Analyse d'impact relative à la protection des données

Traitements de données à caractère personnel provenant des systèmes de vidéoprotection mis en œuvre par les autorités publiques

Responsable du traitement :

Identité : [A COMPLETER]

Adresse : [A COMPLETER]

Service gestionnaire :

Direction : [A COMPLETER]

Adresse : [A COMPLETER]

TABLE DES MATIERES

1. PRÉSENTATION GÉNÉRALE

Les systèmes de vidéoprotection se définissent comme des systèmes d'une ou plusieurs caméras disposées sur la voie publique ou dans des lieux et établissements ouverts au public et permettant la captation, l'enregistrement et la transmission d'images à des fins énumérées à l'article L.251-2 du code de la sécurité intérieure :

- La protection des bâtiments et installations publics et de leurs abords ;
- La sauvegarde des installations utiles à la défense nationale ;
- La régulation des flux de transport ;
- La constatation des infractions aux règles de la circulation ;
- La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions ;
- La prévention d'actes de terrorisme;
- La prévention des risques naturels ou technologiques ;
- Le secours aux personnes et la défense contre l'incendie ;
- La sécurité des installations accueillant du public dans les parcs d'attraction ;
- Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ;
- La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets ;
- La sécurité des personnes et des biens dans les lieux et établissements ouverts au public lorsqu'ils sont particulièrement exposés à des risques d'agression ou de vol.

1.1. Cadre juridique

Les systèmes de vidéoprotection sont régis par :

- Les dispositions du titre V de livre II du code de la sécurité intérieure (CSI), ainsi que par celles du chapitre III du titre II du même livre en ce qui concerne les systèmes de vidéoprotection mis en œuvre à des fins de prévention d'actes de terrorisme, qui les soumettent à un régime d'autorisation préfectorale ;
- Les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » et, le cas échéant, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

L'installation des systèmes de vidéoprotection est subordonnée à une autorisation préfectorale donnée, sauf en matière de défense nationale, après avis d'une commission départementale.

Le contenu du dossier de demande est fixé par l'article R. 252-3 du CSI.

2. PRÉSENTATION DU TRAITEMENT DES IMAGES

2.1 Vue d'ensemble

Finalités	☐	La protection des bâtiments et installations publics et de leurs abords
	☐	La sauvegarde des installations utiles à la défense nationale
	☐	La régulation des flux de transport
	☐	La constatation des infractions aux règles de la circulation
	☐	La prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées à ces infractions, des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes et des délits prévus à l'article 415 du même code portant sur des fonds provenant de ces mêmes infractions
	☐	La prévention d'actes de terrorisme, dans les conditions prévues au chapitre III du titre II du présent livre
	☐	La prévention des risques naturels ou technologiques
	☐	Le secours aux personnes et la défense contre l'incendie
	☐	La sécurité des installations accueillant du public dans les parcs d'attraction
	☐	Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile
	☐	La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets
	☐	La sécurité des personnes et des biens dans les lieux et établissements ouverts au public lorsqu'ils sont particulièrement exposés à des risques d'agression ou de vol
Identité et coordonnées du responsable de traitement	[Dénomination de l'autorité publique + adresses postale et électronique].	
Le cas échéant, identité et coordonnées du Délégué à la protection des données	[A compléter]	
Régime(s) juridique(s) applicable(s)	☐	Titre II et RGPD
	☐	Titre III
	☐	Titre IV
Enjeux du traitement	[Description concrète du besoin de recourir à un système de vidéoprotection]. ▪ Dissuader Présence visible des caméras dans les secteurs de délinquance avérés ou les territoires sensibles ; Contrôle des points de fixation de la délinquance : lieux de regroupements, de troubles à la tranquillité publique, points de passage obligés…	

	▪ Surveiller Identification, surveillance de certains individus recherchés, dans le cadre de procédures judiciaires : les services de police peuvent être amenés à solliciter les opérateurs pour l'identification de personnes recherchées Identification de véhicules impliqués dans des procédures judiciaires, Surveillance constante à distance de quartiers éloignés, difficiles d'accès ou très sensibles Protection des établissements sensibles. ▪ Assurer la gestion des événements de voie publique Surveillance et régulation du trafic routier, aide à la décision en matière de service d'ordre ou de maintien de l'ordre (manifestations de voie publique, festivités, déplacements officiels…) Les images permettent au responsable du dispositif de mieux appréhender la situation, la réactivité du dispositif à la situation est ainsi améliorée Vérification de l'adéquation des effectifs policiers à employer à la suite d'une demande d'intervention (appel 17), Appui des effectifs intervenants en zone difficile. ▪ Identifier des auteurs d'infraction En direct, l'opérateur détecte un événement, il avise immédiatement les services en charge de la sécurité qui jugent de la suite à donner aux faits observés. Dans le cadre d'une intervention, l'opérateur suit et guide, le cas échéant, l'unité d'intervention. En temps différé, les services de sécurité consulteront les enregistrements à des fins judiciaires, afin d'obtenir des éléments permettant d'identifier un auteur ou d'orienter une enquête.
Nombre de caméras	[Nombre de caméras]
Sous-traitant(s)	[Dénomination + siège social des sous-traitants + objet du contrat (ex : maintenance/exploitation)]

Textes applicables au traitement
Textes législatifs et réglementaires
Règlement général relatif à la protection des données Code de sécurité intérieure, [préciser si : chapitre III du titre II et] le titre V de son livre II de ses parties législatives et réglementaires Loi informatique et libertés, [préciser : son/ses titre II, III et/ou IV] Arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure Arrêté préfectoral d'autorisation [renseigner les références de l'arrêté]

Textes applicables au traitement	**Conditions d'applicabilité au traitement**	**Applicabilité au traitement (oui/non)**
Textes législatifs et réglementaires applicables en matière de protection des		

données		
Dispositions générales de la loi du 6 janvier 1978	Ces dispositions sont applicables à tout traitement de données à caractère personnel	Oui
Titre II de la loi du 6 janvier 1978 et règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD)	Le traitement relève du RGPD	**Oui/Non**
Titre III de la loi du 6 janvier 1978	Le traitement poursuit des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces par une autorité publique compétente	**Oui/Non**
Titre IV de la loi du 6 janvier 1978	Le traitement poursuit pour le compte de l'Etat et qui intéressent la sûreté de l'Etat ou la défense	**Oui/Non**

2.2. Données, processus et supports

2.1.1 Description des données

Données	Justification
Images captées	La collecte de ces images est nécessaire à la poursuite de l'une des finalités prévues par l'article L. 251-2 du code de la sécurité intérieure
Jour et plages horaires d'enregistrement	Besoin de traçabilité sur l'emploi du traitement par le responsable de traitement

Lieu où ont été collectées les données	Besoin de traçabilité sur l'emploi du traitement par le responsable de traitement
Identifiant de l'auteur, date, heure et motif de l'opération de collecte, de modification, de consultation, de communication et d'effacement des données à caractère personnel et informations, et, le cas échéant, destinataire des données	Besoin de traçabilité sur l'emploi du traitement par le responsable de traitement

Traçabilité :

Les opérations de collecte, de consultation, de communication et d'effacement des données à caractère personnel et informations, ainsi que les signalements générés par les traitements font l'objet d'un enregistrement.

Les journaux des opérations de consultation et de communication permettent d'établir la date, l'heure et le motif de ces opérations et d'identifier les personnes en étant à l'origine.

Ces informations sont conservées pour une durée maximale de 3 ans.

2.1.2. Accédants

Catégories d'accédants	Accédant concerné	Profil	Catégorie de données pouvant être obtenues
S'agissant des accédants visionnant des images prises dans des lieux et établissements ouverts au public			
Les opérateurs et agents qui relèvent du responsable du système, individuellement désignés et dûment habilités par lui	**[choisir oui ou non]**	**[A compléter]**	Les images prises dans des lieux et établissements ouverts au public
Les opérateurs privés agissant pour le compte du responsable du système, dans les conditions prévues à l'article L. 613-13	**[choisir oui ou non]**	**[A compléter]**	Les images prises dans des lieux et établissements ouverts au public
S'agissant des accédants visionnant des images prises sur la voie publique			
Les agents des services de police ou des unités de gendarmerie nationales et les agents des douanes et des services d'incendie et de secours, individuellement désignés et dûment habilités par le chef de service ou le chef d'unité à compétence départementale, régionale, zonale ou nationale sous l'autorité duquel ils sont affectés	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
Le maire ainsi que, lorsqu'ils sont délégataires de fonctions de police municipale au sens de			

Pour les seules images issues de systèmes implantés sur le territoire de la ou des communes pour lesquelles ils sont compétents	l'article L. 2212-2 du code général des collectivités territoriales et en application de l'article L. 2122-18 du même code, ses adjoints et les membres du conseil municipal	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
	Les agents de police municipale ainsi que les agents mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1 individuellement désignés et habilités par le maire	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
	Les agents des communes et les agents des établissements publics de coopération intercommunale et des syndicats mixtes agréés par le représentant de l'Etat en application de l'article L. 132-14-1	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
Les agents individuellement désignés et dûment habilités par les autres autorités publiques responsables du système		**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
Pour les seules images issues de son système de vidéoprotection	Les opérateurs qui relèvent de la personne morale autorisée à mettre en œuvre un système de vidéoprotection en application du premier alinéa de l'article L. 223-1, individuellement désignés et dûment habilités par elle	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur la voie publique
	Les opérateurs privés agissant pour le compte de la personne morale autorisée à mettre en œuvre un système de vidéoprotection en	**[choisir oui ou non]**	**[A compléter]**	Les images prises sur

	application du premier alinéa de l'article L. 223-1, dans les conditions prévues à l'article L. 613-13			la voie publique

2.1.3. Destinataires

Catégories de destinataires	Destinataire concerné	Catégorie de données pouvant être obtenues
les agents des services de police ou des unités de gendarmerie nationales, les agents des douanes ou des services d'incendie et de secours, les agents de police municipale ainsi que les agents mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1, individuellement désignés et dûment habilités, pour les seuls besoins de leurs missions, par le chef de service ou le chef d'unité à compétence départementale, régionale, zonale ou nationale sous l'autorité duquel ils sont affectés, et pour les seules images issues de systèmes implantés sur le territoire de la commune ou de l'établissement public de coopération intercommunale dont ils relèvent par le maire, s'agissant des agents de police municipale ainsi que les agents mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1	Oui	Les données mentionnées à l'article R. 253-1 du code de la sécurité intérieure
Les autorités administratives et judiciaires dont la présence est requise dans les salles de commandement au sein desquelles des images de vidéoprotection sont transmises	Oui	Les données mentionnées à l'article R. 253-1 du code de la sécurité intérieure
L'autorité administrative et les services compétents dans le cadre d'une procédure administrative	Oui	Les données mentionnées à l'article R. 253-1 du code de la sécurité intérieure
Les officiers et agents de police judiciaire	Oui	Les données mentionnées à l'article R. 253-1 du code de la sécurité intérieure
Les agents des services d'inspection générale de l'Etat	Oui	Les données mentionnées à l'article R. 253-1 du code de la sécurité intérieure

2.1.4. Données sensibles ou relatives aux condamnations pénales, infractions ou mesures de sûreté

Catégorie	Enregistrement (oui / non)	Justification de la collecte
Données sensibles de l'article 6 de la loi du 6 janvier 1978		
La prétendue origine raciale ou l'origine	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir

ethnique		des faits visibles enregistrés dans le fichier vidéo
Les opinions politiques	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
Les convictions religieuses	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
Les convictions philosophiques	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
L'appartenance syndicale	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
La santé	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
La vie sexuelle ou l'orientation sexuelle	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo
Les données génétiques	Non	Sans objet
Les données biométriques aux fins d'identifier une personne physique de manière unique	Non	Sans objet
Données de l'article 46 de la loi du 6 janvier 1978		
Les condamnations pénales	Non	Sans objet
Les infractions	Oui	L'enregistrement de ces données n'est pas réalisé à dessein, mais de telles données peuvent être collectées, directement ou indirectement, à partir des faits visibles enregistrés dans le fichier vidéo.
Les mesures de sûreté	Non	Sans objet

2.1.5. Description des traitements de données et supports

Traitements données	Description détaillée des traitements de données	Supports des données concernés
1. Captation, enregistrement et transmission des images	[Décrire les différents composants du système de vidéoprotection procédant à la captation, à l'enregistrement des images et à leur transmission vers les opérateurs vidéo : - Nombre et lieu d'implantation des caméras ; - Centre de supervision ; - Système analogique ou numérique ; - Caméras fixes ou orientables, caméras dômes, caméras PTZ, caméras mégapixel, plan large ou plan étroit, résolution des images, standards vidéo,	[A compléter]

	capacité de zoom, sensibilité à la lumière ; - Câbles de transmission des images (cuivre coaxial, fibre optique, cuivre multipolaires, liaison radio) ; - Convertisseurs, normes de compression des images ; - Système d'enregistrement des données (DVR ou NVR), capacité de stockage ; - Postes informatiques de visualisation/pilotage (IHM), mur d'images, main courante informatisée, système de journalisation…] [Indiquer si le système est supervisé ou non, les plages horaires].	
2. Transfert des données	[Le cas échéant, indiquer les modalités de transfert des images vers les destinataires mentionnés à l'article L.252-3 du CSI (ex : services de police)]	[A compléter]
3. Consultation des données	[Décrire les modalités de consultation des données, y compris des enregistrement en direct]	[A compléter]
4. Extraction des données	[Décrire les modalités d'extraction des données en direct ainsi que des enregistrements]	[A compléter]

3. PRINCIPES FONDAMENTAUX

3.1. Mesures garantissant la proportionnalité et la nécessité du traitement

3.1.1. Finalités

Finalités	Légitimité
[Par exemple : Régulation des flux de transport]	[Par exemple : embouteillages et accidents fréquents…]

3.1.2. Fondement juridique et base légale

Le traitement des images provenant de systèmes de vidéoprotection est mis en œuvre dans les conditions prévues aux chapitres II et IV du titre V du livre II du code de la sécurité intérieure.
Le traitement des images relève du titre II de la loi informatique et libertés et du règlement (UE) 2016/679 du 27 avril 2016 ou du titre III de la loi informatique et libertés applicables aux traitements entrant dans le champ de la directive (UE) 2016/680.

La base de licéité des traitements d'images dépend de leur finalité et de la qualité du responsable du système peuvent. Ainsi, lorsque le système est mis en œuvre par une autorité publique compétente, le traitement aura pour base de licéité la nécessité à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement. En revanche, si celle-ci n'est pas applicable ou lorsque le système est mis en œuvre par des personnes morales de droit privé, le traitement aura pour base de licéité la nécessité aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Les traitements ont pour base de licéité le XX de l'article 5 de la loi n° 78-17 du 6 janvier 1978 ou le XX du 1. de l'article 6 du règlement n°2016/679.

3.1.3. Minimisation des données

Détail des données traitées	Mesures de minimisation
Images captées. Jour et plages horaires d'enregistrement. Lieu où ont été collectées les données.	[Indiquer les mesures de minimisation (par ex : formation des opérateurs vidéo ; séparation des enregistrements et des images en temps réel ; plusieurs salles dédiées respectivement à l'exploitation des images, aux équipements techniques, et à la relecture des images ; limitation des accès aux images aux seuls agents habilités ; floutage des lieux d'habitation)]

3.1.4. Qualité des données

Mesures pour la qualité des données	Modalités de mise en œuvre
Intégrité des images	Les données collectées sont exclusivement tirées des images collectées. Il n'est pas possible de procéder à une rectification matérielle des images. Le format et la fréquence des images sont définis par l'arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure.
Horodatage et lieu où ont été collectées les données	La date et les plages horaires de la collecte des images sont générées automatiquement et ne peuvent être modifiés
[A compléter]	[A compléter]

A cet égard, les systèmes de vidéoprotection doivent être conformes à l'arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure.

3.1.5. Durées de conservation

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Images captées Jour et plages horaires d'enregistrement.	[Indiquer la durée de conservation, qui est celle des images fixées par l'arrêté préfectoral dans la limite d'un mois, conformément à l'article L.252-3 du CSI]	Permettre le traitement des enregistrements des images et la prise de décision d'une éventuelle extraction de données pour les besoins d'une procédure judiciaire, administrative ou disciplinaire.	Hors le cas où ils sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire, les enregistrements sont automatiquement effacés.

Lieu où ont été collectées les données.			

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable	Si améliorable, mesures prévues dans le plan d'action
Finalités : déterminées, explicites et légitimes Les finalités des traitements sont expressément définies à l'article L. 251-2 CSI.	**Acceptable**	
Fondement : licéité du traitement	**Acceptable**	
Minimisation des données : adéquates, pertinentes et limitées.	**Acceptable/ améliorable**	[à compléter le cas échéant]
Qualité des données : exactes et tenues à jour.	**Acceptable**	
Durée de conservation : limitée à une durée maximale de trente jours dans le cas de données à caractère personnel.	**Acceptable**	

3.2. Évaluation des mesures protectrices des droits des personnes concernées

3.2.1. Mesures pour l'information des personnes

Les personnes concernées par les traitements doivent être informées dans les conditions prévues par la loi informatique et libertés et le code de la sécurité intérieure.

L'article R. 253-6 du CSI prévoit que l'information doit aussi être apportée au moyen d'affiches ou de panonceaux comportant un pictogramme représentant une caméra.

Les informations prévues [à l'article 14 du règlement (UE) 2016/679 du 27 avril 2016] ou {[à l'article 104] ou [à l'article 116] de la loi du 6 janvier 1978} sont mises à disposition des personnes concernées.

Mesures pour le droit à l'information	Modalités de mise en œuvre et justifications
Présentation des conditions d'utilisation/confidentialité	L'information du responsable de traitement est délivrée sur les lieux d'installation des caméras à l'aide d'affiches ou de panonceaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié [détailler : site internet du service autorisé à recourir aux traitements par exemple]
Possibilité d'accéder aux conditions d'utilisation/confidentialité	L'information du responsable de traitement est délivrée sur les lieux d'installation des caméras à l'aide d'affiches ou de panonceaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié [détailler : site internet du service autorisé à recourir aux traitements par exemple]
Conditions lisibles et compréhensibles	L'information du responsable de traitement est délivrée sur les lieux d'installation des caméras à l'aide d'affiches ou de panonceaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié [détailler : site internet du service autorisé à recourir aux traitements par exemple]
Présentation détaillée des finalités des	L'information du responsable de traitement est délivrée sur les lieux

traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)	d'installation des caméras à l'aide d'affiches ou de panonceaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié [détailler : site internet du service autorisé à recourir aux traitements par exemple]
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)	L'information du responsable de traitement est délivrée sur les lieux d'installation des caméras à l'aide d'affiches ou de panonceaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié [détailler : site internet du service autorisé à recourir aux traitements par exemple]
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation	[A compléter le cas échéant]
Modalités de contact du responsable de traitement (identité et coordonnées) pour les questions de confidentialité	Les coordonnées du responsable de traitement sont [à compléter]. Le Délégué à la protection des données (DPD) du responsable de traitement peut également être contacté au courriel suivant [à compléter]
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité	[A compléter le cas échéant]

3.2.2 Mesures pour le recueil du consentement

Le consentement ne constitue pas la base de licéité des traitements. Il n'est donc pas recueilli.

3.2.3. Mesures pour les droits d'accès et à la portabilité

Le droit d'accès prévu [à l'article 105 de la loi n° 78-17 du 6 janvier 1978] ou [à l'article 15 du règlement (UE) 2016/679 du 27 avril 2016 s'exerce directement auprès du responsable de traitement] ou [le droit d'accès s'exerce auprès de la CNIL dans les conditions prévues à l'article 118 de la loi n° 78-17 du 6 janvier 1978.]

[OPTION 1 : Afin d'éviter de gêner des enquêtes et des procédures administratives ou judiciaires ou d'éviter de nuire à la prévention ou la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière, le droit d'accès peut faire l'objet de restrictions en application des 2° et 3° du II et du III de l'article 107 de la même loi.

La personne concernée par ces limitations exerce son droit auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 108 de la même loi.]

[OPTION 2 : Afin de garantir la sécurité nationale, la protection contre les menaces pour la sécurité publique ou la prévention de telles menaces, le droit d'accès peut faire l'objet de restrictions en application de l'article 23 du même règlement.

La personne concernée par ces limitations exerce son droit auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 118 de la même loi.]

Le droit à la portabilité des données prévu à l'article 20 du règlement UE 2016/679 du 27 avril 2016 n'est pas applicable au traitement.

3.2.4. Mesures pour les droits de rectification et d'effacement

[OPTION 1] Les droits de rectification et d'effacement prévus {[à l'article 106 de la loi n° 78-17 du 6 janvier 1978] ou [aux articles 16 et 17 du règlement (UE) 2016/679 du 27 avril 2016] s'exercent directement auprès du responsable de traitement ou [auprès de la CNIL dans les conditions prévues à l'article 118 de la loi n° 78-17 du 6 janvier 1978]}.

[OPTION 2] Le droit de rectification prévu [à l'article 16 du règlement (UE) 2016/679 du 27 avril 2016 s'exercent directement auprès du responsable de traitement. Le droit à l'effacement ne s'applique pas.]

3.2.5. Mesures pour les droits à la limitation du traitement et d'opposition

Le droit à la limitation prévu {[à l'article 106 de la loi n° 78-17 du 6 janvier 1978] ou [à l'article 18 du règlement (UE) 2016/679 du 27 avril 2016] s'exerce directement auprès du responsable de traitement] ou [Lorsque le traitement relève du titre IV de la loi n° 78-17 du 6 janvier 1978, aucun droit à la limitation n'est prévu.]}

Conformément à l'article 110 de la même loi ou à l'article 23 du même règlement, le droit d'opposition ne s'applique pas au présent traitement.

3.2.6. Mesures pour la sous-traitance

Nom du sous-traitant	Objet du contrat	Référence du contrat	Conformité
[A compléter]	[A compléter]	[A compléter]	[A compléter]

3.2.7. Mesures pour le transfert de données en dehors de l'Union européenne

Dans l'hypothèse où il était recouru à un sous-traitant soumis au droit d'un Etat n'appartenant pas à l'Union européenne, impliqué dans un transfert de données à caractère personnel en dehors de l'Union européenne, celui-ci devra respecter les règles et, le cas échéant, les garanties appropriées prévues, selon le champ d'application du traitement :

- au « Chapitre IV : Transferts de données à caractère personnel vers des États n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des États n'appartenant pas à l'Union européenne » de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,
- au « Chapitre V : Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales » du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ou
- à la section 3 : « Transferts de données à caractère personnel vers des Etats n'appartenant pas à l'Union européenne ou vers des destinataires établis dans des Etats n'appartenant pas à l'Union européenne » du chapitre 2 de la même loi.

Mesures protectrices des droits des personnes concernées	Acceptable / Améliorable ?	Si améliorable, mesures prévues dans le plan d'action
Information des personnes concernées (traitement loyal et transparent)	Acceptable	
Recueil du consentement	Non applicable	
Exercice des droits d'accès et à la portabilité	Droit d'accès : Acceptable Droit à la portabilité : non applicable	

Exercice des droits de rectification et d'effacement	Droit de rectification : acceptable Droit d'effacement : Acceptable/non applicable	
Exercice des droits à la limitation du traitement et d'opposition.	Droit d'opposition : non applicable Droit à la limitation : Acceptable/non applicable	
[Sous-traitance : identifiée et contractualisée]	Acceptable/Améliorable/non applicable	

4. ETUDE DES RISQUES LIÉS À LA SÉCURITÉ DES DONNÉES

4.1. Évaluation des mesures

Le responsable de traitement devra mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

4.1.1. Mesures contribuant à traiter des risques liés à la sécurité des données

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Si améliorable, mesures prévues dans le plan d'action
Chiffrement	Les systèmes commercialisés prévoient des enregistrements chiffrés. Il existe plusieurs modes de cryptage en fonction du choix effectué par le responsable de traitement mais ce dernier devra prévoir a minima un chiffrement conforme à l'état de l'art. Seul l'administrateur du système a les clefs du chiffrement pour les relectures et extractions. Chaque responsable de traitement devra faire en sorte de vérifier que le procédé de chiffrement permettra de contribuer à lutter contre la suppression des enregistrements sur les caméras elles-mêmes et dans les serveurs.	Acceptable	
Cloisonnement des données	Pour la grande majorité des dispositifs de vidéoprotection, aucune connexion au réseau Internet n'est réalisée, afin d'éviter tout piratage des images collectées.	Acceptable/ améliorable	
Sécurité physique	Les locaux où sont enregistrées les images font l'objet d'un contrôle d'accès (soit accès par badge, par code ou clé conservée par le responsable, soit local sous alarme). Ces locaux ne sont accessibles qu'aux personnes autorisées à visionner les images au sens du I. de l'article R. 253-3 du code de la sécurité intérieure.	Acceptable	

Contrôle des accès logiques	Il n'est possible d'accéder aux données qu'après une authentification.	Acceptable	
Journalisation	Les opérations de collecte, de modification, de consultation, de communication et d'effacement des données à caractère personnel font l'objet d'un enregistrement comprenant l'identifiant de l'auteur, la date, l'heure, le motif de l'opération et, le cas échéant, les destinataires des données. Ces informations sont conservées pendant 3 ans maximum.	Acceptable	
Pseudonymisation	[A compléter]	Acceptable/ améliorable	
Archivage	[Définir l'ensemble des modalités de conservation et gestion d'archives électroniques contenant des données à caractère personnel destinées à garantir leur valeur, notamment juridique, pendant toute la durée nécessaire (versement, stockage, migration, accessibilité, élimination, politique d'archivage, protection de la confidentialité, etc.)] Il doit se conformer aux exigences de l'arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure	Acceptable	

4.1.2. Mesures générales de sécurité

Sécurité de l'exploitation	Les mises à jour des systèmes et logiciels sont assurés par l'administrateur. Les gestionnaires sont clairement identifiés et formés.	Acceptable	
Lutte contre les logiciels malveillants	La lutte contre les logiciels malveillants est garantie par le fait que le serveur où les images sont enregistrées est hors réseau. En particulier, il est recommandé d'installer un antivirus sur les serveurs et postes de travail, de le configurer et de tenir à jour les logiciels antivirus, de mettre en œuvre des mesures de filtrage des flux et de faire remonter les événements de sécurité de l'antivirus. Il est également recommandé d'installer un programme de lutte contre les logiciels espions sur les postes de travail, le configurer et le tenir à jour.	Acceptable	
Mot de passe	Il n'est possible d'accéder aux données qu'après une authentification qui s'effectue par le biais de mots de passe individualisés avec un contrôle des logs de connexion. La politique de mot de passe pour accéder aux données est conforme à la délibération n° 2022-100 du 21 juillet 2022 de la CNIL	Acceptable	
Sécurité des sites web	Pour la grande majorité des dispositifs de vidéoprotection, aucune connexion au réseau Internet n'est réalisée, afin d'éviter tout piratage des	Acceptable	

	images collectées.		
Sauvegarde des logs	[Préciser si la sauvegarde des logs est cryptée au même niveau de sécurité que la solution en production et efface les contenus au bout de XXXX.]	Acceptable/ améliorable	
Maintenance	La maintenance est assurée par le fournisseur du dispositif pour remise en service du système en cas de panne ou de dysfonctionnement des enregistrements. Ce dernier n'a pas de droit de déchargement des contenus vidéos.	Acceptable	
Sécurité des canaux informatiques (réseaux)	La solution est sécurisée dans une zone de commutation distincte par Vlan, le Firewall protège ces zones par l'ouverture des ports strictement nécessaire et fourni les Logs d'accès à cet élément technique des PC ou équipements se connectant à cet équipement. Les logs des firewalls sont conservés trois ans.	Acceptable	
Surveillance	Contrôle régulier par le responsable de la journalisation, de l'accès aux postes informatiques et de leur utilisation	Acceptable	
Sécurité des matériels	Le serveur de stockage des images est placé dans un local dédié sous contrôle d'accès physique.	Acceptable	

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Si améliorable, mesures prévues dans le plan d'action
Organisation	Chaque responsable de traitement définit son organisation : - chef de service ; - responsable sécurité ; - responsable juridique ; - responsable technique ; - délégué à la protection des données ; - numéro d'urgence pour l'accès aux images- ; règlement intérieur ; - convention de partenariat avec les FSI[…]	Acceptable/ améliorable	
Politique (gestion des règles)	Formation, charte informatique, règles de gestion des habilitations des administrateur, agents habilités et leurs profils	Acceptable	
Gestion des risques	Traçabilité des connexions consultables par le biais de la journalisation. Un plan de prévention ou de gestion des risques peut être prévu par le responsable de traitement.	Acceptable	
Gestion des projets	Le choix du dispositif mis en place relève de chaque responsable de traitement. Il peut être prévu un comité de pilotage intégré au CLSPD, des référents sûreté de la police ou gendarmerie ou encore une aide à la maîtrise d'ouvrage	Acceptable/ améliorable	
Gestion des incidents et des	Les rôles et responsabilités des parties prenantes ainsi que les procédures de remontées d'informations et de	Acceptable	

violations de données	réaction cas de violation de données sont prévues. Une qualification et un traitement adapté des violations de données sont effectués selon leur impact sur les droits et libertés des personnes concernées. [Des mesures préventives sont mises en place, se traduisant par une information sur l'utilisation de la caméra, la signature d'une charte d'utilisation ou encore une procédure de remontée d'information en cas de constat de violation de données. Un enregistrement au journal de la défaillance constatée et une alerte des agents du dysfonctionnement constaté peut être mis en place.]		
Gestion des personnels	Les accès aux traitements sont restreints à un nombre limité d'agents qui sont formés à l'usage et l'emploi des dispositifs de vidéoprotection.	Acceptable	
Relations avec les tiers	[Préciser : convention, relation avec la police, les pompiers etc.]	Acceptable/ améliorable	
Supervision	Le responsable de traitement veille par des contrôles aux connexions afin de détecter des accès anormaux mais aussi aux éventuels incidents.	Acceptable	

4.2. Appréciation des risques : les atteintes potentielles aux droits et libertés des personnes physiques

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données	Usurpation ou divulgation de mot de passe Action interne par un personnel Cyberattaque automatisée (virus) ou volontaire par ingénierie sociale. Acte involontaire : un utilisateur légitime dispose d'un accès élargi (suite à un dysfonctionnement) et accède à des données auxquelles il n'aurait pas dû Piratage du flux de transmission des données entre les caméras de vidéoprotection et les salles de commandement Vol du matériel par un tiers	Mauvaise gouvernance Intégrité et confidentialité des données. Effacement des données Consultation et extraction des données collectées en vue d'une divulgation ou d'une utilisation illégale	Risque d'atteinte à la vie privée Concernant les enregistrements mettant en cause une personne, une victime ou un témoin : risque de menaces ou harcèlement et perte de réputation, de dégradation de biens en représailles ou de violences si diffusion des données suite à un accès illégitime Discrédit de l'usage du dispositif Accessoirement atteinte au secret dans le cadre d'une procédure judiciaire	Respect stricte des règles de confidentialité, des accès aux locaux, des mots de passe avec mesures de contrôle des logs.	Importante Les images vidéo permettent d'identifier des personnes physiques et, le cas échéant, leur associer des comportements. Un accès illégitime pourrait avoir des conséquences importantes pour la personne filmée, et notamment atteinte au droit au respect de la vie privée.	Limitée

Modification non désirées de données	Accès physique à la caméra, à la salle de commandement ou à la solution de stockage	Modification des informations collectées ne permettant plus d’utiliser celles-ci à l’appui d’une procédure.	Impossibilité d’exploiter les informations et de les utiliser dans le cadre d’une procédure qu’elle soit judiciaire, administrative ou disciplinaire en tant que preuve. Intégrité et confidentialité des données, perte de crédibilité, perte de réputation, sentiment d’injustice si les images altérées accusent à tort ou empêchent la saisie correcte de justice Risque de dégradations de biens en représailles ou de violence pour une personne injustement mise en cause Perte de chance pour la victime d’obtenir réparation du préjudice subi si le ou les responsables sont supprimés des enregistrements	Gestion des accès logique et physique à la solution, fermeture des ports de communications non utiles, traçabilité. Information des personnels sur la gestion de données critiques. Sauvegarde des données	Importante mais une modification des images captées serait nécessairement détectée car portant atteinte à l’intégrité de la donnée.	Limitée

Disparition de données	Perte de contrôle sur la caméra de vidéoprotection Destruction de la caméra par les personnels du service Destruction par un tiers Introduction usurpée ou frauduleuse dans le système de conservation Cas de force majeure : incendie, inondation	Dysfonctionnement du stockage, erreur de manipulation du personnel, problème de maintenance ou défaillance technique	Incapacité à produire lesinformation attendues au regard des finalités Impossibilité d’exploiter les informations et de les utiliser dans le cadre d’une procédure judiciaire, administrative ou disciplinaire. Perte de confiance des agents et des personnes liées au défaut de sécurisation des enregistrements Destruction de matériels, pertes financières	Maintenance, contrôles réguliers du dispositif et des connexions Stockage des données en lieu sécurisé, et accès logique aux données contrôlées. Cryptage des données sur la zone de stockage. Mise en place d’un mécanisme rendant impossible la suppression des images par les personnels. Mise en place de procédures de sauvegarde ou de réplication	Importante mais une suppression des données serait détectée par les informations de traçabilité.	Limitée

5. VALIDATION DE L'ANALYSE D'IMPACT

5.1. Eléments utiles à la validation

Finalités	Evaluation	Si améliorable, mesures prévues dans le plan d'action
Mesures garantissant la proportionnalité et la nécessité du traitement		
Finalités : déterminées, explicites et légitimes	Acceptable	
Fondement : licéité du traitement, interdiction du détournement de finalité	Acceptable	
Minimisation des données : adéquates, pertinentes et limitées	Acceptable	
Qualité des données : exactes et tenues à jour	Acceptable	
Durées de conservation : limitées	Acceptable	
Mesures protectrices des droits des personnes des personnes concernées		
Information des personnes concernées (traitement loyal et transparent)	Acceptable	
Recueil du consentement	Non applicable	
Exercice des droits d'accès et à la portabilité	Droit d'accès : Acceptable Droit à la portabilité : non applicable	
Exercice des droits de rectification et d'effacement	Droit de rectification : acceptable Droit d'effacement : Acceptable/non applicable	
Exercice des droits à la limitation du traitement et d'opposition	Droit d'opposition : non applicable Droit à la limitation : Acceptable/non applicable	
Sous-traitance : identifiée et contractualisée	Acceptable/Améliorable/non applicable	

Finalités	Evaluation
Mesures portant spécifiquement sur les données du traitement	

Chiffrement	Acceptable
Pseudonymisation	Acceptable/améliorable
Cloisonnement des données (par rapport au reste du système d'information)	Acceptable/améliorable
Contrôle des accès logiques des utilisateurs	Acceptable
Traçabilité (journalisation)	Acceptable
Archivage	Acceptable
Sécurité des documents papier	Sans objet
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	
Sécurité de l'exploitation	Acceptable
Lutte contre les logiciels malveillants	Acceptable
Sécurité des sites web	Acceptable
Sauvegardes	Acceptable
Maintenance	Acceptable
Sécurité des canaux informatiques (réseaux)	Acceptable
Surveillance	Acceptable
Sécurité des matériels	Acceptable
Mesures organisationnelles (gouvernance)	
Organisation	Acceptable/améliorable
Politique (gestion des règles)	Acceptable
Gestion des risques	Acceptable
Gestion des projets	Acceptable/améliorable
Gestion des incidents et des violations de données	Acceptable
Gestion des personnels	Acceptable
Relations avec les tiers	Acceptable/améliorable
Supervision	Acceptable

5.1.3. Cartographie des risques liés à la sécurité des données

Avant mesures :

Accès illégitime à des données

Modification non désirée de données

Disparition de données

Gravité du risque	**Maximale**				
	Importante				
	Limitée				
	Négligeable				
Cartographie des risques		**Négligeable**	**Limitée**	**Importante**	**Maximale**
		Vraisemblance du risque			

Après mesures :

 Accès illégitime à des données

 Modification non désirée de données

 Disparition de données

Gravité du risque	**Maximale**				
	Importante				
	Limitée				
	Négligeable				
Cartographie des risques		**Négligeable**	**Limitée**	**Importante**	**Maximale**
		Vraisemblance du risque			

5.1.3. Plan d'actions (si mesures correctives prévues) :

Mesures à améliorer	Mesures correctives prévues	Calendrier
[A compléter]	[A compléter]	[A compléter]
[A compléter]	[A compléter]	[A compléter]
[A compléter]	[A compléter]	[A compléter]

5.2. Validation formelle

Avis du délégué à la protection des données :

[A compléter]

Validation par le responsable de traitement

[A compléter]

Le (*responsable du traitement)* atteste que la présente analyse décrit la mise en œuvre du traitement. Il estime le niveau des risques résiduels pour les droits et les libertés des personnes concernées comme suffisamment faible et acceptable et s'engage à traiter les données conformément à la présente analyse, au règlement général sur la protection des données et la loi n°78-1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

6. ANNEXES

Echelles d’analyse des risques :

- Echelle de gravité
- Echelle de vraisemblance (cf. partie REF _Ref514201510 \n \h

• Niveaux de gravité	• Descriptions génériques des impacts (directs et indirects)	• Exemples d'impacts corporels	• Exemples d'impacts matériels	• Exemples d'impacts moraux
1. Négligeable	• Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté.	• Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) • Maux de tête passagers	• Perte de temps pour réitérer des démarches ou pour attendre de les réaliser • Réception de courriers non sollicités (ex. : spams) • Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier) • Publicité ciblée pour des produits de consommation courants	• Simple contrariété par rapport à l'information reçue ou demandée • Peur de perdre le contrôle de ses données • Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale) • Perte de temps pour paramétrer ses données • Non-respect de la liberté d'aller et venir en ligne du fait du refus d'accès à un site commercial (ex : alcool du fait d'un âge erroné)

2. Limitée	• Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	• Affection physique mineure (ex. : maladie bénigne suite au non- respect de contre-indications) • Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) • Diffamation donnant lieu à des représailles physiques ou psychiques	• Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement • Refus d'accès à des services administratifs ou prestations commerciales • Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne) • Promotion professionnelle manquée • Compte à des services en ligne bloqué (ex. : jeux, administration) • Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées • Élévation de coûts (ex. : augmentation du prix d'assurance) • Données non mises à jour (ex. : poste antérieurement occupé) • Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.) • Publicité ciblée en ligne sur	• Refus de continuer à utiliser les systèmes d'information (*whistleblowing*, réseaux sociaux) • Affection psychologique mineure mais objective (diffamation, réputation) • Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance) • Sentiment d'atteinte à la vie privée sans préjudice irrémédiable • Intimidation sur les réseaux sociaux

3. Importante	• Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.	• Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non- respect de contre-indications) • Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.	• Détournements d'argent non indemnisé • Difficultés financières non temporaires (ex. : obligation de contracter un prêt) • Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen) • Interdiction bancaire • Dégradation de biens • Perte de logement • Perte d'emploi • Séparation ou divorce • Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage / *phishing*) • Bloqué à l'étranger • Perte de données clientèle	• Affection psychologique grave (ex. : dépression, développement d'une phobie) • Sentiment d'atteinte à la vie privée et de préjudice irrémédiable • Sentiment de vulnérabilité à la suite d'une assignation en justice • Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression) • Victime de chantage - *Cyberbullying* et harcèlement moral
4. Maximale	• Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	• Affection physique de longue durée ou permanente (ex. : suite au non-respect d'une contre-indication) • Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l'intégrité physique	• Péril financier • Dettes importantes • Impossibilité de travailler • Impossibilité de se reloger • Perte de preuves dans le cadre d'un contentieux • Perte d'accès à une infrastructure vitale (eau, électricité)	• Affection psychologique de longue durée ou permanente • Sanction pénale • Enlèvement • Perte de lien familial • Impossibilité d'ester en justice • Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)

• Niveaux de vraisemblance	• Description générique du niveau de vraisemblance d'une menace donnée
1. Négligeable	• Il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).
2. Limité	• Il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).
3. Important	• Il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).
4. Maximal	• Il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).