Concept SIPD - vidéosurveillance
commune XY

*(Le texte en italique peut être supprimé une fois le concept achevé. La commune complète les parties signalées en jaune.)*

En-tête\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* Installation d’un système de vidéosurveillance de bâtiments ou d’espaces publics dans la commune XY
* Responsable du projet, y compris coordonnées
* Responsable SIPD, y compris coordonnées
* Version 1.0
* Paraphe du mandant du projet :

# 1. Données relatives au projet

*(Le texte peut aussi renvoyer à des documents existants*.*)*

La commune XY a décidé, par arrêté du XY, de placer certains espaces publics sous la surveillance de caméras vidéo aux fins autorisées par la loi.

En application des bases légales en vigueur[[1]](#footnote-1), le conseil communal a demandé l’approbation de la Police cantonale bernoise (POCA) concernant ces mesures de surveillance (voir  XY).

Dans sa demande du XY, la commune a sollicité la mise en place d’une surveillance dans les lieux et aux horaires suivants :

* rue, place, façade, etc. aux horaires XY
* rue, place, façade, etc. aux horaires XY
* etc.

Le projet XY exposé ci-après vise à installer et à mettre en exploitation un système TI approprié pour exécuter l’arrêté du conseil communal du XY dans les conditions prévues par l’autorisation cantonale du XY. Il ne crée pas de nouveaux processus administratifs. Le système doit pouvoir être exploité sans autre intervention des autorités communales, sauf dans le cas d’éventuels travaux de maintenance. Les informations enregistrées par le système, c’est-à-dire les enregistrements vidéo et sonores de lieux et de personnes, sont accessibles exclusivement aux services de police habilités par la loi.

L’exploitation de la solution envisagée pose d’importantes contraintes au plan SIPD en ce qui concerne la confidentialité des données traitées. Par contre, des aspects comme la disponibilité ou l’intégrité des données sont moins importants en termes de SIPD, si bien que le présent concept ne contient pratiquement que des exigences et des mesures visant la protection des personnes intéressées. Les autres exigences et mesures sont conformes à la norme cantonale en matière de protection de base (voir le point 4).

Le système dispose des interfaces d’entrée suivantes :

* Caméras : XY caméras de type XY seront installées aux emplacements autorisés. Ce type de caméras se caractérise par le fait que …
* Interfaces réseau : la technologie XY est utilisée pour transmettre les données des caméras vers le système destiné à les traiter. Ce système dispose au total de XY interfaces associées, dont XY sont activées.
* Réseau communal ? Le système est en outre connecté au réseau de données administratives de la commune, en particulier pour permettre les actualisations du système d’exploitation et des logiciels mis en œuvre ainsi que la maintenance à distance du système via le réseau en accès distant. Il n’est pas prévu d’accès distant aux données utiles pour les travaux de maintenance.

Le système dispose des interfaces de sortie suivantes :

* Ecran : destiné à l’administration du système et à l’utilisation autorisée du logiciel d’enregistrement d’images.
* Interfaces USB et autres interfaces inscriptibles de supports de données : l’utilisation autorisée du logiciel d’enregistrement d’images comprend impérativement l’exportation de certaines données vers des supports de données de la Police cantonale.
* Imprimante ?
* Réseau communal ? Voir ci-dessus. Il n’est pas prévu d’exporter des données par l’intermédiaire des interfaces réseau, et le logiciel d’enregistrement d’images n’est pas configuré à cette fin.
* Aucune procédure d’accès en ligne aux données du logiciel d’enregistrement d’images n’est prévue ou installée.

*Description de la (des) solution(s) TI disponible(s) à la sélection.
(éventuellement référence à la documentation du produit, à des offres, contrats, etc, Voir aussi la demande d’approbation à la POCA conformément à l’art. 49, al. 2, lit. f et h OPol.*

Le système à installer comprend les composants suivants :

* serveur,
* système d’exploitation,
* application spécifique,
* caméras,
* réseaux,
* partenaires/fournisseurs.

# 2. Protection des données

La vidéosurveillance qui est prévue doit être considérée comme le traitement de données personnelles au sens de la loi cantonale sur la protection des données (LCPD), en conséquence de quoi cette loi est applicable. La surveillance est mise en place conformément à la loi du 10 février 2019 sur la police (LPol, RSB 551.1) et à l’ordonnance du 20 novembre 2019 sur la police (OPol, RSB 551.111). Ces textes législatifs autorisent la surveillance dans les conditions que la Police cantonale bernoise a approuvées pour la commune par décision du XY. Aucune autre base légale n’est nécessaire pour exploiter la solution envisagée.

La durée de conservation autorisée pour les enregistrements d’images et de sons est conforme aux bases légales mentionnées. En conséquence, le système supprime automatiquement les données non utilisées 100 jours après leur enregistrement. La suppression des enregistrements est consignée dans un procès-verbal. Aucun autre archivage des données n’est réalisé dans la sphère de compétence de la commune.

Les personnes intéressées ont un droit de regard sur les enregistrements. Les demandes en ce sens doivent être adressées à la Police cantonale, qui permet la consultation des données dans les limites autorisées et veille à l’exécution des autres revendications légitimes.

Le concept des droits d’utilisateur du système prévoit les rôles suivants :

* admin externe : qui ?
* admin interne : qui ?
* utilisateur principal (rôle POCA ; attribué de façon ad hoc au sein de la POCA à la personne compétente)

Ces différents rôles d’utilisateurs bénéficient uniquement des droits d’accès qui sont impérativement nécessaires pour accomplir les tâches qui leur incombent :

* admin externe : accès administratif aux commandes système et analogues, mais pas aux données utiles du système ;
* admin interne : accès administratif aux commandes système et analogues ; accès aux données utiles du système à des fins de maintenance conformément à l’article 14 de l’ordonnance sur la vidéosurveillance ;
* utilisateur principal (rôle POCA ; attribué de façon ad hoc au sein de la POCA à la personne compétente) avec droits d’utilisation des données traitées, mais sans accès aux commandes système et analogues.

Le recueil de données est déclaré à l’autorité de surveillance de la protection des données dès que celle-ci met à disposition des formulaires à cette fin.

# 3. Sûreté de l’information

La classification de la solution envisagée, réalisée au moyen de la grille prévue à cet effet (annexe 1 de l’Instruction d’exécution de l’OIO du 1er octobre 2008 relative à l’Instruction du Conseil-exécutif concernant la sûreté de l’information et la protection des données, IE-SIPD, a montré que compte tenu de l’importance de la protection des données dans tous les objectifs de contrôle, il convenait de réaliser une analyse approfondie des risques conformément à l’ACE SIPD.

En réalité, seuls sont pertinents les domaines qui garantissent directement ou indirectement la confidentialité des données traitées ; en ce qui concerne la vidéosurveillance, il ne s’agit pas d’une tâche essentielle qui incombe à une administration publique, mais d’une possibilité supplémentaire dont celle-ci dispose pour exécuter sa mission de sécurité générale. Il n’existe donc pas, pour cette raison ou pour des considérations SIPD, des exigences importantes en termes de disponibilité du système de surveillance, ni d’ailleurs des impératifs qualitatifs concernant l’intégrité des données ou des aspects analogues.

# 4. Analyse des risques

L’analyse des risques a permis de tirer les conclusions suivantes :

* Concernant les objectifs de contrôle des accès, de la disponibilité et de la séparation, aucune autre mesure ne s’impose en plus de celles qui sont spécifiées dans la liste de contrôle « protection de base » (annexe 3 de l‘IE-SIPD).
* Le risque lié à l’objectif de contrôle des entrées n’est pas pertinent en l’absence d’entrée de données utiles.
* L’objectif de contrôle des transmissions doit être modifié conformément aux mesures décrites ci-après.

# 5. Mesures

Les mesures doivent fondamentalement être comprises, dans la mesure du possible, comme des critères de sélection qualitative pour le système à acquérir.

Un concept des droits d’utilisateur est élaboré dans tous les cas avec les rôles susmentionnés. Il est signé par l’autorité responsable du système. Ce concept contient limitativement les rôles prévus assortis des droits d’accès correspondants ; il décrit aussi comment et par qui ces rôles sont octroyés aux différents collaborateurs internes et externes.

Les autres mesures prévues dans la liste de contrôle « protection de base » susmentionnée sont intégralement mises en œuvre ; les divergences éventuelles sont motivées au cas par cas. Cela inclut la mesure M-5.1.1 (Réglementation des droits d'utilisateur et de la responsabilité de la protection des données), mais dans les limites du concept des droits d’utilisateur. Parallèlement aux mesures de protection de base, la Police cantonale doit veiller à ce que toute exportation ou transmission de données utiles à partir du système intervienne exclusivement sous forme cryptée, quel que soit le support des données.

Un programme de mesures est établi dès que cela s’avère opportunément possible (généralement après la décision d’achat, de sorte que la réalisation des mesures connues puisse être planifiée avec le fournisseur).

# 6. Contrôle

Le contrôle du respect des prescriptions SIPD est réalisé au moyen de la décision d’approbation de la Police cantonale pour l’exploitation du système de surveillance précédemment décrit. Au surplus, les dispositions de la législation cantonale sur la protection des données sont applicables ; cela signifie que le service communal chargé de la surveillance de la protection des données peut aussi contrôler ou faire contrôler ultérieurement que les prescriptions en matière de protection des données sont respectées.

1. En particulier la loi du 10 février 2019 sur la police (LPol), l’ordonnance du 29 avril 2009 sur l’utilisation d’appareils de vidéosurveillance lors de manifestations de masse et dans les lieux publics (Ordonnance sur la vidéosurveillance, OVid) et la loi du 19 février 1986 sur la protection des données (LCPD). [↑](#footnote-ref-1)