentralisé:** les actions et le contrôle est effectué par un transfert de responsabilité (encadré par un contrat, des SLA, …) sur une exploitation externe, afin de pouvoir gérer les actions à entreprendre ainsi que la coordination des ressources pour les interventions. On entend par exploitation externe, une exploitation localisée sur un site de l'entreprise ou outsourcé auprès d'un prestataire de service compétent dans le domaine.

Le centre d'exploitation peut, en fonction de son cahier des charges, visualiser les images en direct, procéder à des requêtes provenant d'un système d'analyse d'image, visualiser des images préenregistrées, etc. Le contrat doit mentionner les principes à respecter en matière de données personnelles et la responsabilité du sous-traitant pour la part qui lui a été déléguée.

FICHE TECHNIQUE ANALYSE AUTOMATISÉE D'IMAGES

L'analyse automatisée d'images (video content analytics ou video analysis software (VCA), intelligent video analysis, …) permet d'optimiser deux axes:

> **opérationnel:** en supportant le travail des opérateurs de vidéoprotection par des alertes configurées et automatisées en fonction du besoin (voir fiche technique "analyse d'images en direct");
> **enquête:** en assistant le travail d'enquête dans la recherche d'éléments concrets dans des séquences vidéo (voir fiche technique "analyse d'images en différé").

Le software qui analyse les images peut être conçu soit par le fabricant de la caméra, soit par des sociétés tierces et peut être installé sur:

> les **caméras** (interagit directement avec les séquences en direct, utilise les ressources processus de la caméra, décharge le système central et minimise l'utilisation de la bande passante);
> le **système central** (utilise les ressources du système central et nécessite un flux d'images continu entre la camera et le système qui analyse les images);
> une **infrastructure dédiée** (épargne les processeurs du système central mais implique des coûts d'investissements et de maintenance).

FICHE TECHNIQUE ANALYSE D'IMAGES EN DIRECT (LIVE)

Ces outils peuvent, par exemple, prendre en compte la détection automatique de mouvements lors de franchissement de ligne, de pénétration de zones définies, la mise en évidence de phénomènes suspects comme l'abandon ou le retrait d'objet, le groupement de personnes, les mouvements de foule, …

Ces dispositifs permettent un gain opérationnel en:

> **orientant le travail des opérateurs** par la détection de certains événements ou conditions et le déclenchement d'alertes de manière automatique;
> **diminuant le risque d'inattention** qui chute drastiquement au bout de quelques minutes, notamment en fonction du nombre de flux de caméras surveillés, d'écrans et de systèmes tiers à piloter (gestion d'alarmes, réception de personnes, flux de véhicules, …).

FICHE TECHNIQUE ANALYSE D'IMAGES EN DIFFÉRÉ (SUR ENREGISTREMENT)

Ces outils peuvent, par exemple, faciliter la recherche rapide d'un événement en lien avec une enquête dans des séquences de vidéosurveillance enregistrées à partir de critères simples uniques ou combinés (recherche d'un objet, sur une plage horaire, sur une ou plusieurs caméras).

Ces dispositifs permettent un gain dans l'enquête en:

> **permettant de traiter plusieurs recherches** en même temps (économie de moyen humain);
> **optimiser le type de recherche** au travers de critère précis;
> **éviter le risque d'erreur humaine** (inattention).

PROCEDURE EXTRACTION

Début de la procédure **Extraction**

Est-ce qu'une demande de préservation a été faite?

non → La demande de préservation de séquence pourrait provenir de tout un chacun et doit faire l'objet d'une appréciation.

FICHE TECHNIQUE
Demande de préservation

oui

Est-ce qu'une demande d'extraction officielle formelle a été faite?

non → La demande d'extraction doit provenir d'une instance reconnue par l'institution ou l'entreprise, cas échéant, et doit faire l'objet d'un formulaire dûment rempli.

FICHE TECHNIQUE
Demande d'extraction

oui

Est-ce que l'extraction est réalisable?

non → Les collaborateurs autorisés doivent disposer, avoir les accès et maîtriser le système et les procédures pour effectuer des extractions dans les règles de l'art.

FICHES TECHNIQUES
- Traçabilite
- Extraction

oui

Est-ce que la remise de l'extraction est faite sur la base d'un document?

non → La remise d'extraction doit être faite sur la base d'un formulaire dûment rempli.

FICHE TECHNIQUE
Communication des extractions

oui

non

non

non

Fin de la procédure **Extraction**

FICHE TECHNIQUE DEMANDE DE PRESERVATION

Les séquences de vidéosurveillance, les images ou autres métadonnées peuvent faire l'objet de demandes de préservation (mise en sûreté des preuves au sens large) en vue d'une extraction ultérieure pour éviter la suppression automatisée du système par exemple.

L'opérateur ou le responsable, de service ou de piquet, doivent apprécier la qualité de la demande formulée en fonction de la situation et doivent se déterminer sur la pertinence de la préservation. S'ils l'estiment nécessaire, ils en référeront à leur supérieur compétent pour toute détermination.

Un journal des événements contiendra les éléments pertinents relatifs au demandeur, à l'événement à proprement parlé ainsi que tout élément pertinent (cf. fiche technique "TRAÇABILITE").

FICHE TECHNIQUE DEMANDE D'EXTRACTION

Les demandes d'extractions de séquences, d'images et de métadonnées relatives à la vidéosurveillance doivent correspondre à une finalité légitime et répondre à une procédure claire, supporté par un formulaire et provenir d'une entité autorisée:

> un responsable de l'entreprise;
> une autorité pénale.

Responsable de l'entreprise
Seul un responsable de l'entreprise, ou une personne qui en a reçu la délégation, peut demander et obtenir l'extraction (cf. fiche technique "communication des extractions").

Autorité pénale
L'autorité pénale est constituée des autorités de poursuite pénale (la police, le ministère public, les autorités pénales compétentes en matière de contraventions) et des tribunaux (tribunal de mesures de contrainte, le tribunal de première instance, l'autorité de recours, la juridiction d'appel) qui sont légitimes à demander des extractions lorsque les circonstances le commandent.

En cas de besoin d'informations complémentaires sur une procédure pénale, qu'elle soit genevoise, d'un autre canton ou de la Confédération, il y a lieu de contacter le Ministère public émetteur de l'acte.

FICHE TECHNIQUE EXTRACTION

Les collaborateurs en charge du système de vidéosurveillance (opérateur, gestionnaire, superviseur, …) doivent être formés et expérimentés afin de répondre aux demandes d'extractions en toute conformité selon les principes ci-dessous:

Horodatage

Durant toute la procédure d'extraction, les informations relatives à l'horodatage (date, heure, fuseau horaire) de tous les composants du système (serveur, stockage, système de visualisation et d'extraction, caméras, OSD,...) doivent être relevées, consignés et comparées avec un système synchronisé (horloge atomique) afin d'assurer la conformité temporelle des données et notées dans un rapport d'extraction.

Des sites internet permettent de faire des conversions rapides et sans erreurs entre des temps relevés et des temps réels (changement d'horaire été – hiver inclus). Des systèmes d'extractions forensiques existent sur le marché. On peut citer l'outil de capture de séquences vidéo digitales "Omnivore" de la société Ocean Systems (www.oceansystems.com).

L'extraction peut contenir les fichiers suivants:

Image ou vidéo au format propriétaire

Cela permet de garantir l'intégrité des preuves (fichiers non modifiés). Les fichiers peuvent être lourds en terme informatique et doivent très souvent être accompagnés de leur viewer. A relever qu'il est préférable de fournir un viewer qui requiert son exécution en mémoire vive plutôt qu'une installation sur le système qui nécessiterait des privilèges administrateurs que peu de collaborateurs possèdent au sein d'une entreprise.

Image au format ouvert non compressé ou compressé sans perte (lossless compression)

Le format BMP (Bitmap), par exemple, est ouvert et peut être lu sur de très nombreux ordinateurs. Souvent non compressé, il ne devrait pas altérer la preuve mais constitue des fichiers lourds, difficilement manipulables. Certains formats permettent des compressions sans pertes (se renseigner auprès du fournisseur).

Image ou vidéo au format ouvert compressé avec perte (lossy compression)

Les images (JPG par exemple) ou vidéos (AVI, famille des MPG / MPEG, H264,…) par exemple, sont souvent compressées. De ce fait, la preuve est altérée par la suppression d'information (perte de données), mais constitue des fichiers plus légers qui peuvent être rapidement et facilement manipulés en cas d'urgence.

Support

L'extraction de séquence vidéo peut se faire sur n'importe quel support pour autant que les conditions suivantes soient respectées:

> étiquetage des preuves (traçabilité);
> emballage des preuves (protection contre la destruction physique, magnétique, …);
> stockage des preuves (soit sur support dédié et protégé, soit sur un serveur dont les accès sont fortement limités et journalisé (logs) pour être conforme à la politique en vigueur au sein de l'institution et au contexte légal de ce présent document);
> récusation (si le collaborateur est impliqué de près ou de loin, il doit se défaire de l'affaire).

Mesures compensatoires

Si l'extraction de séquence n'est pas possible pour des raisons de compétences, de connaissances spécifiques ou à cause de problèmes techniques, il y a lieu de prendre toutes les mesures compensatoires à disposition pour préserver les preuves. Ces mesures peuvent être des copies d'écran, des photos de l'écran, ou tout autre moyen qui permettrait de faire le lien avec l'événement, afin de préserver les preuves.

En cas de copies d'écran (avec un appareil photo, un smartphone, …), il y aurait lieu de ne pas se limiter au sujet à capturer (image à proprement parlé), mais d'agrandir la zone de capture à l'environnement de l'image (logiciel de lecture) et également à l'environnement informatique en capturant, par exemple, la date et l'heure de l'ordinateur.

FICHE TECHNIQUE COMMUNICATION DES EXTRACTIONS

La communication de données d'entreprise (images, séquences vidéos, plans et schémas du système de vidéosurveillance / sécurité, mains courantes de loges sécuritaires, …) doit être réalisée à un destinataire autorisé / habilité et doit également être effectuée sur la base d'un formulaire afin d'en assurer leur imputabilité et leur traçabilité. Le formulaire utilisé lors de la demande d'extraction peut être complété avec, par exemple, les données suivantes:

> la date de remise;
> les noms et signatures des personnes impliquées (extracteur et réceptionnaire);
> le nombre de séquences extraites (avec leurs plages horaires);
> le numéro des caméras impliquées;
> le type de support transmis.

Au même titre que les extractions, la tenue d'un registre des communications des données (qui peut être constitué des copies des demandes d'extraction et de communication, cas échéant) permet de satisfaire aux exigences légales et réglementaires et sera réclamé en cas d'audit de conformité, interne ou externe.

Si la remise des données se fait de manière spontanée ou volontaire suite à la demande de l'autorité pénale, cette dernière qui reçoit le matériel doit faire signer un "avis de dépôt de moyen de preuve" à la personne qui le lui remet. Une copie de ce document peut lui être remise.

Si les données sont saisies lors d'une perquisition, l'autorité pénale se présentera accompagnée d'un mandat de perquisition écrit, ou oral en cas d'urgence, qui mentionnera les locaux à fouiller, le but de la mesure et les autorités ou personnes chargées de l'exécution.

L'intéressé en charge de procéder à l'extraction peut préalablement s'exprimer sur le contenu des extractions.

Pour ne pas s'exposer à une poursuite pénale (entrave à l'action pénale et …), il y a lieu de ne pas divulguer ce qui est relatif à la demande d'extraction (images, séquences, données, personnes et objets concernés, …).

FICHE TECHNIQUE TRAÇABILITE

Afin d'assurer la traçabilité du traitement du matériel relatif à la vidéosurveillance, les collaborateurs en charge du système de vidéosurveillance (opérateur, gestionnaire, superviseur, …) doivent être formés et expérimentés. Ils doivent pouvoir s'appuyer sur un champ documentaire (directive, procédure, guide, formulaire, …) formalisé et validé par la hiérarchie qui cadre les activités relatives à la vidéosurveillance.

La traçabilité s'exprime notamment de manière non exhaustive au travers:

> d'une charte pour les visiteurs (langues différentes);
> d'un formulaire intégrant les données relatives à:
  - la demande de préservation de séquence;
  - la demande d'extraction de séquence;
  - la communication des extractions;
> de l'étiquetage des preuves (traçabilité);
> de l'emballage des preuves (protection contre la destruction physique, magnétique, …);
> du stockage des preuves (soit sur support dédié et protégé, soit sur un serveur dont les accès sont fortement limités et journalisé (logs) pour être conforme à la politique en vigueur au sein de l'institution et au contexte légal de ce présent document);
> de récusation (si le collaborateur est impliqué, il ne peut procéder aux actes).

Formulaire de demande d'extraction

Ces demandes doivent être effectuées sur la base d'un formulaire afin d'assurer l'imputabilité et la traçabilité des extractions. Le formulaire en question devrait, par exemple, préciser les points non exhaustifs suivants:

> date de la demande;
> identité du demandeur avec signature;
> description de l'événement recherché;
> motif de la demande;
> lieu concerné (site, secteur, zone, caméra, …);
> plage horaire à extraire (date et heure) pour chaque séquence.

Formulaire de communication d'extraction

Le formulaire de la demande d'extraction peut être complété avec, par exemple, les données non exhaustives suivantes:

> la date de remise;
> les noms et signatures des personnes impliquées;
> le nombre de séquences extraites (avec leurs plages horaires);
> le numéro des caméras impliquées;
> le type de support transmis.

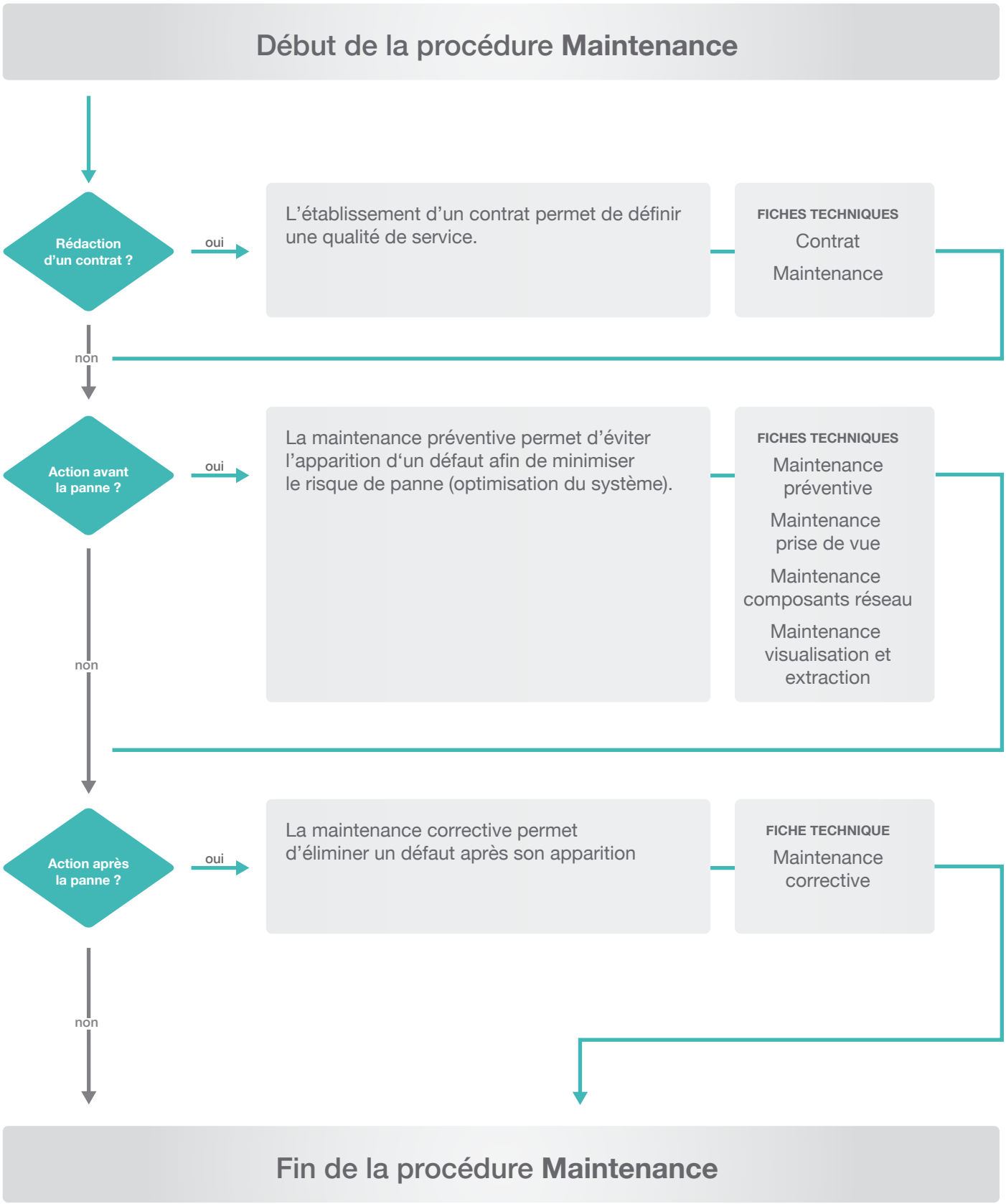
Tenue d'un registre

La tenue d'un registre des extractions (qui peut être constitué des copies des demandes d'extraction, cas échéant) permet de satisfaire aux exigences légales et réglementaires et sera réclamé en cas d'audit de conformité, interne ou externe.

Validation juridique

On relèvera que la validation du champ documentaire interne (directives, procédures, formulaires, …) ainsi que l'identification des autorités autorisées à faire des demandes d'extraction, de préservation et de réception des données par le service juridique interne peut être bénéfique, voire indispensable afin d'éliminer toute demande non conforme (motifs flous et contrevenants au contexte légal du présent document). Si le service juridique n'existe pas, la supervision par un organe compétent est recommandée.

PROCEDURE MAINTENANCE



FICHE TECHNIQUE CONTRAT

La rédaction d'un contrat est primordiale pour définir les différents types de maintenances en permettant de fournir l'assurance raisonnable du bon fonctionnement de l'installation à long terme (garantie des investissements). Au travers du contrat, il est possible de négocier et définir la qualité de service (SLA) requise entre un prestataire et un client en vue de cadrer au mieux les besoins de l'installation (disponibilité, performance, rapidité d'intervention, planification, matériel de réserve, ...).

Lorsque l'on sous-traite tout ou partie du traitement des données personnelles, le sous-traitant devient co-responsable du traitement, sans que le mandant ne soit libéré de ses propres responsabilités. Le contrat doit mentionner les principes à respecter en matière de données personnelles et la responsabilité du sous-traitant pour la part qui lui a été déléguée. Le mandant doit se réserver un droit d'audit.

Différents type de contrats sont proposés ci-dessous en fonction du degré de disponibilité nécessaire à chaque client:

> **Contrat de type support simple:** mise à disposition de personnel formé et expérimenté uniquement (en fonction de délais prédéfini);
> **Contrat de type support complet:** mise à disposition de personnel formé et expérimenté (en fonction de délais prédéfini) avec mise à disposition de matériel de réserve et prise en charge de la réparation;
> **Contrat de type support à la carte:** mixité des besoins en fonction des types de maintenance demandés (voir ci-dessous : caméras; éclairage et projecteur infrarouge; encodeur et décodeur IP; composants réseau; serveur, équipements de visualisation; …).

FICHE TECHNIQUE MAINTENANCE

La maintenance d'installations en général et plus particulièrement les installations liées à la vidéosurveillance appellent au respect de normes légales, des prescriptions techniques et des bonnes pratiques. Elle se développe, de manière non exhaustive, au travers:

> **de la documentation technique** (indispensable pour maintenir l'installation opérationnelle);
> **du cahier de contrôle** (suivi de l'installation, de son comportement et des éventuels problèmes);
> **des équipements de réserve et de tests** (pour assurer la continuité de fonctionnement de l'installation dans des conditions opérationnelles);
> **des mises à jour logicielles** (équipements, résolution de problèmes, amélioration du fonctionnement de base du système, …);
> **des guides utilisateur** (instruction du personnel pour garantir le fonctionnement correct et efficace du système).

La maintenance doit pouvoir couvrir les parties d'un système de vidéosurveillance relatives à:

> **la prise de vue** (caméra, projecteur infrarouge, éclairage d'appoint, etc.);
> **les composants réseau** (encodeurs et décodeurs IP, switch, serveurs, stockage, etc.);
> **les équipements de visualisation et d'extraction d'images** (ordinateur du bureau ou dédié, mur d'images, imprimante, etc.).

La maintenance doit être un savant mélange entre les notions légales, techniques, organisationnelle, de gouvernance, de continuité de l'activité, …

FICHE TECHNIQUE MAINTENANCE PRÉVENTIVE

La maintenance préventive permet d'effectuer des actions (mise à jour, contrôle de fonctionnement, nettoyage) de tout ou partie d'un système de vidéosurveillance avant la survenance d'un dysfonctionnement partiel ou total.

Son but est de minimiser le temps d'inactivité du système pour optimiser les investissements consentis dans le système et de garantir la conformité de son utilisation en assurant l'alignement avec le cadre légal défini.

La maintenance préventive peut être effectuée selon un calendrier, sur la base d'indicateurs (temps d'utilisation, se déploie sur tous les composants du système de vidéosurveillance (cf. fiche technique maintenance) sur la base de:

> la **mise à jour** des composants (hardware, firmware ou software);
> le **contrôle** des paramètres requis pour éviter les déviances;
> le **nettoyage** en général.

MAINTENANCE

FICHE TECHNIQUE MAINTENANCE CORRECTIVE

La maintenance corrective permet d'effectuer des actions de tout ou partie d'un système de vidéosurveillance après la survenance dysfonctionnement partiel ou total.
Son but est de maximiser le temps de reprise des activités pour optimiser les investissements consentis dans le système et de garantir la conformité de son utilisation en assurant l'alignement avec le cadre légal défini.

Cette maintenance peut être de type:

> **corrective-palliative**: permet d'assurer un dépannage provisoire le plus rapidement possible afin d'assurer la reprise d'activité dans un temps minimal (s'appuyer sur les principes de la continuité de l'activité) sans recherche du défaut;
> **corrective-curative**: permet d'assurer une remise à l'état initial afin de minimiser la probabilité de retour de la panne.

FICHE TECHNIQUE MAINTENANCE DES COMPOSANTS RELATIFS À LA PRISE DE VUE

La caméra, ainsi que les dispositifs complémentaires à la prise d'images (projecteur infrarouge et éclairage d'appoint), qu'ils soient installés à l'intérieur ou à l'extérieur d'un bâtiment, sont soumis à l'usure interne des composants ainsi qu'aux éléments extérieurs. Ainsi, les mesures doivent être prises pour préserver les capacités de cet outil au travers:

> **de la mise à jour du firmware** (logiciel interne de la caméra): permet la résolution de problèmes et l'amélioration du fonctionnement de base du système;
> **du contrôle des paramètres de configuration** (masquage, cadrage, position de base, rondes, interface de commande, etc.): permet d'éviter d'éventuels dysfonctionnements non ou peu perceptible par l'opérateur;
> **du contrôle de fonctionnement des dispositifs complémentaires**: permet d'assurer le fonctionnement des ampoules, les paramètres des seuils de commutation des cellules crépusculaires, la qualité des alimentations, etc.;
> **du nettoyage de la caméra, de l'objectif et du boîtier**: permet d'assurer une qualité optimale de l'image car des poussières, des salissures ou la présence d'animaux (nid d'oiseau, toile d'araignées, ...) peuvent se déposer;

MAINTENANCE

FICHE TECHNIQUE MAINTENANCE DES COMPOSANTS RÉSEAU

Les "composants réseau" comprennent les encodeurs et décodeurs IP, switch, serveurs, stockage, etc. Ces composants doivent également faire l'objet de contrôles des paramètres afin d'éviter le blocage du système, la perte de données, etc., au travers:

> **de la mise à jour du firmware et software:** permet la résolution de problèmes et l'amélioration du fonctionnement de base du système;
> **du contrôle des fonctionnalités générales:** enregistrement (durée de garde des images en regard des spécificités légales et techniques); implémentation de l'analyse d'images (voir procédure exploitation); contrôle de la charge du serveur, des paramètres de sécurité (accès, privilèges, logs, etc.); des processus de démarrage des services et applications; des disques durs et systèmes RAID (scan-disk, défragmentation, analyse de surface, messages d'erreurs, etc.); des alimentations (alimentation redondante, de secours - UPS), etc.
> **du contrôle des encodeurs et décodeurs IP:** permet de contrôler la qualité des données vidéo (compression, résolution, qualité, etc.), la qualité du signal vidéo reçu, la mise à jour du firmware et software relatif aux équipements;
> **du nettoyage en général:** permet d'éviter un encrassement des gaines de ventilation du matériel ou des locaux empêchant un bon refroidissement du matériel, des problèmes de connectique et décharges électriques dues à l'électricité statique.

FICHE TECHNIQUE MAINTENANCE DES ÉQUIPEMENTS DE VISUALISATION ET D'EXTRACTION

Les équipements de visualisation et d'extraction d'images font partie intégrante du système, même si aucun centre d'exploitation n'est déployé. Ils peuvent être représentés par un simple ordinateur du bureau, un ou plusieurs ordinateurs dédiés voire un mur d'écrans ou de téléviseurs pilotés par un ordinateur. Afin de garantir leurs bons fonctionnements, il a lieu d'effectuer:

> **la mise à jour des composants hardware, firmware et software:** contrôle des connexions internes et externes pour garantir la qualité et la fluidité de l'image, de l'audio et des commandes en général (permutation et pilotage des caméras) ainsi que la compatibilité avec les caméras et les autres équipements réseau;
> **la maintenance des écrans:** contrôle du vieillissement, des connexions, etc.;
> **le nettoyage des équipements en général** (écran, ordinateur, clavier, souri, pad, joystick, imprimante, etc.) pour éviter l'accumulation de poussière et de salissure afin de garantir l'hygiène.

ANNEXE

GLOSSAIRE

Archivage électronique
Ensemble des actions, outils et méthodes destinés à conserver des contenus électroniques sur un support sécurisé dans un format figé (sur une bande magnétique par exemple). Il ne faut pas confondre avec la sauvegarde (cf. sauvegarde et enregistrement).

AVI (Audio Video Interleave)
Format vidéo prenant simultanément en charge les lectures vidéo et audio.

Catalogue des fichiers
Les fichiers détenus par les institutions ou par les privés, contenant des données personnelles, doivent faire l'objet d'une déclaration : au registre des fichiers du préposé fédéral s'agissant du privé, dans le catalogue des fichiers du préposé genevois, s'agissant des institutions publiques. Pour celles-ci, les lois cantonales déterminent en effet si le préposé tient un registre des fichiers.

CCTV
Closed circuit TV (Télévision en circuit fermé).

CIF (Common Intermediate Format)
Désigne les résolutions d'images analogiques 352x288 pixels (PAL).

Chiffrement
Appelé également cryptage, il s'agit d'un procédé permettant de cacher le sens d'un document à toute personne qui n'a pas la clé de déchiffrement.

Cloud computing (cloud) - informatique en nuage
Désigne l'accès via un réseau de télécommunications, à la demande et en libre-service, à des ressources informatiques partagées configurables (NIST).

CO
Code des obligations

Codec – COde and DECode
Désigne un algorithme permettant de compresser / décompresser les signaux vidéo.

Compression d'images
Technique permettant de réduire la taille (en octets) des fichiers images.

CP
Code pénal suisse.

CPP
Code de procédure pénale suisse.

ANNEXE

GLOSSAIRE

Cryptage
Appelé également chiffrement, il s'agit d'un procédé permettant de cacher le sens d'un document à toute personne qui n'a pas la clé de déchiffrement.

CAE
Centrale d'Alarme et d'Engagement

CSU
Centre de Supervision Urbain

Destruction (des données enregistrées)
Toute action technique permettant concrètement de rendre les données enregistrées - ainsi que leurs sauvegardes et archivage- totalement et définitivement inutilisables (effacement ou démagnétisation, écrasement, …).

Données personnelles
Toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable.

Données personnelles sensibles
Les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles, sur la santé, la sphère intime de l'appartenance ethnique, sur les mesures d'aide sociale, sur les poursuites ou sanctions pénales ou administratives.

DVR
Digital video recorder - enregistreur digital vidéo : comme son nom l'indique, l'enregistreur permet d'enregistrer des vidéo sur un support digital (disque dur par exemple) sans être connecté au réseau de l'entreprise (les flux des caméras arrivent en directe sur le DVR).

eDiscovery - electronic discovery
Investigations numériques au travers d'Internet par exemple.

Edge
Système de stockage permettant d'enregistrer des images de caméras de vidéosurveillance sur une carte embarquée (stockage local ou enregistrement embarqué).

Employeur institutionnel
Une institution publique (par exemple : administration communale ou cantonale)
Une personne morale ou un autre organisme de droit privé sur lesquels une institution publique exerce une maîtrise effective, notamment par un subventionnement ou une délégation de compétence.
Une personne physique ou morale ou un organisme chargé de remplir des tâches de droit public cantonal ou communal (contrat de prestation).

ANNEXE

GLOSSAIRE

Employeur privé
Au sens de la loi sur le travail : une entreprise dont l'organisation relève du droit privé (par exemple : société, association, prestataire de service, profession libérale) pour autant qu'il y ait rapport de travail.
L'employeur privé est soumis à la loi fédérale sur la protection des données et à la compétence du préposé fédéral.

Enregistrement
Ensemble des actions, outils et méthodes destinés à enregistrer des contenus électroniques en cours d'utilisation ou en vue d'une utilisation future.

Fichier
Tout système destiné à réunir, sur quelque support que ce soit, des données personnelles d'un segment de population déterminée, et structuré de manière à permettre de relier les informations recensées aux personnes qu'elles concernent. Voir catalogue des fichiers.

Fréquence d'images
Désigne le taux de rafraîchissement d'un flux vidéo et s'exprime en nombre d'images par seconde (IPS) ou frame per second (FPS). Une fréquence d'images supérieure est intéressante lorsque le flux vidéo présente du mouvement parce qu'elle assure une qualité d'image cohérente de bout en bout.

Forensique
Les sciences forensiques regoupent l'ensemble des différentes méthodes d'analyse destinées à résoudre des enquêtes judiciaires. Elles englobent les méthodes de police scientifique (analyses d'empreintes – ADN - informatiques et de médecine légale. www.wikipedia.org

FTTx
Le FTTx (fiber to the...) consiste à amener la fibre optique au plus près de l'utilisateur, afin d'augmenter la qualité de service (en particulier le débit) dont celui-ci pourra bénéficier. Le x peut être N (Neighbourhood : quartier), C (Curb : trottoir), S (Street : rue), B (Building : bâtiment), … www.wikipedia.org

H.264
Également connue sous l'appellation MPEG-4 AVC (Advanced Video Coding,), ou MPEG-4 Part 10, est une norme de codage vidéoISO/IEC 14496-10 et ITU-T H.264. Il s'agit d'une norme de compression pour la vidéo numérique publiée en 2003 dont la version la plus récente date de 2012.

H.265
Également connue sous l'appellation MPEG-4 HEVC (High Efficiency Video Coding) est une norme du codage vidéo ISO/IEC 23008-2 et ITU-T H.264. Il s'agit d'une norme de compression de nouvelle génération pour la vidéo numérique publiée en 2013.

ANNEXE

GLOSSAIRE

LIPAD
Loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (rsGE A 2 08).

Lossless compression
La compression est dite sans perte lorsqu'il n'y a aucune perte de données sur l'information d'origine. Il y a autant d'information après la compression qu'avant, elle est seulement réécrite d'une manière plus concise. www.wikipedia.org

Lossy compression
La compression avec pertes ne s'applique qu'aux données «perceptibles», en général sonores ou visuelles, qui peuvent subir une modification, parfois importante, sans que cela soit perceptible par un humain. La perte d'information est irréversible, il est impossible de retrouver les données d'origine après une telle compression. www.wikipedia.org

LPD
Loi fédérale sur la protection des données du 19 juin 1992 (RS 235 1).

LTr
Loi sur le travail.

Maître du fichier
La personne qui décide ou détermine les finalités et le contenu du fichier, et qui en est responsable. Le fichier des données de vidéosurveillance enregistrées doit être déclaré à l'organe compétent (préposé fédéral ou cantonal à la protection des données).

Motion JPEG
Technique de compression et de décompression simple des images vidéo sur IP, Motion JPEG permet une latence faible et une qualité d'image assurée, quel que soit le mouvement ou la complexité de l'image. La qualité de l'image peut être contrôlée par réglage du niveau de compression, lequel détermine simultanément la taille du fichier et, par conséquent, la fréquence d'images. Des images individuelles de haute qualité peuvent aisément être extraites des flux Motion JPEG.

MPEG (Moving Picture Experts Group)
Groupe de travail chargé de développer des normes de compression dans les domaines de la vidéo numérique et de l'audio. Le groupe opère sous les auspices de l'ISO, l'Organisation internationale de normalisation. Les normes formulées par le MPEG représentent une série évolutive, chaque norme étant destinée à une fin particulière.

MPEG-2 (Moving Picture Experts Group)
MPEG-2 désigne un ensemble de normes d'encodage audio et vidéo, surtout utilisées pour l'encodage audio et vidéo des signaux de télédiffusion, notamment en ce qui concerne la télévision numérique par satellite et le câble. Le format MPEG-2, avec quelques adaptations, est également le format habituel utilisé pour les films proposés au public en DVD.

ANNEXE

GLOSSAIRE

MPEG-4
MPEG-4 regroupe un ensemble de normes audio et vidéo, ainsi que la technologie utilisée. La norme MPEG-4 est essentiellement affectée à la distribution de contenu via Internet (diffusion multimédia en continu) et sur CD, la vidéophonie et la télédiffusion.
La mise en œuvre des fonctionnalités prises en charge par le format MPEG-4 étant pour l'essentiel laissée à la libre appréciation de chaque développeur, les normes MPEG-4 n'ont probablement jamais été mises en œuvre en totalité. Afin de tenir compte de cette particularité, la norme utilise les concepts de «profils» et de «niveaux» permettant de définir un ensemble de fonctionnalités adaptées à un groupe déterminé d'applications.

NAS
Network Attached Storage - serveur de stockage en réseau: serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé.

Natif (propriétaire)
Correspond au format de base, appelé également propriétaire. En manipulant des formats de ce type, on évite d'altérer la qualité de l'image en la ré-encodant dans un format ouvert (.avi ou .jpg par exemple). Au niveau de l'analyse forensique, on évite ainsi l'altération de la preuve et on se prémunit contre des problèmes liés à son éventuelle irrecevabilité.

NVR
Network video recorder - enregistreur vidéo sur réseau : comme son nom l'indique, l'enregistreur permet d'enregistrer des vidéo sur un support digital (disque dur par exemple) en capturant les flux des caméras en réseau.

Objectif enquête
Relatif à l'enquête après événement. La caméra envoie les données sur un espace de stockage pour être utilisé à postériori afin de comprendre le déroulement des faits, chercher des indices, collecter des preuves, …

Objectif opérationnel
Relatif aux opérations en cours d'événement. La caméra envoie les données en direct sur des écrans afin que des opérateurs puissent prendre des décisions cohérentes (aide à la décision).

OSD
On Screen Display (ou over screen display) consiste à l'affichage d'informations (horodatage, numéro de caméra, emplacement, …) sur l'image.

PAL – résolution
Résolution pouvant atteindre 720x576 lignes, soit ~ 0,4 mégapixel.

Personnel
Toute personne employée, qu'il s'agisse d'un travailleur dépendant (salarié) ou indépendant (consultant,…).

ANNEXE

GLOSSAIRE

Pixel
Unité de base permettant de mesurer la définition d'une image.

PoE
Power on Ethernet - courant sur ethernet: défini la capacité de la caméra à s'alimenter électriquement avec l'aide unique du réseau ethernet.

Préposé cantonal à la protection des données et à la transparence
Chargé de la surveillance de l'application de la loi genevoise sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) à laquelle sont soumises les institutions publiques et parapubliques cantonales et communales (cf. employeurs institutionnels).

Préposé fédéral à la protection des données et à la transparence
Chargé de la surveillance de l'application de la loi fédérale sur la protection des données (LPD) à laquelle sont soumises les personnes privées (cf. employeurs privés).

Propriétaire (format)
Voir Natif

PTZ
Pan Tilt Zoom - Rotation Inclinaison Zoom : Pan est la rotation de la caméra autour de l'axe Z, Tilt est l'inclinaison de la caméra sur l'axe X, et Zoom est le mouvement de la lentille motorisée le long de l'axe Y.

QoS
Quatliy of Service - Qualité de service est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets… La QoS est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure. Elle permet ainsi aux fournisseurs de services (départements réseaux des entreprises, opérateurs) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP.

Quad - résolution
Le quart de la résolution PAL, soit ~ 0,1 mégapixel.

RCC
Remote control Center

SAN
Storage Area Network - réseau de stockage : réseau spécialisé permettant de mutualiser des ressources de stockage.

ANNEXE

GLOSSAIRE

Sauvegarde
Ensemble des actions, outils et méthodes destinés à dupliquer des contenus électroniques pour éviter leur perte en cas de dysfonctionnement du dispositif sur lequel ils sont enregistrés. (cf. enregistrement et archivage)

SLA
Service Level Agreement - contrat de niveau de service est un document qui définit la qualité de service requise entre un prestataire et un client.

SSL
Acronyme de Secure Sockets Layer définissant un protocole de sécurisation des échanges sur Internet, actuellement renommé en TLS (Transport Layer Security) cf. TLS.

TIFF
Tagged Image File Format – non compressé.

TLS
Acronyme de Transport Layer Security (anciennement SSL) définissant un protocole de sécurisation des échanges sur Internet par échange de clés de cryptage assymétriques. Il fournit, par exemple, les objectifs de sécurité suivants : authentification du serveur, confidentialité et intégrité des données échangées.

Traitement (de données personnelles)
Toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.

Usager
Correspond aux citoyennes et citoyens lorsqu'on parle de lieux publics et aux clients lorsqu'on parle de lieux privés.

VCA
Vidéo Content Analytics : analyse de contenu vidéo

Vidéosurveillance
Collecte ouverte ou non au moyen de caméras d'images et d'informations sur des personnes, sous la forme d'enregistrements vidéo.

XaaS
Cette notion fait appel au cloud computing: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

ANNEXE

CONTACTS UTILES

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE:

Préposé fédéral à la protection des données et à la transparence Feldeggweg 1 3003 Berne www.edoeb.admin.ch	**Hanspeter Thür** Préposé fédéral **Jean-Philippe Walter** Préposé fédéral suppléant	031 322 43 95 hanspeter.thur@edoeb.admin.ch 031 322 41 31 jean-philippe.walter@edoeb.admin.ch

Préposés cantonaux:
La liste des préposés et leurs coordonnées figurent sur une liste tenue à jour par le Préposé fédéral, que vous trouverez ici: http://www.edoeb.admin.ch/dokumentation/00614/index.html?lang=fr

LIENS UTILES

www.fgsonline.ch
Forum genevois de la Sécurité

www.ge.ch/ppdt
Préposé cantonal à la PDT

www.edoeb.admin.ch
Préposé fédéral à la PDT

www.ge.ch/legislation
Législation genevoise

https://www.admin.ch/gov/fr/accueil/droit-federal/recueil-systematique.html
Recueil systématique de la Confédération

www.seco.admin.ch
Secrétariat d'Etat à l'économie: Centre de compétence de la Confédération pour toutes questions ayant trait à la politique économique.