

Analyse d'impact relative à la protection des données

La Vidéoprotection

Responsable du traitement :

Identité : **Commune de Montmédy**

Adresse : 1 place Raymond Poincaré 55600 Montmédy

Service gestionnaire :

Direction : Direction Générale des Services

Adresse : 1 place Raymond Poincaré 55600 Montmédy

Table des matières

1. Présentation générale	4
1.1. Cadre juridique.....	4
2. Présentation du traitement des images	5
2.1. Vue d'ensemble.....	5
2.2 Données, processus et supports	8
2.1.1. Description des données	8
2.1.1. Accédants.....	9
2.1.3. Destinataires	12
2.1.4. Données sensibles ou relatives aux condamnations pénales, infractions pu mesures de sûreté.....	13
2.1.5. Description des traitements de données et supports	14
3. Principe fondamentaux	14
3.1. Mesures garantissant la proportionnalité et la nécessité du traitement.....	14
3.1.1. Finalités.....	14
3.1.2. Fondement juridique et base légale	15
3.1.3. Minimisation des données.....	16
3.1.4. Qualité des données	17
3.1.5. Durées de conservation.....	17
3.1.6. Axe d'amélioration	18
3.2. Evaluation des mesures protectrices des droits des personnes concernées.....	19
3.2.1. Mesures pour l'information des personnes.....	19
3.2.2. Mesures pour le recueil du consentement.....	20

3.2.3. Mesures pour les droits d'accès et à la portabilité	20
3.2.4. Mesures pour les droits de rectification et d'effacement.....	21
3.2.5. Mesures pour les droits à la limitation du traitement et d'opposition.....	21
3.2.5. Mesures pour la sous-traitance	21
3.2.7. Mesures pour transfert de données en dehors de l'Union européenne.....	22
4. Etude des risques liés à la sécurité des données.....	23
4.1. Evaluation des mesures.....	23
4.1.1. Mesures générales de sécurité	23
4.1.2. Mesures organisationnelles	24
4.2. Appréciation des risques : les atteintes potentielles aux droits et libertés des personnes physiques	28
5. Validation de l'analyse d'impact	30
5.1. Eléments utiles à la validation.....	30
5.1.1. Synthèse relative à la conformité	30
5.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données	32
5.1.3. Cartographie des risques liés à la sécurité des données	33
5.1.3. Plan d'actions (si mesures correctives prévus)	Erreur ! Signet non défini.
5.2 Validation formelle	35
6. Annexes	36

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	X	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
	X	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
	X	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
	X	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
	X	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	Commune de Montmédy – 1 place Raymond Poincaré 55600 Montmédy dgs@montmedy.fr - Sous la responsabilité du maire	
Identité et coordonnées du Délégué à la protection des données	Centre de gestion de la Meuse 92 Rue des Capucins, 55200 COMMERCY dpo.informatique@cdg55.fr	
Régime(s) juridique(s) applicable(s)	X	Titre II et RGPD
	X	Titre III
		Titre IV
Enjeux du traitement	<ul style="list-style-type: none"> ▪ <u>Dissuader</u> 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... ▪ <u>Surveiller</u> Prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés aux dégradations et actes de vandalisme et à la délinquance urbaine. ▪ <u>Assurer la gestion des événements de voie publique</u> Surveillance 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 de mieux appréhender la situation. ▪ <u>Identifier des auteurs d'infraction</u> Dans le cadre d'une intervention, l'opérateur suit et guide, le cas échéant, l'unité d'intervention sur demande expresse des services de l'Etat. 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	<ul style="list-style-type: none">- 0 caméra intérieure (installée dans des lieux ouverts au public).- 0 caméra extérieure (ne filmant pas la voie publique mais les abords des bâtiments).- 11 caméras visionnant la voie publique.
Sous-traitant(s)	INEO INFRACOM 5 rue Lavoisier 21 600 LONGVIC Installateur

Textes applicables au traitement

Textes législatifs et réglementaires

Règlement général relatif à la protection des données

Code de sécurité intérieure, **titre V de son livre II de ses parties législatives et réglementaires**

Loi informatique et libertés, **ses titres II et III**

Arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure : Arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance - NOR : IOCD0762353A

Arrêté préfectoral d'autorisation : AP-2022-1499 du 4 juillet 2022 de la Préfecture de la Meuse

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
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
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	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.

2.1.1. 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 NON CONCERNE			

Les opérateurs et agents qui relèvent du responsable du système, individuellement désignés et dûment habilités par lui	Non		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	Non		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	Non		Les images prises sur la voie publique	
Pour les seules images issues de systèmes implantés sur le territoire de la ou des communes pour lesquelles ils sont compétents	Le maire ainsi que, lorsqu'ils sont délégués de fonctions de police municipale au sens de 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	Oui	Le maire	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	Oui	Le DGS	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	Non		Les images prises sur la voie publique
Les agents individuellement désignés et dûment habilités par les autres autorités publiques responsables du système	Non		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	Non		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 application du premier alinéa de l'article L. 223-1, dans les conditions prévues à l'article L. 613-13	Non		Les images prises sur 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 pu mesures de sûreté

Catégorie	Enregistrement (oui / non)	Justification de la collecte
<u>Données sensibles de l'article 6 de la loi du 6 janvier 1978</u>		
La prétendue origine raciale ou l'origine ethnique	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. En conséquence aucune exploitation à dessein ne pourra être réalisée sur ces catégories de données sensibles susceptibles d'être collectées.
Les opinions politiques	Oui	
Les convictions religieuses	Oui	
Les convictions philosophiques	Oui	
L'appartenance syndicale	Oui	
La santé	Oui	
La vie sexuelle ou l'orientation sexuelle	Oui	
Les données génétiques	Non	Sans objet
Les données biométriques aux fins d'identifier une personne physique de manière unique	Non	Sans objet
<u>Données de l'article 46 de la loi du 6 janvier 1978</u>		
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	Le système est composé de 11 caméras numériques (0 intérieure, 1 extérieure et 10 sur la voie publique) implantées sur le territoire de la Commune de Montmédy. Les images sont captées en continu sur un mur d'images. La transmission des images vers le serveur d'enregistrement s'effectue via un réseau physique dédié et fermé, sans connexion à Internet, ce qui garantit un haut niveau de sécurité contre les intrusions distantes. Le système n'est pas supervisé en temps réel par un opérateur dédié ; les images sont consultées a posteriori en cas d'incident.	<ul style="list-style-type: none">- Caméras de vidéoprotection- Câblage réseau (fibre optique ou cuivre)- Serveur d'enregistrement (NVR)
2. Transfert des données	Aucun transfert systématique des données vers des destinataires externes n'est opéré. Les images ne sont communiquées qu'aux autorités compétentes (forces de l'ordre, services de secours) sur la base d'une réquisition judiciaire formelle.	Non applicable (hors réquisition)
3. Consultation des données	La consultation des images, en direct ou enregistrées, s'effectue depuis un poste de visualisation unique situé dans les locaux de la Mairie, au 1 place Raymond Poincaré. L'accès à ce poste est restreint aux 2 personnes habilitées et sécurisé par un code d'accès.	<ul style="list-style-type: none">- Poste informatique de visualisation- Serveur d'enregistrement (NVR)
4. Extraction des données	L'extraction des enregistrements est une opération exceptionnelle, réalisée uniquement pour les besoins d'une procédure judiciaire, administrative ou disciplinaire. Elle est effectuée par l'une des personnes habilitées sur un support externe (ex : clé USB, disque dur). Une procédure stricte doit encadrer cette opération pour garantir la traçabilité et la sécurité des données exportées.	<ul style="list-style-type: none">- Supports de stockage amovibles (clé USB, disque dur externe)

3. Principe fondamentaux

3.1. Mesures garantissant la proportionnalité et la nécessité du traitement

3.1.1. Finalités

Finalités	Légitimité
-----------	------------

Protection des bâtiments et installations publics et de leurs abords	Cette finalité est prévue par l'article L. 251-2 (1°) du Code de la sécurité intérieure (CSI). Elle est justifiée par la nécessité de surveiller des sites comme la Mairie, le centre technique, la salle polyvalente et le cinéma pour prévenir les dégradations et les intrusions.
Secours aux personnes et défense contre l'incendie	Correspondant à la finalité "Protection Incendie/Accidents" déclarée, cet objectif est prévu par l'article L. 251-2 (8°) du CSI. Il s'inscrit dans la mission générale de sécurité civile de la commune.
Prévention d'actes de terrorisme	Cette finalité est prévue par l'article L. 251-2 (6°) du CSI. Elle justifie une surveillance des lieux publics et des rassemblements de personnes pour anticiper et prévenir les menaces graves à la sécurité publique.
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	Prévue par l'article L. 251-2 (5°) du CSI, cette finalité inclut la "Prévention du trafic de stupéfiants" déclarée par la commune. Elle vise également à lutter contre les vols, les dégradations de biens et les rodéos urbains dans les zones identifiées comme sensibles.
Constatation des infractions aux règles de la circulation	Cette finalité est prévue par l'article L. 251-2 (4°) du CSI. Le système est utilisé pour prévenir et constater les infractions routières, contribuant ainsi à la sécurité sur la voie publique.
Prévention et constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets	Prévue par l'article L. 251-2 (11°) du CSI, cette finalité répond à la problématique concrète des "Dépôts sauvages" identifiée par la commune. Les caméras implantées au sein de l'espace public doivent permettre de dissuader et identifier les auteurs de ces incivilités.

[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 et 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 E 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.	<p>Le principe de minimisation est appliqué à travers plusieurs mesures techniques et organisationnelles :</p> <ul style="list-style-type: none"> - Pertinence de l'implantation : Chaque caméra est positionnée pour répondre à une finalité précise et documentée. Par exemple, la caméra C7 surveille spécifiquement les abords de l'école primaire et du gymnase, en lien avec la lutte contre les trafics de stupéfiants (ces abords étant connus comme points de deal la nuit), et les deux caméras C6 sont implantées pour surveiller la place centrale de la commune, où se situe la mairie, lieu récurrent de troubles nocturnes de l'ordre public (nuisances sonores, rodéos, ...) et de dégradations fréquentes. - Contrôle du champ de vision : Les caméras sont orientées de manière à ne pas visualiser l'intérieur des habitations ni, de façon spécifique, leurs entrées, conformément à l'article L. 251-3 du Code de la sécurité intérieure. Des procédés de masquage permanent ("floutage") doivent être mis en œuvre pour toutes les zones privées qui apparaîtraient inévitablement dans le champ et notamment pour masquer l'enceinte de la cour de l'école (caméra C7), en premier plan de cette implantation.
Jour et plages horaires d'enregistrement.	<ul style="list-style-type: none"> - Adaptation technologique : La Commune privilégie la pose de caméras multi-objectifs qui offrent une vision large et fixe, limitant ainsi les risques de surveillance ciblée et abusive. - Absence de son : Le système ne capte que les images, à l'exclusion des sons, ce qui limite la collecte de données aux seules informations visuelles pertinentes.
	<p>L'enregistrement est effectué en continu (24h/24, 7j/7). Cette modalité est justifiée par la nécessité de pouvoir constater des infractions et des incidents à tout moment, y compris en dehors des heures d'ouverture des services municipaux.</p>

Lieu où ont été collectées les données.	La collecte du lieu (identifiants de la caméra) est indispensable pour contextualiser les images enregistrées et est donc limitée à cette seule nécessité opérationnelle.
---	---

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
Format et fréquence des images	Le format et la fréquence des images sont conformes à l'arrêté du 3 août 2007 définissant les normes techniques des systèmes de vidéoprotection. La résolution des caméras (allant jusqu'à 5 Mégapixels pour certains modèles) et la fréquence d'enregistrement (au minimum 12 images par seconde pour les systèmes des autorités publiques) sont adaptées pour permettre une exploitation efficace des images au regard des finalités poursuivies (ex : identification de personnes, constatation d'infractions).

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
------------------	-----------------------	---	--

<p>Images captées</p> <p>Jour et plages horaires d'enregistrement</p> <p>Lieu où ont été collectées les données</p>	<p>La durée de conservation est fixée à 15 jours, conformément à la déclaration en préfecture.</p> <p>Cette durée est fixée par l'arrêté préfectoral dans la limite maximale d'un mois, conformément à l'article L. 252-3 du CSI.</p> <p>Les données sont collectées et stockées dans un serveur au sous-sol de la Mairie au 1 Place Raymond Poincaré</p>	<p>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.</p>	<p>Hormis le cas où ils sont utilisés dans le cadre d'une procédure judiciaire, administrative ou disciplinaire, les enregistrements sont automatiquement effacés.</p>
---	---	--	--

3.1.6. Axe d'amélioration

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorabile	Si améliorabile, mesures prévues dans le plan d'action
<p>Finalités : déterminées, explicites et légitimes.</p> <p>Les finalités des traitements sont expressément définies à l'article L. 251-2 CSI.</p>	Acceptable	
<p>Fondement : licéité du traitement</p>	Acceptable	
<p>Minimisation des données : adéquates, pertinentes et limitées.</p>	Acceptable	Une revue systématique du champ de vision des caméras est nécessaire pour s'assurer de l'absence de visualisation des zones privatives et mettre en œuvre des masques de confidentialité si besoin.
<p>Qualité des données : exactes et tenues à jour.</p>	Acceptable	
<p>Durée de conservation : limitée à une durée maximale de trente jours dans le cas de données à caractère personnel.</p>	Acceptable	

3.2. Evaluation 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 et à l'article 104 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. L'information du public est assurée par un double niveau : Premier niveau : 6 panonceaux d'information sont installés aux entrées de la ville (Avenue de Verdun, Route de Villécloye, Rue du Lieutenant Bourguignon, Route de Sedan, Route de Thonne les Prés et Rue Albert 1er). Ces panonceaux comportent un pictogramme de caméra et les informations essentielles : finalités, durée de conservation (15 jours), modalités d'accès aux images et droit de réclamation auprès de la CNIL. Second niveau : Une information complète, incluant toutes les mentions requises par l'article 13 du RGPD, doit être accessible via une page dédiée sur le site internet de la commune (www.montmedy.fr)
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. L'information est accessible en permanence via les panonceaux sur les lieux concernés et sera détaillée sur une page dédiée sur le site internet de la commune (www.montmedy.fr)
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. Les panonceaux utilisent un pictogramme clair et un texte concis pour une compréhension immédiate par le public.

Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)	L'information du responsable de traitement est délivrée sur les lieux d'installation des caméras à l'aide d'affiches ou de panneaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié. Les finalités principales sont listées sur les panneaux d'information : Protection des bâtiments et installations publics et de leurs abords, Prévention des atteintes à la sécurité des personnes et des biens dans les lieux particulièrement exposés à des risques d'agression et de vol ou de trafic de stupéfiants, Prévention des actes de terrorisme.
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 panneaux comportant un pictogramme représentant une caméra ainsi que par tout moyen approprié. Le panneau informe explicitement les personnes de leur droit d'accès aux images les concernant et de la possibilité d'introduire une réclamation auprès de la CNIL.
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation	Cette information technique détaillée (stockage sur serveur local dans un local sécurisé) figurera sur la page dédiée sur le site internet de la commune (www.montmedy.fr)
Modalités de contact du responsable de traitement (identité et coordonnées) pour les questions de confidentialité	Les coordonnées du responsable de traitement sont l'adresse mail suivante : dgs@montmedy.fr Le Délégué à la protection des données (DPD) du responsable de traitement peut également être contacté au courriel suivant dpo.informatique@cdg55.fr .
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité	Toute modification substantielle du traitement (ajout de caméras, changement de finalité) entraînera une mise à jour des supports d'information et, si nécessaire, une nouvelle déclaration en préfecture.

[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 15 du règlement (UE) 2016/679 du 27 avril 2016 s'exerce directement auprès du responsable de traitement.

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.

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

Le droit de rectification prévu à l'article 16 du règlement (UE) 2016/679 du 27 avril 2016 s'exerce 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 par l'article 106 de la loi n° 78-17 du 6 janvier 1978 ainsi que par l'article 18 du règlement (UE) 2016/679 du 27 avril 2016, s'exerce directement auprès du responsable du traitement. Toutefois, lorsque le traitement relève du titre IV de la loi n° 78-17 du 6 janvier 1978, ce droit n'est pas applicable. Dans notre cas, le droit à la limitation entrant dans ce cadre, il ne trouve donc pas à s'appliquer.

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

3.2.5. Mesures pour la sous-traitance

Nom du sous-traitant	Objet du contrat	Référence du contrat	Conformité
INEO INFRACOM	Fourniture, mise en service et maintenance curative du serveur d'enregistrement vidéo et des caméras.	Contrat de maintenance à terme de la garantie	Ce contrat formalise la maintenance du cœur du système (serveur), ce qui constitue une mesure positive pour la fiabilité et la sécurité de l'exploitation. Il inclut des engagements sur les délais d'intervention en cas de panne. Par ailleurs, conformément aux exigences liées à la certification APSAD, le contrat prévoit également la maintenance des caméras elles-mêmes.

3.2.7. Mesures pour transfert de données en dehors de l'Union européenne **NON CONCERNE**

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
- A 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 : Non applicable	
Exercice des droits à la limitation du traitement et d'opposition	Droit d'opposition : Non applicable Droit à la limitation : Non applicable	

[Sous-traitance : identifiée et contractualisée]

Acceptable

4. Etude des risques liés à la sécurité des données

4.1. Evaluation 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 générales de sécurité

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorabile	Si améliorabile, 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 à 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	Le serveur utilise un chiffrement AES 256 bits pour les enregistrements vidéo. Les clés de chiffrement sont générées et stockées localement, accessibles uniquement par l'administrateur système. Les extractions de données sont journalisées.
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	Le serveur est physiquement isolé du réseau Internet. Il est connecté uniquement au réseau interne sécurisé de la mairie via VLAN dédié.

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	Le local serveur est sécurisé par code. Accès limité aux agents habilités.
Contrôle des accès logiques	Il n'est possible d'accéder aux données qu'après une authentification.	Acceptable	Accès via identifiants individuels avec segmentation des profils (administrateur, superviseur, visualiseur). Journalisation des connexions activée.
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	Les mises à jour sont planifiées mensuellement par l'administrateur. Les agents sont formés à l'utilisation du système.
Pseudonymisation	Non applicable. La pseudonymisation n'est pas une mesure pertinente pour des données vidéo brutes dont la finalité est l'identification.		Non applicable
Archivage	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 organisationnelles

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Si améliorable, mesures prévues dans le plan d'action
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	Les mises à jour sont planifiées mensuellement par l'administrateur. Les agents sont formés à l'utilisation du système.

Lutte contre les logiciels malveillants	<p>La lutte contre les logiciels malveillants est garantie par le fait que le serveur où les images sont enregistrées est hors réseau.</p> <p>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.</p> <p>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.</p>	Acceptable	Antivirus installé sur les postes de supervision, mis à jour automatiquement. Le serveur est hors réseau Internet, réduisant les risques.
Mot de passe	<p>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.</p> <p>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</p>	Acceptable	Mots de passe complexes (12 caractères minimum, majuscules, minuscules, chiffres, caractères spéciaux), renouvelés tous les 90 jours. Conformité CNIL 2022-100.
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 images collectées.	Acceptable	Aucun accès Internet depuis le serveur. Les postes de supervision sont cloisonnés et filtrés.
Sauvegarde des logs	La journalisation des accès et des consultations est une fonctionnalité requise. Les journaux doivent être conservés pour une durée maximale de 3 ans.	Acceptable	Les logs sont sauvegardés automatiquement. Accès restreint aux administrateurs.
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	Maintenance assurée par INEO INFRACOM. Aucun accès aux contenus vidéo.
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	VLAN dédié, firewall configuré avec règles strictes. Logs des connexions conservés 3 ans.

Surveillance	Contrôle régulier par le responsable de la journalisation, de l'accès aux postes informatiques et de leur utilisation	Acceptable	Contrôle des accès et des journaux par le responsable de traitement.
Sécurité des matériels	Le serveur de stockage des images est placé dans un local dédié sous contrôle d'accès physique.	Acceptable	Serveur dans local ventilé, sécurisé, non accessible au public. Contrôle d'accès physique.
Organisation	L'organisation est définie par le responsable de traitement. Les rôles sont les suivants : - chef de service ; - délégué à la protection des données ;	Acceptable	
Politique (gestion des règles)	Formation, charte informatique, règles de gestion des habilitations des administrateur, agents habilités et leurs profils	Acceptable	Charte informatique signée, profils différenciés (accès en direct / différé), formation annuelle : Mise à jour de la charte et renforcement des formations.
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.	Améliorable	Journalisation des connexions
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	Améliorable	Référent sûreté impliqué.
Gestion des incidents et des violations de données	Les rôles et responsabilités des parties prenantes ainsi que les procédures de remontées d'informations et de 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.	Acceptable	Procédure de remontée d'incident, journalisation des défaillances.
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	Agents sélectionnés (déclaration préfectorale), formés et sensibilisés à la vidéoprotection. Accès restreint.

Relations avec les tiers	Les relations avec les tiers se limitent à la transmission des images aux forces de l'ordre (Police, Gendarmerie) sur réquisition judiciaire, conformément au cadre légal.	Acceptable	Transmission des images uniquement sur réquisition judiciaire.
Supervision	Le responsable de traitement veille par des contrôles aux connexions afin de détecter des accès anormaux mais aussi aux éventuels incidents.	Améliorable	Supervision mensuelle des connexions et des incidents par le responsable de traitement.

PROJET

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	<p>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</p> <p>Piratage du flux de transmission des données entre les caméras de vidéoprotection et les salles de commandement Vol du matériel par un tiers</p>	<p>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</p>	<p>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</p>	<p>Respect stricte des règles de confidentialité, des accès aux locaux, des mots de passe avec mesures de contrôle des logs.</p>	<p>Importante</p> <p>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.</p>	<p>Limitée</p>

<p>Modification non désirées de données</p>	<p>Accès physique à la caméra, à la salle de commandement ou à la solution de stockage</p>	<p>Modification des informations collectées ne permettant plus d'utiliser celles-ci à l'appui d'une procédure.</p>	<p>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</p>	<p>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</p>	<p>Importante mais une modification des images captées serait nécessairement détectée car portant atteinte à l'intégrité de la donnée.</p>	<p>Limitée</p>
--	--	--	---	---	--	----------------

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

5. Validation de l'analyse d'impact

5.1. Eléments utiles à la validation

5.1.1. Synthèse relative à la conformité

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	La formalisation d'une Charte d'Utilisation et la revue périodique des journaux de consultation visent à prévenir tout détournement de finalité




Minimisation des données : adéquates, pertinentes et limitées	Acceptable	Une revue systématique du champ de vision des caméras est nécessaire pour s'assurer de l'absence de visualisation des zones privées et mettre en œuvre des masques de confidentialité si besoin
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	La mise à jour des panneaux d'information et la création d'une page dédiée sur le site internet de la Commune sont prévues pour assurer une information complète et conforme
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 : non applicable	
Exercice des droits à la limitation du traitement et d'opposition	Droit d'opposition : non applicable Droit à la limitation : non applicable	
Sous-traitance : identifiée et contractualisée	Améliorable	Ajouter des mentions RGPD dans le contrat de sous-traitance visant à limiter les actions et l'accès à celui-ci




5.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données

Finalités	Evaluation
Mesures portant spécifiquement sur les données du traitement	
Chiffrement	Acceptable
Pseudonymisation	Non applicable
Cloisonnement des données (par rapport au reste du système d'information)	Acceptable
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	Améliorable
Politique (gestion des règles)	Acceptable
Gestion des risques	Acceptable
Gestion des projets	Améliorable
Gestion des incidents et des violations de données	Acceptable
Gestion des personnels	Acceptable
Relations avec les tiers	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				

5.2 Validation formelle

Avis du délégué à la protection des données :

Le Délégué à la Protection des Données atteste avoir pris connaissance de la présente Analyse d'Impact relative à la Protection des Données (AIPD) portant sur la mise en œuvre du dispositif de vidéoprotection.

Au regard des mesures techniques et organisationnelles décrites, il estime que le niveau de risque résiduel pour les droits et libertés des personnes concernées est suffisamment faible et acceptable.

Validation par le responsable de traitement :

Le Maire, en tant que 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	<ul style="list-style-type: none">• Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté.	<ul style="list-style-type: none">• Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle)• Maux de tête passagers	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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)

<p>2. Limitée</p>	<ul style="list-style-type: none"> • Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • 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 un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) • Profilage imprécis ou abusif 	<ul style="list-style-type: none"> • Refus de continuer à utiliser les systèmes d'information (<i>whistleblowing</i>, 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
-------------------	---	--	---	---

<p>3. Importante</p>	<ul style="list-style-type: none"> Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 / <i>phishing</i>) Bloqué à l'étranger Perte de données clientèle 	<ul style="list-style-type: none"> 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 - <i>Cyberbullying</i> et harcèlement moral
<p>4. Maximale</p>	<ul style="list-style-type: none"> Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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) 	<ul style="list-style-type: none"> 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)

<ul style="list-style-type: none"> Niveaux de vraisemblance 	<ul style="list-style-type: none"> Description générique du niveau de vraisemblance d'une menace donnée
1. Négligeable	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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).