



**MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER**

*Liberté
Égalité
Fraternité*

Paris, le **20 MARS 2024**

Le ministre de l'Intérieur et des Outre-mer

à

**Monsieur le préfet de police
Mesdames et Messieurs les préfets de département
Monsieur le préfet de police des Bouches-du-Rhône**

Référence	NOR : IOMD2405307J
Date de signature	20 mars 2024
Emetteur	Ministre de l'Intérieur et des Outre-mer
Objet	Mise en conformité du régime de la vidéoprotection avec le droit européen relatif à la protection des données
Commande	Des précisions sont apportées quant à la mise en conformité du régime de la vidéoprotection avec le droit relatif à la protection des données opérée par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions
Action(s) à réaliser	Veiller à l'application des précisions contenues dans la présente circulaire
Echéance	Effet immédiat
Contact utile	Direction des libertés publiques et des affaires juridiques – Sous-direction des libertés publiques – Bureau du droit des données et des nouvelles technologies Direction des entreprises et partenariats de sécurité et des armes
Nombre de pages et annexes	109 pages dont 5 annexes

Documents annexés :

1. Fiche 1-A : Tableau synthétique relatif aux règles issues de la loi ancienne restées inchangées avec la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 (JOP2024) et aux principales nouveautés apportées par cette loi
2. Fiche 1-B : Evolutions induites par la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions
3. Fiche 2 : Définition des systèmes de vidéoprotection

4. Fiche 3 : Les lieux d'installation des systèmes de vidéoprotection
5. Fiche 4 : Les personnes qui peuvent être autorisées à installer un système de vidéoprotection
6. Fiche 5 : La demande d'autorisation
7. Fiche 6 : Le rôle de la commission départementale de vidéoprotection
8. Fiche 7 : La décision préfectorale
9. Fiche 8 : Les contrôles et sanctions
10. Annexe 1 : Modèle d'AIPD « cadre » pour les autorités publiques
11. Annexe 2 : Modèle d'AIPD pour les autorités privées
12. Annexe 3 : Formulaire Cerfa n° 13810*03 - Déclaration simplifiée - Engagement de conformité
13. Annexe 4 : Formulaire CERFA n°13806*04 - Demande d'autorisation d'un système de vidéoprotection
14. Annexe 5 : Notice d'information relative au formulaire CERFA n° 13806*03 - Demande d'autorisation d'un système de vidéoprotection

Depuis la création de son cadre juridique par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, la vidéoprotection s'est largement développée comme un outil d'amélioration de la sécurité de nos concitoyens et apparaît désormais pleinement acceptée.

La vidéoprotection est un outil efficace, qui bénéficie par conséquent d'un effort budgétaire important du fonds interministériel de prévention de la délinquance et de la radicalisation (FIPDR) dont les crédits destinés à la vidéoprotection seront triplés au cours des cinq années à venir et viendront cofinancer les projets portés par les collectivités territoriales, notamment des audits des éventuelles failles de sécurité présentes dans les caméras déjà installées, comme l'indique le rapport annexé à la LOPMI promulguée le 24 janvier 2023.

A cet effort financier devait correspondre une mise à niveau juridique.

Il était en effet impératif de mettre en conformité le cadre légal de la vidéoprotection « fixe » avec le nouveau cadre juridique relatif à la protection des données à caractère personnel entré en vigueur en 2018, issu des règles du règlement général sur la protection des données (RGPD) et de la directive dite « *police-justice* », les dispositions relatives aux caméras mobiles (caméras-piétons, aéroportées, embarquées) ayant, quant à elles, déjà été récemment mises en conformité. Alors que la vidéoprotection était considérée par une jurisprudence européenne constante¹ comme un traitement de données à caractère personnel, la loi précitée de 1995 prévoyait plusieurs règles dérogatoires en matière de droit des personnes filmées et de droit de contrôle de la Commission nationale de l'informatique et des libertés (CNIL).

L'article 9 de la loi n° 2023-380 du 19 mai 2023 *relative aux jeux Olympiques et Paralympiques de 2023 et portant diverses autres dispositions*, complétée par le décret n° 2023-1102 du 27 novembre 2023², ont procédé à cette actualisation indispensable, en renforçant les obligations qui pèsent sur les responsables de systèmes de vidéoprotection et le contenu du dossier de demande d'autorisation, et en rendant pleinement effectifs les droits des personnes et les pouvoirs de contrôle et de sanction de la CNIL. Cette actualisation était en outre rendue nécessaire par la prochaine expérimentation de la vidéoprotection « *intelligente* », que la même loi précitée a autorisée, pour une mise en œuvre à compter des marchés de Noël 2023 et jusqu'au 31 mars 2025³.

Au terme de cette réforme, les préfets conservent un rôle central en matière de vidéoprotection :

- Vous demeurez décisionnaires pour **autoriser ou rejeter les demandes d'installation de systèmes de vidéoprotection**. Le dossier de demande soumis à l'instruction de vos services sera enrichi, en particulier du fait de la nécessité pour les responsables de traitement dans certains cas d'y adjoindre une analyse d'impact relative à la protection des données (AIPD) et un engagement de conformité à la CNIL (cf. fiche n° 1-B) ;
- vous pouvez faire procéder par les services de police ou de gendarmerie à des **contrôles de vérification** des prescriptions émises dans les autorisations préfectorales ;
- vos services continuent à assurer **le secrétariat de la commission départementale de vidéoprotection**, cette dernière pouvant diligenter des contrôles de sa propre

¹ CJUE, 11 décembre 2014, C-212/13.

² Décret n° 2023-1102 du 27 novembre 2023 portant application des articles L. 251-1 et suivants du code de la sécurité intérieure et relatif à la mise en œuvre des traitements de données à caractère personnel provenant de systèmes de vidéoprotection et des caméras installées sur des aéronefs.

³ Article 10 de la loi n° 2023-380 du 19 mai 2023 et décret n° 2023-828 du 30 août 2023.

initiative ou sur saisine, et vous proposer le cas échéant la suspension ou la suppression d'un système lorsqu'elle constate qu'il n'est pas autorisé ou qu'il en est fait un usage anormal ou non conforme à son autorisation ;

- lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, vous conservez la faculté de **délivrer aux autorités publiques compétentes ou aux personnes morales concernées une autorisation provisoire** d'installation d'un système de vidéoprotection sans avis préalable de la commission départementale de vidéoprotection ;
- vous pouvez enfin **demander à une commune la mise en œuvre de systèmes de vidéoprotection** aux fins de prévention d'actes de terrorisme ou de protection des abords des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ou de protection des intérêts fondamentaux de la Nation.

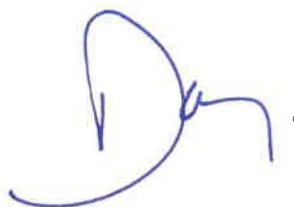
Dans la mesure où la loi précitée laisse inchangé le régime d'autorisation des systèmes de vidéoprotection, vous n'avez pas besoin de prendre de nouvelles autorisations pour les systèmes déjà déployés et autorisés dans votre département.

Les fiches annexées à la présente circulaire, qui abroge et remplace les circulaires des 12 mars 2009 et 14 septembre 2011, résument les évolutions induites par la loi du 19 mai 2023 précitée et précisent les modalités de mise en œuvre des systèmes de vidéoprotection.

Elles sont également accessibles sur l'intranet de la direction des libertés publiques et des affaires juridiques (DLPAJ), qui, régulièrement actualisé, doit constituer votre support d'information juridique privilégié (<https://intranet.dlpaj.minint.fr/>).

Concernant en particulier les systèmes de vidéoprotection des collectivités territoriales, vous pouvez vous référer à l'instruction du Gouvernement du 4 mars 2022 relative à la mise en œuvre des dispositions de la loi du 25 mai 2021 et portant sur l'acquisition, l'installation et l'entretien de dispositifs de vidéoprotection par les collectivités territoriales et leurs groupements ainsi que sur l'habilitation du personnel territorial procédant au visionnage, publiée au bulletin officiel du ministère de l'Intérieur du 11 mars 2022.

Vous veillerez à la bonne application de ces précisions par l'ensemble des services sous votre autorité et vous voudrez bien me tenir informé, sous le présent timbre, de toute difficulté d'application de la présente circulaire. Je compte sur vous pour exploiter le potentiel considérable de la vidéoprotection en veillant à la stricte application du droit qui l'encadre.



Gérald DARMANIN

Fiche n° 1-A : Tableau synthétique relatif aux règles issues de la loi ancienne restées inchangées avec la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 (JOP2024) et aux principales nouveautés apportées par cette loi nouvelle

	Règles juridiques actuelles restées inchangées	Principales nouveautés apportées par la nouvelle réglementation
Autorisation d'un système de vidéoprotection		
Instruction de la demande d'autorisation du système de vidéoprotection (Cf. fiches n° 5 et 7)	Les personnes autorisées à installer un système de vidéoprotection doivent constituer un dossier de demande d'autorisation comportant une liste de pièces (cf. fiche n° 5)	<p>Le dossier de demande ne contient plus:</p> <ul style="list-style-type: none"> - les consignes générales données aux personnels d'exploitation du système de vidéoprotection pour le fonctionnement de celui-ci et le traitement des images ; <p>Dans certaines circonstances, le dossier de demande comporte deux nouvelles pièces :</p> <ul style="list-style-type: none"> - une analyse d'impact relative à la protection des données (AIPD), pouvant remplacer certaines pièces du dossier ; - un engagement de conformité destiné à la CNIL. <p>Dans le cadre de sa mission consultative, la commission départementale de vidéoprotection (CDV) devra également examiner ces deux nouvelles pièces (cf. fiche n° 6 sur le rôle des CDV).</p>
Décision d'autorisation préfectorale (cf. fiche n° 7)	L'autorisation préfectorale prévoit toutes les précautions utiles (délai de conservation des images, mesures de sécurité, personnes pouvant accéder au visionnage des images et personnes pouvant en être destinataires, etc.) pour être conforme au cadre juridique applicable à la vidéoprotection.	La liste des personnes pouvant accéder au visionnage des images et des personnes pouvant en être destinataires a été clarifiée et précisée.
Modification des demandes d'autorisation d'un système de vidéoprotection (cf. fiche n° 7)	Lorsque le responsable de système souhaite apporter des modifications à un système, le préfet doit évaluer la nécessité de délivrer une nouvelle autorisation.	Pas de changement
Renouvellement des demandes d'autorisation d'un système de vidéoprotection (cf. fiche n° 7)	Lorsque l'autorisation arrive à expiration, le responsable de système doit demander le renouvellement de sa demande en déposant un nouveau dossier complet, qui devra être instruit par le préfet.	Pas de changement
Procédures particulières d'autorisation		
Prescription préfectorale de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)	Le préfet peut prescrire la mise en œuvre de systèmes de vidéoprotection aux fins de prévention d'actes de terrorisme ou en cas d'urgence et d'exposition particulière à un risque d'actes de terrorisme ou lorsque le préfet a été informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers.	Pas de changement

Autorisation provisoire de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)	Le préfet peut délivrer une autorisation provisoire d'installation d'un système de vidéoprotection, lorsque l'urgence et l'exposition particulière à un risque d'acte de terrorisme le requièrent ou lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers.	Pas de changement
Demande préfectorale de mise en œuvre d'un système de vidéoprotection (cf. fiche n° 7)	Le préfet peut demander à une commune la mise en œuvre de systèmes de vidéoprotection, aux fins de prévention d'actes de terrorisme, de protection des abords de certains établissements, installations ou ouvrages ou de protection des intérêts fondamentaux de la Nation.	Pas de changement
Garanties et droits accordés aux personnes filmées par un système de vidéoprotection		
Droits des personnes concernées (cf. fiche n° 1-B)	Le préfet doit vérifier les modalités de l'information du public et celles de leur droit d'accès. Les personnes concernées sont informées de la mise en œuvre d'un système de vidéoprotection, par voie d'affiches ou de panneaux sur les lieux d'installation des caméras, comportant un pictogramme représentant une caméra et des informations permettant d'identifier le responsable du système.	La liste des informations à mettre à la disposition du public a été substantiellement enrichie. Il doit désormais être fait, par exemple, mention de la durée de conservation des données, des destinataires ou catégories de destinataires des données ou encore de nouveaux droits (il a été ajouté, en complément du droit d'accès, un droit de rectification, d'effacement et à la limitation des données). Cette liste de mentions d'information diffère en fonction du régime juridique applicable au système de vidéoprotection. (cf. fiche n° 1-B).
Contrôles et sanctions		
Contrôles (Cf. fiche n° 8)	La CDV peut exercer des contrôles visant à vérifier la conformité du système de vidéoprotection à son autorisation et proposer au préfet des sanctions en cas de non-respect des conditions d'autorisation du système. Le préfet peut faire procéder, par les services de police ou de gendarmerie, à des contrôles de vérification des prescriptions émises dans les autorisations préfectorales, sur l'existence de systèmes non autorisés et sur la conformité du système aux normes techniques.	Pas de changement
Sanctions (Cf. fiche n° 8)	A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la CDV peut proposer au préfet la suspension de l'autorisation d'installation ou le retrait de l'autorisation d'installation. Le préfet peut également demander la fermeture administrative de l'établissement ou enjoindre de démonter le système de vidéoprotection. La mise en œuvre d'un système de vidéoprotection sans autorisation préalable constitue un délit.	Pas de changement

Fiche n° 1-B : présentation des modifications du régime juridique de la vidéoprotection par l'article 9 de la loi n° 2023-380 du 19 mai 2023 relative aux Jeux olympiques et Paralympiques de 2024 et portant diverses autres dispositions

I. L'application des règles relatives à la protection des données aux systèmes de vidéoprotection

Alors que le code de la sécurité intérieure ne prévoyait l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (dite « informatique et libertés ») qu'aux enregistrements de vidéoprotection utilisés dans des fichiers structurés selon des critères permettant d'identifier les personnes, l'article 9 de la loi du 19 mai 2023 soumet l'ensemble de la vidéoprotection aux dispositions de cette loi.

Dès lors, les responsables des systèmes de vidéoprotection doivent se mettre en conformité avec la loi « informatique et libertés » en se faisant accompagner, le cas échéant, par leur délégué à la protection des données.

Le rôle des préfets est distinct de celui des responsables des systèmes de vidéoprotection : il consiste, lors de l'autorisation des systèmes, à veiller à l'effectivité de cette mise en conformité, en contrôlant en particulier la production par les responsables de systèmes des pièces nécessaires.

A. La détermination du régime juridique applicable

Les traitements de données à caractère personnel issus des systèmes de vidéoprotection peuvent, selon leur finalité et la qualité du responsable du système, relever de différents régimes de protection des données à caractère personnel prévus par la réglementation européenne et par la loi « informatique et libertés ».

La détermination du régime juridique adéquat est essentielle, dans la mesure où le champ dont relève le traitement entraîne des conséquences notables à plusieurs niveaux, notamment quant aux droits des personnes concernées et aux obligations imposées aux responsables de traitement.

Il appartient aux responsables de système de vidéoprotection de déterminer le régime applicable à leur système. Les développements ci-dessous présentent les différents régimes susceptibles de s'appliquer.

1. Le titre IV de la loi « informatique et libertés » : les systèmes de vidéoprotection qui intéressent la sûreté de l'Etat et la défense

Ce régime juridique est applicable aux traitements qui sont mis en œuvre pour le compte de l'Etat et qui intéressent la sûreté de l'Etat et la défense.

Concrètement, ce régime juridique ne concerne que les systèmes de vidéoprotection mis en œuvre par le ministère des armées pour assurer la sauvegarde des installations utiles à la défense nationale (le 2° de l'article L. 251-2 du code de la sécurité intérieure).

2. Le titre III de la loi « informatique et libertés » (issu de la directive dite « police-justice ») : les systèmes de vidéoprotection mis en œuvre à des fins « police-justice »

Les systèmes de vidéoprotection peuvent relever de ce régime lorsqu'ils remplissent deux critères cumulatifs prévus à l'article 87 de la loi « informatique et libertés » :

1. Ils poursuivent des **finalités 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**. Une analyse au cas par cas, au regard des circonstances particulières, doit être menée par le responsable du système pour déterminer si ce dernier poursuit une de ces finalités.
2. Ils sont mis en œuvre par une **autorité compétente pour ces fins** : par « autorité compétente », il faut entendre toute autorité publique ou tout autre organisme ou entité à qui a été confié, aux fins précitées, l'exercice de l'autorité publique et des prérogatives de puissance publique. Peu de services sont des autorités compétentes au sens de la loi « informatique et libertés ». C'est le cas par exemple des services de la police nationale et de la gendarmerie nationale ou encore d'un maire. A l'inverse, ne sont par exemple pas des « autorités compétentes » le responsable d'un établissement scolaire ou hospitalier, le responsable d'un service d'incendie ou de secours ou un commerçant.

Concrètement, ce régime juridique s'applique essentiellement aux systèmes de vidéoprotection mis en œuvre par les services de la police nationale et de la gendarmerie nationale et par les communes.

3. Le RGPD et le titre II de la loi « informatique et libertés » : les autres systèmes de vidéoprotection

Les systèmes de vidéoprotection peuvent relever de ce régime juridique lorsqu'ils n'entrent ni dans le champ du titre III, ni dans celui du titre IV de la loi « informatique et libertés », soit parce que leur finalité n'intéresse pas la sûreté de l'Etat ou la défense ou la « police-justice », soit parce que le responsable de ces traitements n'est pas une autorité compétente au sens de cette loi.

Sauf si elles se sont vues confier l'exercice de l'autorité publique et des prérogatives de puissance publique à 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 (exemple : les fédérations sportives agréées aux fins de sécurisation des manifestations sportives), les systèmes de vidéoprotection mis en œuvre par des personnes privées relèvent par principe du RGPD et du titre II de la loi « informatique et libertés ».

Concrètement, ce régime juridique s'applique « par défaut » lorsque les deux régimes spécifiques prévus par le titre IV et le titre III de la loi « informatique et libertés » ne s'appliquent pas. Il concerne donc la majeure partie des systèmes de vidéoprotection mis en œuvre.

4. L'application d'un régime mixte en cas de finalités multiples

La mise en œuvre de systèmes de vidéoprotection pour plusieurs finalités peut conduire à l'application simultanée de plusieurs régimes de protection des données (titre IV, titre III et/ou titre II de la loi « informatique et libertés »).

Dans ce cas, le responsable du système de vidéoprotection devra distinguer les régimes applicables en fonction des finalités de son système.

Personnes	Finalités	Titre pouvant être applicable
Autorités publiques	La protection des bâtiments et installations publics et de leurs abords	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne ⁴ : Titre II
	La sauvegarde des installations utiles à la défense nationale	Titre IV
	La régulation des flux de transport	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La constatation des infractions aux règles de la circulation	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	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	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention d'actes de terrorisme	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention des risques naturels ou technologiques	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Le secours aux personnes et la défense contre l'incendie	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La sécurité des installations accueillant du public dans les parcs d'attraction	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
	Sécurité des personnes et des biens dans les lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol	Autorité compétente au sens de la directive : Titre III Autre autorité ou personne : Titre II
	Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme	Autorité compétente au sens de la loi informatique et libertés : Titre III Autre autorité ou personne : Titre II
Personnes morales de droit privé, y compris les commerçants	Protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme	Titre II
	Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol	Titre II
	Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme	Titre II
Commerçants uniquement	Protection des abords immédiats de leurs bâtiments et installations dans les lieux particulièrement exposés à des risques d'agression ou de vol	Titre II

⁴ Signifie que le responsable du système n'est pas une autorité compétente aux 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

B. La rédaction d'une analyse d'impact relative à la protection des données (AIPD)

En application du RGPD et de la loi « informatique et libertés », la mise en œuvre de systèmes de vidéoprotection peut être subordonnée à la réalisation d'une analyse d'impact relative à la protection des données (AIPD)⁵.

L'AIPD permet de démontrer la conformité du système de vidéoprotection envisagé au regard de la réglementation applicable en matière de protection des données à caractère personnel. Elle vise à présenter le traitement (sa nature, sa portée, son contexte, ses finalités et ses enjeux), à en évaluer la nécessité ainsi que la proportionnalité et à aider le responsable du traitement à gérer les risques pouvant affecter les droits et libertés des personnes physiques concernées en les évaluant et en déterminant les mesures nécessaires pour y faire face.

Le cas échéant, il appartient à la personne ou au service qui demande l'autorisation d'installer un système de vidéoprotection d'élaborer cette AIPD. Si une AIPD est réalisée, elle a vocation à remplacer certaines pièces du dossier de demande d'autorisation (cf. fiche n°5).

1. Situations dans lesquelles la rédaction d'une AIPD est obligatoire

La rédaction d'une AIPD est obligatoire dans l'hypothèse où le système de vidéoprotection est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Cette obligation n'est pas applicable en matière de défense nationale.

Dans cette optique, la CNIL a établi une liste de **neuf critères** permettant de déterminer si un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes :

- Evaluation ou notation (« *scoring* ») (y compris les activités de profilage et de prédiction) ;
- Prise de décision automatisée avec effet juridique ou effet similaire significatif ;
- Surveillance systématique ;
- Collecte de données sensibles ou données à caractère hautement personnel ;
- Données traitées à grande échelle ;
- Croisement ou combinaison d'ensembles de données ;
- Données concernant des personnes vulnérables (personnes âgées, enfants, etc.) ;
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles ;
- Traitements en eux-mêmes qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

Dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD. D'une manière générale, plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD. Néanmoins, dans certains cas, le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD.

⁵ Pour plus d'informations sur l'AIPD, voir le site de la CNIL : <https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd>

Au regard des éléments caractéristiques des systèmes de vidéoprotection, les critères de « la surveillance systématique » et de la « collecte de données personnelles à large échelle » sont susceptibles d'être remplis.

Cette AIPD devra être jointe à la demande d'autorisation du système.

2. Modèles d'AIPD

Afin de faciliter le travail d'analyse, il est proposé en annexe de cette circulaire deux modèles d'AIPD qui pourront être communiqués au demandeur :

- Pour les autorités publiques : il s'agit de l'AIPD « cadre » présentée à la CNIL lors de l'élaboration du décret n° 2023-1102 du 27 novembre 2023 précité. Elle a vocation à constituer le socle de référence des garanties minimales à mettre en œuvre destinées à préserver les droits et libertés et à assurer le fonctionnement du système en conformité avec les exigences de la loi « informatique et libertés ». Si cette trame est utilisée par le responsable du système de vidéoprotection, ce dernier doit la compléter par les éléments nécessités par les circonstances locales (champs surlignés en jaune).
- Pour les personnes privées : il s'agit d'une proposition de modèle pré-rempli avec les éléments communs à l'ensemble des systèmes de vidéoprotection.

C. La rédaction d'un engagement de conformité

Lorsqu'un traitement répond à une même finalité, porte sur des catégories de données identiques et a les mêmes destinataires ou catégories de destinataires et qu'il fait ainsi l'objet d'un acte réglementaire unique au sens du IV de l'article 31 de la loi « informatique et libertés », chaque responsable de traitement adresse à la CNIL un engagement de conformité de celui-ci à la description figurant dans cet acte.

L'article R. 253-7 du code de la sécurité intérieure subordonne ainsi la mise en œuvre des systèmes de vidéoprotection à l'envoi préalable de cet engagement de conformité et prévoit que certains responsables de systèmes de vidéoprotection doivent adresser à la CNIL un engagement de conformité.

L'article R. 253-7 du code de la sécurité intérieure subordonne la mise en œuvre d'un système de vidéoprotection par une autorité publique à l'envoi préalable à la CNIL d'un engagement de conformité aux dispositions réglementaires.

Cette formalité ne s'impose qu'aux autorités publiques, donc notamment aux services de l'Etat centraux et déconcentrés ainsi qu'aux collectivités territoriales.

L'engagement de conformité est joint au dossier de demande d'autorisation auprès du préfet mais ne doit être envoyé à la CNIL qu'après autorisation du système de vidéoprotection par ce dernier.

Le formulaire d'engagement de conformité (Cerfa n° 13810*03) figure en annexe. À la rubrique 2, la case « Acte réglementaire unique » devra être cochée et complétée par le « N° de référence », en l'occurrence RU-74.

L'engagement de conformité peut également être réalisé en ligne, sur le site de la CNIL à la rubrique « Effectuer une déclaration de conformité » : <https://www.cnil.fr/fr/declarer-un-fichier>

II. Les droits des personnes concernées par un système de vidéoprotection

A. L'information des personnes concernées

Par principe, le public doit être informé par la personne ou le service responsable de la mise en œuvre d'un système de vidéoprotection.

Les informations à mettre à la disposition du public diffèrent en fonction du régime applicable au système de vidéoprotection (cf. I). Il s'agit des informations mentionnées :

- Dans la section 2 du chapitre III du RGPD s'agissant des systèmes relevant de ce règlement et du titre II de la loi « informatique et libertés » ;
- A l'article 104 de la loi « informatique et libertés » s'agissant des systèmes relevant du titre III de cette loi
- A l'article 116 de la loi « informatique et libertés » s'agissant des systèmes relevant du titre IV de cette loi

Le tableau ci-après détaille les informations devant être obligatoirement fournies aux personnes concernées par le traitement en fonction du régime juridique applicable au traitement.

RGPD et titre II de la loi « informatique et libertés » Article 13 du RGPD	Titre III de la loi « informatique et libertés » Article 104 de la loi « informatique et libertés »	Titre IV de la loi « informatique et libertés » Article 116 de la loi « informatique et libertés »
L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement	L'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement	L'identité du responsable du traitement et, le cas échéant, de celle de son représentant
Le cas échéant, les coordonnées du délégué à la protection des données	Le cas échéant, les coordonnées du délégué à la protection des données	
Les finalités du traitement auquel sont destinées les données à caractère personnel	Les finalités poursuivies par le traitement auquel les données sont destinées	La finalité poursuivie par le traitement auquel les données sont destinées
La base juridique du traitement, soit les articles L. 251-2 et suivants du code de la sécurité intérieure	La base juridique du traitement, soit les articles L. 251-2 et suivants du code de la sécurité intérieure	
Le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel	Le cas échéant, les catégories de destinataires des données à caractère personnel, y compris ceux établis dans les Etats n'appartenant pas à l'Union européenne ou au sein d'organisations internationales	Les destinataires ou catégories de destinataires des données
Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne ou d'une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission européenne, ou la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition		Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne
La durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	La durée de conservation des données à caractère personnel ou, à défaut lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	La durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée
Lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f) du RGPD, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers		
L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée	L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée	Les droits que la personne concernée tient des dispositions des articles 117 à 120 de la loi « informatique et libertés »
Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés	Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission	

D'autres informations additionnelles peuvent être adressées aux personnes concernées par le responsable du système, conformément au II de l'article 104 de la loi « informatique et libertés ».

En application de l'article R. 253-6 du code de la sécurité intérieure, cette information doit être délivrée par voie d'affiches ou de panonceaux sur les lieux d'installation des caméras, comportant un pictogramme représentant une caméra.

Par exception, un double niveau d'information peut être délivré si le responsable le souhaite. Dans ce cas :

- les affiches ou panonceaux doivent mentionner au minimum l'identité du responsable du système, les finalités poursuivies par le traitement et les droits des personnes concernées ;
- les autres informations exigées par le RGPD ou la loi « informatique et libertés » peuvent être communiquées par tout autre moyen, par exemple par le biais d'un renvoi vers un site internet.

En tout état de cause, les modalités d'information (format, nombre et localisation des affiches ou panonceaux) doivent être adaptées aux circonstances dans lesquelles elles sont déployées, notamment à la situation des lieux et établissements.

Les modalités d'information font partie du dossier de demande. **Le préfet doit donc, à ce titre, les contrôler.**

B. Les droits d'accès, de rectification, à la limitation, d'effacement des données et d'opposition

Dans leur demande d'autorisation, les responsables de systèmes doivent détailler les modalités d'information du public, et, à ce titre, la façon dont les personnes pourront exercer leurs droits auprès d'eux.

Il appartient au préfet de vérifier que l'information des personnes précise l'ensemble de leurs droits prévus par le RGPD et la loi. La personne ou le service à contacter pour exercer leur droit d'accès ainsi que ses coordonnées doivent être précisés dans le dossier de demande d'autorisation.

Avant l'entrée en vigueur de la loi du 19 mai 2023, le code de la sécurité intérieure ne conférait aux personnes que le droit d'obtenir un accès aux enregistrements qui les concernaient.

Ce droit est maintenu et permet aux personnes concernées de demander au responsable de traitement si des données les concernant ont ou n'ont pas été traitées et d'en obtenir l'accès. Cet accès, demandé par écrit ou sur place, se matérialise par un visionnage des images qui concernent la personne ou par la fourniture d'une copie de ces images, après y avoir appliqué un système de « floutage » permettant de protéger les droits des tiers.

L'article R. 253-6 du code de la sécurité intérieure prévoit que le responsable de système de vidéoprotection peut, pour garantir la sécurité nationale ou la protection contre les menaces pour la sécurité publique ou la prévention de telles menaces, restreindre le droit d'accès des personnes.

La mise en conformité du régime de la vidéoprotection avec le droit sur la protection des données entraîne en principe l'ouverture de nouveaux droits aux personnes⁶ :

- Droit à l'effacement : les personnes concernées peuvent demander au responsable de traitement d'effacer les données à caractère personnel les concernant dans les meilleurs délais. Lorsque le système de vidéoprotection relève du RGPD et du titre II de la loi « informatique et libertés » et qu'il est nécessaire pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, le droit à l'effacement ne s'applique pas ;
- Droit à la limitation du traitement : les personnes concernées peuvent demander au responsable de traitement d'arrêter, temporairement, d'utiliser certaines données.

L'article R. 253-6 du code de la sécurité intérieure prévoit que le droit d'opposition n'est pas applicable au traitement : les personnes concernées ne peuvent pas s'opposer au traitement de leurs données à caractère personnel.

Pour exercer leurs droits, les personnes concernées s'adressent directement au responsable du système de vidéoprotection.

III. La mise en conformité des systèmes de vidéoprotection existants

Dans la mesure où le décret n° 2023-1102 du 27 novembre 2023 précité met en conformité le cadre juridique des systèmes de vidéoprotection avec les règles relatives à la protection des données, de nouvelles obligations s'imposent aux systèmes déjà autorisés.

D'une part, si une AIPD est obligatoire (cf. partie I. B.), le responsable du système devra la rédiger.

De plus, pour les systèmes mis en œuvre par les autorités publiques, les responsables de traitement devront envoyer un engagement de conformité à la CNIL.

Enfin, le contenu de l'information faite à destination des personnes susceptibles d'être filmées doit être adapté aux nouvelles exigences juridiques.

Il n'est néanmoins pas nécessaire de prendre de nouvelles autorisations pour les systèmes déjà déployés et autorisés.

⁶ Le droit de rectification s'applique en principe à tout traitement. Les personnes concernées peuvent donc normalement demander au responsable d'un traitement que les données à caractère personnel les concernant, qui sont inexactes, soient rectifiées dans les meilleurs délais ou soient complétées. La portée de sa mise en œuvre pour des enregistrements vidéo est *a priori* limitée.

Fiche n°2 : Définition des systèmes de vidéoprotection

Les systèmes de vidéoprotection se définissent par la réunion de différents critères tenant à la technique utilisée, aux lieux filmés et aux finalités poursuivies, ainsi qu'à la personne qui les met en œuvre. Cette définition n'a pas été modifiée par la loi du 19 mai 2023 et reste inchangée.

Techniquement, ces systèmes consistent en l'usage d'au moins une caméra et d'un moniteur, c'est-à-dire un écran permettant la visualisation des images.

La ou les caméras sont installées sur la voie publique ou dans les lieux ou établissements ouverts au public qu'elles permettent de filmer.

Les systèmes de vidéoprotection sont à distinguer des systèmes de vidéosurveillance qui, depuis la loi du 14 mars 2011, désignent des systèmes installés dans les lieux privés ou les lieux professionnels non ouverts au public.

La captation d'images issues de systèmes de vidéoprotection, qu'elle donne lieu à un visionnage des images filmées en temps réel sans conservation ou à un enregistrement, constitue un traitement de données à caractère personnel, au sens du RGPD et de la loi « informatique et libertés ». En effet, les images sur lesquelles apparaissent des personnes qui peuvent être identifiées livrent des informations relatives notamment à leur présence à un endroit et un moment déterminés.

Les systèmes de vidéoprotection ne peuvent pas capter de sons⁷.

A l'inverse, certains dispositifs ne constituent pas des systèmes de vidéoprotection. A titre d'exemple, les dispositifs de contrôle automatisé des données signalétiques des véhicules, plus communément appelés lecture automatisée de plaques d'immatriculation (LAPI), ne constituent pas des systèmes de vidéoprotection.

Il en va de même pour les dispositifs de pièges photographiques ou encore des caméras mobiles (caméras individuelles, caméras installées sur des aéronefs ou caméras embarquées) autorisées dans les cas définis par le titre IV du livre II de la partie législative du code de la sécurité intérieure.

⁷ Article R. 253-1 du code de la sécurité intérieure : « Peuvent être enregistrées dans les traitements mentionnés à l'article R. 251-1, les données à caractère personnel et informations suivantes : « 1° Les images, à l'exclusion des sons, captées par les systèmes de vidéoprotection ; [...] ».

Fiche n°3 : Les lieux d'installation des systèmes de vidéoprotection

Le régime d'autorisation préfectorale de l'article L. 252-1 du code de la sécurité intérieure (auquel renvoie l'article L. 223-1 du même code) ne s'applique qu'aux systèmes installés sur la voie publique ainsi que dans les lieux et établissements ouverts au public. Cette définition n'a pas été modifiée par la loi du 19 mai 2023 et reste inchangée.

I. La voie publique

Un système de vidéoprotection installé sur la voie publique ne saurait visualiser les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées. Si un tel système filme de tels lieux, les entrées, fenêtres de domiciles ou tout lieu privé devront être « floutés ».

Les commerçants peuvent être autorisés à filmer la voie publique pour assurer la protection des abords immédiats des bâtiments et installations dans les lieux particulièrement exposés à des risques d'agression ou de vol (article L. 251-2 CSI).

En outre, dans le seul cas de la protection contre des menaces terroristes, des personnes privées peuvent être autorisées à filmer la voie publique, et plus particulièrement les abords immédiats des bâtiments et installations concernés (article L. 223-1 CSI).

La notion d'« abords immédiats » recouvre la portion de trottoir ou de voie publique strictement nécessaire à la protection de l'établissement.

II. Les lieux et établissements ouverts au public

Dans les conditions prévues par la loi, des systèmes de vidéoprotection peuvent également être mis en œuvre dans des lieux ou établissements ouverts au public.

Au sens de la jurisprudence, un lieu ouvert au public est « *un lieu accessible à tous, sans autorisation spéciale de quiconque, que l'accès en soit permanent et inconditionnel ou subordonné à certaines conditions, heures ou causes déterminées* » (Cass. crim. 29 juin 1988, 87-85.460). Ainsi, l'acquittement d'un droit d'entrée ne fait pas obstacle à ce qu'un lieu soit regardé comme ouvert au public (piscine ou cinéma par exemple).

Les locaux à usage d'habitation, que leur accès soit physiquement limité ou non (par un code d'accès par exemple), ne sont pas considérés comme des lieux ouverts au public, tout comme les espaces extérieurs d'une copropriété (parking ou espace vert, par exemple).

Les locaux à usage professionnel ne relèvent pas de la vidéoprotection lorsqu'ils ne sont pas ouverts au public. A l'inverse, les locaux à usage professionnel qui accueillent du public sont considérés comme des lieux ouverts au public. Pour un même lieu de travail, le régime juridique applicable peut donc varier selon l'espace considéré.

Par exemple, les caméras installées à l'intérieur des transports publics collectifs de personnes constituent des systèmes de vidéoprotection, à moins que les espaces considérés soient fermés au public.

Les lieux ouverts au public sont des espaces clos, non couverts ou partiellement couverts. Ils font l'objet d'aménagements pour recevoir du public (CE, 11 décembre 1985, *Ville d'Annecy*, Lebon p. 369). Les établissements ouverts au public sont quant à eux des espaces clos et couverts.

Fiche n°4 : Les personnes qui peuvent être autorisées à installer un système de vidéoprotection

I. Les autorités compétentes

La loi fixe de manière limitative les personnes autorisées à mettre en œuvre un système de vidéoprotection qui sont responsables de système et revêtent la qualité de responsable de traitement au sens du RGPD ou de la loi « informatique et libertés ». Il s'agit :

- Des autorités publiques compétentes pour assurer les finalités prévues à l'article L. 251-2 du code de la sécurité intérieure, qui peuvent être, à titre d'exemple, le maire d'une commune, le dirigeant d'un établissement public (RATP, hôpital, etc.), le responsable d'une administration publique. Dans le cadre de délégation d'attributions, certaines personnes morales peuvent être regardées comme des autorités publiques compétentes. A titre d'exemple, les sociétés concessionnaires d'autoroutes peuvent être regardées comme des autorités publiques en raison de la délégation, par une autorité publique, d'attributions en matière de régulation des flux routiers ;
- De certains commerçants ;
- De certaines autres personnes morales de droit privé (gestionnaires d'un lieu ou établissement ouvert au public particulièrement exposé à des risques d'agression ou de vol et propriétaires de bâtiments et installations dans des lieux susceptibles d'être exposés à des actes de terrorisme).

II. Les finalités de la vidéoprotection

La loi prévoit que la ou les finalités que peut poursuivre le système de vidéoprotection varie selon le lieu de son installation et la qualité de la personne qui le met en œuvre.

1. Sur la voie publique

Sur la voie publique, la vidéoprotection peut être mise en œuvre par les autorités publiques compétentes pour assurer :

- 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 ;
- 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.

Pour la protection des abords immédiats de leurs bâtiments et installations, les personnes morales de droit privé peuvent être autorisées à mettre en œuvre des systèmes de vidéoprotection dans les lieux susceptibles d'être exposés à des actes de terrorisme.

L'existence d'un risque d'actes de terrorisme s'apprécie au regard des circonstances et du lieu.

Les commerçants peuvent également mettre en œuvre sur la voie publique un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol. Dans cette hypothèse, les commerçants ne peuvent pas procéder au visionnage des images captées, qui n'est autorisé qu'aux agents des services de police et de gendarmerie nationales, aux agents des services de police municipale ainsi qu'aux agents de la Ville de Paris chargés d'un service de police, aux contrôleurs relevant du statut des administrations parisiennes exerçant leurs fonctions dans la spécialité voie publique et aux agents de surveillance de Paris.

L'existence d'un risque d'agression ou de vol s'apprécie au cas par cas. Peuvent, à titre d'exemple, être retenus pour conclure à l'existence de ce risque : l'isolement ou l'ouverture tardive d'un commerce (centre commercial, station-service), la valeur des marchandises détenues (banque, bijouterie) ou leur nature (pharmacie), le nombre d'agressions ou de vols commis au même endroit ou dans des endroits comparables ou le niveau général de la délinquance dans la ville ou le quartier concerné.

2. Dans les lieux et établissements ouverts au public

Les systèmes de vidéoprotection peuvent être mis en œuvre dans des lieux ou établissements ouverts au public, par les autorités publiques compétentes ou par des personnes morales de droit privé, aux seules fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol.

Ces systèmes peuvent également être mis en œuvre dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces lieux et établissements sont susceptibles d'être exposés à des actes de terrorisme.

Personnes	Types de lieux	Fondements juridiques (CSI)	Finalités
Autorités publiques	Voie publique	Article L. 251-2 Article L. 223-1	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 ; 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.
	Lieux et établissements ouverts au public	Article L. 251-2 (avant dernier alinéa) Article L. 223-1 (deuxième alinéa)	Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol. Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme.
Personnes morales de droit privé, y compris les commerçants	Voie publique (abords immédiats)	Article L. 223-1 (premier alinéa)	Protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.
	Lieux et établissements ouverts au public	Article L. 251-2 (avant dernier alinéa) Article L. 223-1 (deuxième alinéa)	Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol. Sécurité des personnes et des biens dans les lieux et établissements susceptibles d'être exposés à des actes de terrorisme.
Commerçants uniquement	Voie publique (abords immédiats)	Articles L. 251-2 (dernier alinéa) et R. 252-3-1	Protection des abords immédiats de leurs bâtiments et des installations dans les lieux particulièrement exposés à des risques d'agression ou de vol. Les bâtiments et installations concernés sont : - les lieux ouverts au public où se déroulent les opérations de vente de biens ou de services ; - les lieux où sont entreposés lesdits biens ou marchandises destinés à ces opérations de vente.

Fiche n°5 : La demande d'autorisation

Les systèmes de vidéoprotection requièrent une autorisation préalable du préfet dans le département avant d'être déployés.

Pour ce faire, les personnes ou services qui adressent une demande au préfet en ce sens doivent fournir la documentation adéquate dont les composantes peuvent varier en fonction de la nécessité d'une AIPD ou non.

Le responsable d'un système est tenu de déclarer toute modification de son système présentant un caractère substantiel.

I. Contenu de la demande d'autorisation présentée par le responsable du système de vidéoprotection.

- *En l'absence d'une AIPD.*

La demande d'autorisation préalable à l'installation d'un système de vidéoprotection est déposée par le chef de service responsable localement compétent. Elle est accompagnée d'un dossier administratif et technique comprenant les éléments listés ci-dessous.

Contrairement à la procédure antérieure à l'entrée en vigueur du décret n° 2023-1102 du 27 novembre 2023 précité, ce dossier ne comprend plus les consignes générales données aux personnels d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images.

Il doit comprendre en revanche :

- Un **rapport de présentation** : il détaille les finalités pour lesquelles le système de vidéoprotection est installé et les caractéristiques techniques du système mis en œuvre. Le responsable de traitement devra notamment détailler la nature de l'activité exercée et les risques d'agression ou de vol auquel est soumis le lieu ou l'établissement à protéger ;
- Si les systèmes de vidéoprotection portent sur la voie publique, un **plan de masse** des lieux montrant les bâtiments du demandeur et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures, ainsi qu'un **plan de détail** à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci. Ce plan de masse ou de détail peut être remplacé par un **plan du périmètre d'installation du système**, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras, lorsque la demande est relative à l'installation d'un système de vidéoprotection à l'intérieur d'un ensemble immobilier ou foncier complexe ou de grande dimension.
- Lorsque les systèmes de vidéoprotection comportent au moins huit caméras, un **plan de détail** à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci. Ce plan de détail peut être remplacé par un **plan du périmètre d'installation du système**, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras, lorsque la demande est relative à l'installation d'un système de vidéoprotection à l'intérieur d'un ensemble immobilier ou foncier complexe ou de grande dimension.
- Lorsque des raisons d'ordre public et des raisons liées à l'utilisation de dispositifs mobiles de surveillance de la circulation routière s'opposent à la transmission de tout ou partie de certaines indications, ou dans le cas où des raisons impérieuses touchant

à la sécurité des lieux où sont conservés des fonds ou valeurs, des objets d'art ou des objets précieux s'opposent à la transmission par le demandeur de la totalité des informations contenues dans le plan de détail, le dossier de demande d'autorisation peut justifier l'absence du plan de masse ou du plan de détail ;

- Lorsque les commerçants peuvent mettre en œuvre sur la voie publique un système de vidéoprotection aux fins d'assurer la protection des abords immédiats de leurs bâtiments et installations, dans les lieux particulièrement exposés à des risques d'agression ou de vol, le plan de détail doit montrer la zone couverte par la ou les caméras dont le champ de vision doit être limité aux abords immédiats des bâtiments et installations en cause ;
- La description du **dispositif prévu pour la transmission, l'enregistrement et le traitement des images** ;
- La description des **mesures de sécurité prises pour la sauvegarde et la protection des images** éventuellement enregistrées : le responsable de traitement doit détailler comment est garantie la sécurité de l'exploitation, du réseau informatique, comment sont protégées les images contre les logiciels malveillants, comment l'accès aux images est protégé (local sous contrôle d'accès physique, connexion par mot de passe), comment la maintenance du système est effectuée ;
- Les modalités de **l'information du public** (se référer à la fiche n° 1-B sur ce point) ;
- **Le délai de conservation des images** souhaité, s'il y a lieu, avec les justifications nécessaires. Ce délai sera fixé par l'autorisation préfectorale et ne peut excéder un mois ;
- La **désignation du responsable de la maintenance**, s'il s'agit d'une personne ou d'un service différent de la personne ou du service responsable du système ;
- Les modalités du **droit d'accès** des personnes intéressées ;
- **La justification de la conformité du système de vidéoprotection aux normes techniques** définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure⁸ ;
- Le cas échéant, **l'engagement de conformité** destiné à la CNIL (se référer à la fiche n° 1-B sur ce point).

- *En présence d'une AIPD.*

Lorsqu'une AIPD a été rédigée, elle est jointe à la demande d'autorisation et remplace les éléments du dossier suivants :

- le rapport de présentation ;
- la description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images ;
- la description des mesures de sécurité prises pour la sauvegarde et la protection des images éventuellement enregistrées ;

⁸ Un modèle d'attestation est proposé dans la notice d'information relative au formulaire CERFA n° 13806*03 (annexe 5). Cette notice est en cours d'actualisation mais peut continuer à être utilisée dans l'attente de la publication d'une nouvelle version.

- les modalités d'information du public ;
- la précision du délai de conservation des images ;
- la désignation du responsable de la maintenance ;
- les modalités du droit d'accès des personnes intéressées.

Lorsqu'il a rédigé une AIPD, le demandeur a la possibilité, lors de la complétion du formulaire CERFA n° 13806*04, d'opérer des renvois à son AIPD pour les champs pertinents.

II. Le lieu de dépôt de la demande d'autorisation par le responsable du système de vidéoprotection

Le dossier de demande d'autorisation doit être déposé à la préfecture du département du lieu d'implantation des caméras ou, à Paris et sur les emprises des aéroports de Paris-Charles de Gaulle, Paris-Le Bourget et Paris-Orly, à la préfecture de police de Paris et, dans le département des Bouches-du-Rhône, à la préfecture de police des Bouches-du-Rhône.

Lorsque le système comporte des caméras installées sur le territoire de plusieurs départements, la demande est déposée à la préfecture du département du siège social du demandeur ou, si le siège social du demandeur est situé à Paris, à la préfecture de police, et, s'il est situé dans le département des Bouches-du-Rhône, à la préfecture de police des Bouches-du-Rhône. Cette hypothèse concerne uniquement les systèmes de vidéoprotection qui ont vocation à être déployés de manière continue sur le territoire de plusieurs départements (exemple : un bus équipé de caméras intérieures qui traverse plusieurs départements). A l'inverse, si une même entreprise dispose d'établissements dans plusieurs départements, les systèmes de vidéoprotection doivent être considérés distincts et faire l'objet de demandes d'autorisation dans chaque département.

Le fait que le dispositif comporte un centre de traitement des images éloigné de ce lieu n'affecte pas la compétence du préfet du lieu d'implantation des caméras.

Le dépôt d'un dossier, dès lors que celui-ci est complet, donne lieu à délivrance d'un récépissé qui fixe le point de départ des délais légaux. Le dossier est réputé complet lorsqu'il comporte l'ensemble des documents requis par l'article R. 252-3 du code de la sécurité intérieure et que les informations fournies au titre d'une catégorie de documents sont suffisamment précises. Le caractère limitatif de la liste des informations ne fait en effet pas obstacle à ce que le préfet demande des précisions utiles, y compris sous forme de documents complémentaires.

Lorsque la demande porte sur la mise en œuvre de caméras mobiles installées dans des véhicules, le préfet compétent sera celui du lieu du siège de la personne responsable du système.

Fiche n° 6 : Le rôle de la commission départementale de vidéoprotection

La commission départementale de vidéoprotection est instituée par arrêté préfectoral. Il appartient au préfet dans le département de veiller à sa composition et à son bon fonctionnement.

Elle doit être consultée dans le cadre de la procédure d'autorisation d'un système de vidéoprotection. Elle rend un avis simple, qui ne lie donc pas l'autorité administrative. Dans le cadre de sa mission consultative, elle examine la régularité et la proportionnalité du dispositif envisagé.

Les attributions de cette commission sont exercées, sur les emprises des aérodromes de Paris-Charles de Gaulle, Paris-Le Bourget et Paris-Orly, par la commission départementale de vidéoprotection de Paris.

I. Composition

La commission est composée de quatre membres désignés pour trois ans, chacun ayant un suppléant :

- Un magistrat du siège honoraire, ou, à défaut, une personnalité qualifiée à raison de sa compétence dans le domaine de la vidéoprotection ou des libertés individuelles désignée par le premier président de la cour d'appel, qui la préside ;
- Un maire, désigné par la ou les associations départementales des maires, ou, à Paris, un conseiller de Paris ou conseiller d'arrondissement désigné par le Conseil de Paris ;
- Un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes ;
- Une personnalité qualifiée choisie par le préfet en raison de sa compétence.

Dans le cas où il existe plusieurs associations des maires ou plusieurs chambres de commerce et de l'industrie, le préfet dans le département invite leurs présidents à rechercher un accord sur un seul nom pour ce qui concerne le titulaire et le suppléant. Si un tel accord ne peut être obtenu, le préfet dans le département choisit le représentant de ces associations ou organismes parmi les candidatures qui lui ont été soumises.

La personnalité qualifiée, désignée par le préfet, doit être choisie en raison de sa compétence dans un domaine présentant un lien avec la vidéoprotection : connaissance de la technique employée, compétence dans le domaine de la sécurité publique ou des droits fondamentaux. Cette personnalité qualifiée ne saurait être un agent public en fonction dans les services préfectoraux ou dans les services de police ou de gendarmerie.

II. Fonctionnement

La commission départementale est consultée préalablement à toute décision préfectorale sur les demandes d'autorisation de systèmes de vidéoprotection et de modification de systèmes existants, à l'exception de ceux concernant la défense nationale et en cas d'urgence (voir point C).

Son secrétariat, désigné par le préfet, est assuré par un agent de la préfecture.

A. L'instruction des demandes par la commission départementale de vidéoprotection

La commission peut entendre le demandeur, solliciter tout complément d'information sur les pièces du dossier et, le cas échéant, solliciter l'avis de toute personne qualifiée qui lui paraîtrait indispensable pour l'examen d'un dossier particulier. Elle est, en tout état de cause, tenue d'entendre un représentant de la police ou de la gendarmerie nationales territorialement compétent ou un agent des douanes ou des services d'incendie et de secours ou un représentant de la police municipale concernée. Cette audition d'un responsable de la sécurité joue un rôle déterminant dans l'appréciation que la commission porte sur l'intérêt qui s'attache à l'implantation d'un dispositif. Elle permet à cette dernière d'exercer le contrôle de proportionnalité qui se trouve au centre de sa mission.

B. Les modalités de consultation de la commission départementale de vidéoprotection

La commission doit émettre son avis dans un délai de trois mois. A l'issue de ce délai, si la commission départementale n'a pas émis d'avis, cet avis est réputé donné.

Toutefois, avant l'expiration de ce délai, la commission siégeant en formation plénière peut demander à disposer d'un délai supplémentaire d'un mois, dont l'octroi est de droit.

La réglementation n'organise aucune mesure de publicité de l'avis de la commission ni sa transmission au demandeur. Saisi d'une demande tendant à la communication d'un avis, le préfet doit en apprécier le bien-fondé au regard des règles relatives à la communication des documents administratifs prévue par le code des relations entre le public et l'administration (CRPA). Cet avis est un document produit par une commission administrative dans le cadre d'une mission de service public. A ce titre, il est en principe communicable. Il se peut cependant, dans certains cas, qu'un avis comporte des mentions dont la divulgation porterait atteinte à la sûreté de l'Etat, à la sécurité publique ou à celle des personnes, ou compromettrait un secret protégé par la loi (secret de la vie privée, secret médical, secret professionnel, secret en matière commerciale et industrielle...). Pour préserver la confidentialité des informations protégées, l'administration peut communiquer un document en occultant certains passages.

De façon générale, les membres de la commission doivent s'abstenir de communiquer la teneur de ses avis à des tiers ou de faire état des informations qui auront pu être portées à leur connaissance. De telles divulgations pourraient en effet compromettre la sécurité des lieux et établissements concernés. Cette obligation de discrétion professionnelle doit être rappelée à tous les membres de la commission.

C. L'absence de consultation de la commission départementale de vidéoprotection en cas d'urgence

Dans certains cas d'urgence, le préfet a la faculté de prendre un arrêté d'autorisation d'installation d'un système de vidéoprotection sans avis préalable de la commission départementale, pour une durée maximale de quatre mois.

Cette procédure exceptionnelle vise à accélérer le traitement de deux types de situations :

- les demandes présentées par des pétitionnaires exposés de manière soudaine à des risques terroristes ;
- les manifestations ou rassemblements de grande ampleur dont le préfet est informé dans un délai trop bref pour réunir la commission départementale de

vidéoprotection. Les événements visés par cette procédure d'autorisation provisoire sont ceux présentant un risque particulier pour la sécurité des personnes et des biens en raison du nombre de personnes attendues et/ou de la nature de la manifestation.

Dans ces cas d'urgence, le président de la commission départementale doit être informé sans délai, par le préfet, de sa décision d'appliquer cette procédure d'urgence. Celui-ci aura alors la possibilité de réunir la commission pour qu'elle donne un avis sur la mise en œuvre de cette procédure. Contrairement à la procédure de droit commun, cet avis interviendra postérieurement à l'arrêté d'autorisation provisoire et seulement si la manifestation ou le rassemblement n'a pas encore pris fin.

Si le demandeur souhaite maintenir son dispositif après l'expiration du délai de quatre mois, il devra présenter une demande d'autorisation, qui sera instruite selon la procédure de droit commun. La délivrance d'une autorisation provisoire ne préjugera pas nécessairement du sens de la décision statuant sur cette demande, qui pourra tenir compte d'éléments portés à la connaissance du préfet postérieurement à cette délivrance.

Fiche n° 7 : La décision préfectorale

Ces éléments n'ont pas été modifiés par la loi du 19 mai 2023.

I. Le travail d'instruction préfectorale relative à une demande d'autorisation de déploiement d'un système de vidéoprotection.

Avant d'autoriser le déploiement d'un système de vidéoprotection, le préfet instruit le dossier qui lui a été soumis.

Lorsque le préfet est saisi de demandes relatives à la vidéoprotection sur la voie publique ou dans des lieux et établissements ouverts au public, il vérifie, compte tenu de la nature du lieu surveillé, des finalités poursuivies et des autorités ou personnes morales concernées, la régularité de la demande qui est présentée (cf. fiche n° 5).

Selon les considérations mises en avant par le demandeur, il examine les trois points suivants.

a) Le cas échéant, le lieu est-il particulièrement exposé à des risques d'agression ou de vol ?

Pourront, à titre d'exemple, être retenus pour conclure à l'existence de ce risque :

- l'isolement ou l'ouverture tardive d'un commerce (centre commercial, station-service) ;
- la valeur des marchandises détenues (banque, bijouterie) ou leur nature (pharmacie) ;
- le nombre d'agressions ou de vols commis au même endroit ou dans des endroits comparables ;
- le niveau général de la délinquance dans la ville ou le quartier concerné.

L'intérêt de la vidéoprotection en termes de prévention de la délinquance doit conduire à considérer que ce risque est avéré, dans certains cas, alors même que le lieu ou l'établissement à surveiller n'a pas, au jour de la demande, connu d'agression ou de vol. Il appartient au service de sécurité territorialement compétent de fournir, lors de son audition par la commission départementale, les informations relatives au niveau de risque dans le type d'établissement ou dans le quartier concerné.

b) Le lieu est-il soumis à une menace terroriste ?

Cette condition pourra notamment être tenue pour remplie si le dispositif a pour vocation de protéger des lieux emblématiques d'institutions publiques, de certains groupes ou intérêts faisant notoirement l'objet de menaces, des lieux dans lesquels une éventuelle attaque aurait un retentissement particulier en raison du nombre des victimes potentielles ou du public concerné (ex : lieux de culte). Elle pourra également l'être lorsque sont en cause des lieux couverts par un plan de sécurité prévu par le code de la défense ou par une norme de niveau européen.

c) Le contrôle de proportionnalité.

Le préfet est chargé de veiller à ce que les systèmes de vidéoprotection ne portent pas une atteinte excessive au droit de chacun au respect de sa vie privée, au regard de l'intérêt qu'ils présentent en termes de sécurité ou d'ordre public. Il exerce donc un contrôle de proportionnalité qui constitue le cadre traditionnel d'appréciation des mesures de police administrative, au regard du deuxième alinéa de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales qui impose le respect du droit à la vie privée. Différents éléments sont susceptibles de guider son appréciation en la matière (nécessité avérée de la vidéoprotection, ampleur du dispositif, etc.).

II. La décision d'autorisation

A. Le contenu de la décision d'autorisation.

L'autorisation préfectorale est délivrée pour une durée de cinq ans renouvelable.

L'autorisation précise les précautions utiles, en particulier le délai de conservation des images issues des systèmes de vidéoprotection, les personnes chargées de l'exploitation du système de vidéoprotection, les mesures à prendre pour assurer le respect des dispositions du code de la sécurité intérieure, notamment pour être conformes aux normes techniques définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure.

Concernant le délai de conservation des images par le responsable du système, il ne peut excéder un mois. Au terme de ce délai, les données doivent être effacées automatiquement des traitements. À l'inverse, l'autorisation préfectorale peut prévoir un délai minimal de conservation des enregistrements.

Lorsque les données ont, dans ce délai, été extraites et transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, elles sont conservées selon les règles propres à chacune de ces procédures par l'autorité qui en a la charge.

L'autorisation doit également préciser les personnes pouvant accéder au visionnage des images, et celles pouvant en être destinataires. Il n'est pas nécessaire que l'autorisation comporte les noms des agents des services concernés. Elle indiquera seulement les catégories de personnes concernées, parmi celles listées à l'article R. 253-3 du code de la sécurité intérieure. La désignation revient donc aux services concernés. L'accès peut être autorisé pour la totalité de la durée de validité de l'autorisation ou pour une période plus réduite, correspondant, par exemple, au déroulement d'un évènement précisément identifié.

Le tableau ci-dessous recense les personnes qui, en application de l'article R. 253-3 du code de la sécurité intérieure, peuvent visionner les images issues des systèmes de vidéoprotection mis en œuvre.

Par ailleurs, pourront recevoir communication des images issues d'un système de vidéoprotection mis en œuvre par un tiers service ou une tierce personne, en application du III de l'article R. 253-3 du CSI :

- Les agents des services de police nationale ;
- Les agents des unités de la gendarmerie nationale ;
- Les agents des douanes ;
- Les agents des services d'incendie et de secours ;
- Les agents de police municipale 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 ;
- Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1 pour les seules images issues de systèmes implantés sur le territoire de la ville de Paris ;
- Les autorités administratives et judiciaires dont la présence est requise dans les salles de commandement au sein desquelles des images de vidéoprotection sont transmises ;
- Les officiers et agents de police judiciaire ;
- Les agents des services d'inspection générale de l'Etat.

Responsable du système de vidéoprotection	Lieux de mise en œuvre du système	Accédants	
Autorité publique	Voie publique	Autorités publiques (hors communes)	
		Les agents individuellement désignés et dûment habilités par les autorités publiques responsables du système.	
	Lieux et établissements ouverts au public	Communes	
		<p>Le maire ;</p> <p>Les adjoints au maire et membres du conseil municipal qui sont délégataires d'attributions de police municipale ;</p> <p>Les agents de police municipale ;</p> <p>Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1 ;</p> <p>Les agents des communes, des établissements publics de coopération intercommunale et des syndicats mixtes, agréés par le représentant de l'Etat dans le département, en application de l'article L. 132-14-1 du code de la sécurité intérieure.</p>	
Personne morale de droit privé, hors commerçants	Voie publique (abords immédiats des bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme uniquement)	Les agents qui relèvent de l'autorité publique individuellement désignés et dûment habilités par elle ;	
		Les opérateurs privés agissant pour le compte de la personne morale, en application de l'article L. 613-13.	
	Lieux et établissements ouverts au public	<p>Les agents qui relèvent de la personne morale individuellement désignés et dûment habilités par elle ;</p> <p>Les opérateurs privés agissant pour le compte du responsable du système, dans les conditions prévues à l'article L. 613-13.</p>	
Commerçants	Voie publique (abords immédiats des bâtiments et installations)	Dans les lieux particulièrement exposés à des risques d'agression ou de vol	<p>Les agents des services de police nationale ;</p> <p>Les agents des unités de la gendarmerie nationale ;</p> <p>Les agents de police municipale ;</p> <p>Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1.</p>
		Dans les lieux susceptibles d'être exposés à des actes de terrorisme uniquement	<p>Les opérateurs relevant du commerçant individuellement désignés et dûment habilités par lui ;</p> <p>Les opérateurs privés agissant pour le compte du commerçant, en application de l'article L. 613-13.</p>
	Lieux et établissements ouverts au public	Les opérateurs qui relèvent du commerçant individuellement désignés et dûment habilités par lui ;	
		Les opérateurs privés agissant pour le compte du commerçant, dans les conditions prévues à l'article L. 613-13.	

B. Obligations procédurales encadrant la décision préfectorale.

Le silence gardé par le préfet pendant plus de quatre mois sur une demande d'autorisation vaut décision de rejet.

En application de l'article L. 211-2 du code des relations entre le public et l'administration, les décisions défavorables doivent être motivées.

L'autorisation doit être publiée au recueil des actes administratifs de la préfecture, sauf dérogation motivée par un impératif de défense nationale. Le préfet met à la disposition du public la liste des autorisations de systèmes de vidéoprotection publiées dans les conditions prévues à l'article R. 252-16 du code de la sécurité intérieure, qui précise pour chacun d'eux la date de son autorisation et le service ou la personne responsable. Il communique également la liste des systèmes de vidéoprotection autorisés sur le territoire de chaque commune au maire, qui la met à la disposition du public à la mairie et, le cas échéant, dans les mairies d'arrondissement.

III. L'autorisation provisoire

Lorsque l'urgence et l'exposition particulière à un risque d'acte de terrorisme le requièrent, le préfet peut délivrer aux autorités publiques compétentes ou aux personnes morales, sans avis préalable de la commission départementale de vidéoprotection, une autorisation provisoire d'installation d'un système de vidéoprotection, pour une durée maximale de quatre mois.

De même, lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens, il peut également délivrer, à ces mêmes personnes, sans avis préalable de la commission départementale de vidéoprotection, une autorisation provisoire d'installation d'un système de vidéoprotection, pour une durée maximale de quatre mois.

Dans ces deux hypothèses, le préfet informe immédiatement le président de la commission départementale de vidéoprotection, qui peut la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure d'autorisation provisoire.

Le préfet recueille l'avis de la commission départementale de vidéoprotection sur la mise en œuvre du système de vidéoprotection et se prononce sur son maintien. La commission doit rendre son avis avant l'expiration du délai de validité de l'autorisation provisoire.

IV. La prescription préfectorale

Le préfet peut prescrire la mise en œuvre de systèmes de vidéoprotection dans trois situations.

Aux fins de prévention d'actes de terrorisme, il peut prescrire la mise en œuvre, dans un délai qu'il fixe, de systèmes de vidéoprotection, aux personnes suivantes :

- Les exploitants, publics ou privés, des établissements, installations ou ouvrages, désignés par l'autorité administrative, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, au sens des articles L. 1332-1 et 1332-2 du code de la défense, ainsi que les exploitants de certains établissements, en application de l'article L. 1332-2 du code de la défense⁹ ;

⁹ Usines, ateliers, dépôts, chantiers et, d'une manière générale, les installations exploitées ou détenues par toute personne physique ou morale, publique ou privée, qui peuvent présenter des dangers ou des inconvénients soit pour la commodité du voisinage, soit pour la santé, la sécurité, la salubrité publiques, soit pour l'agriculture, soit pour la

- Les gestionnaires d'infrastructures, les autorités et personnes exploitant des transports collectifs, relevant de l'activité de transports terrestres qui s'effectuent entre un point d'origine et un point de destination situés sur le territoire national, en application de l'article L. 1000-1 du code des transports ;
- Les exploitants d'aéroports qui sont ouverts au trafic international.

Cette prescription préfectorale doit être précédée, sauf en matière de défense nationale, d'une consultation de la commission départementale de vidéoprotection si elle porte sur une installation de vidéoprotection filmant la voie publique ou des lieux et établissements ouverts au public.

De plus, lorsque l'urgence et l'exposition particulière à un risque d'actes de terrorisme le requièrent, il peut également prescrire, sans avis préalable de la commission départementale de vidéoprotection, la mise en œuvre d'un système de vidéoprotection.

Enfin, lorsqu'il est informé de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens, il peut prescrire, sans avis préalable de la commission départementale de vidéoprotection, la mise en œuvre d'un système de vidéoprotection.

Dans ces deux dernières hypothèses, le président de la commission est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure de décision provisoire.

Avant l'expiration d'un délai maximal de quatre mois, le préfet recueille l'avis de la commission départementale de vidéoprotection sur la mise en œuvre du système de vidéoprotection et se prononce sur son maintien.

V. La demande de mise en œuvre d'un système

Aux fins de prévention d'actes de terrorisme, de protection des abords des établissements, installations ou ouvrages mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ou de protection des intérêts fondamentaux de la Nation, le préfet peut demander à une commune la mise en œuvre de systèmes de vidéoprotection. Le conseil municipal doit alors délibérer dans un délai de trois mois sur cette demande. En cas de décision positive, la commune doit réaliser une demande d'autorisation de mise en œuvre d'un système de vidéoprotection, dans les conditions exposées dans la fiche n° 5 de la présente circulaire, pour une ou plusieurs finalités visées à l'article L. 251-2 du code de la sécurité intérieure.

Les conditions de financement du fonctionnement et de la maintenance du système de vidéoprotection font l'objet d'une convention conclue entre la commune de son lieu d'implantation et le préfet.

VI. La procédure de modification des demandes

Lorsque des modifications apportées à un système sont portées à la connaissance du préfet, il doit évaluer la nécessité de délivrer une nouvelle autorisation au responsable de système.

protection de la nature, de l'environnement et des paysages, soit pour l'utilisation économe des sols naturels, agricoles ou forestiers, soit pour l'utilisation rationnelle de l'énergie, soit pour la conservation des sites et des monuments ainsi que des éléments du patrimoine archéologique, ainsi que les exploitants des établissements comprenant une installation nucléaire de base, à savoir, réacteur nucléaire, installations de préparation, d'enrichissement, de fabrication, de traitement ou d'entreposage de combustibles nucléaires ou de traitement, d'entreposage ou de stockage de déchets radioactifs, installations contenant des substances radioactives ou fissiles et répondant à des caractéristiques définies, accélérateurs de particules répondant à des caractéristiques définies où les centres de stockage en couche géologique profonde de déchets radioactifs, quand la destruction ou l'avarie de certaines installations de ces établissements peut présenter un danger grave pour la population.

Les modifications nécessitant une nouvelle autorisation préfectorale sont les suivantes :

- la modification de la nature des lieux protégés ;
- la modification des finalités du système ;
- la modification des conditions d'exploitation des images ;
- la modification de la durée de conservation des images ;
- la modification des caractéristiques techniques du système.

Dans d'autres cas, il convient d'apprécier si les modifications apportées au système appellent, compte tenu de leur nature et de leur ampleur, le retrait de l'autorisation et la délivrance d'une nouvelle autorisation. Il y aura place pour une telle appréciation face à une augmentation limitée du nombre des caméras ou de la surface couverte. Il en ira de même dans le cas où un changement dans l'organisation de la personne morale titulaire de l'autorisation survient. A titre d'exemple, un changement radical de la nature de l'activité commerciale dans un local équipé de vidéoprotection devra sans doute conduire le préfet à retirer l'autorisation et à en délivrer une nouvelle.

VII. La procédure de renouvellement des demandes d'autorisation

Dans le cadre de demandes de renouvellement, le demandeur doit déposer un nouveau dossier complet.

S'agissant des demandes de renouvellement d'autorisation de systèmes de vidéoprotection inchangés depuis leur autorisation, une attention particulière doit être portée au contexte du site dans lequel le système est installé, celui-ci ayant pu évoluer (réalisation d'aménagements urbains, évolution du risque d'atteinte aux biens ou aux personnes, etc.). Quels que soient le nombre de caméras et la nature des lieux visionnés, les services de préfecture doivent avoir communication des documents relatifs au contexte ayant évolué depuis la demande d'autorisation initiale.

Même si le système de vidéoprotection est inchangé, son autorisation doit être renouvelée après avis de la commission départementale.

Enfin, si les titulaires d'autorisations venues à échéance ne sollicitent pas une demande de renouvellement, le préfet peut considérer l'autorisation délivrée comme caduque.

Fiche n° 8 : Les contrôles et sanctions

I. Le contrôle de la commission départementale de vidéoprotection

Dans le cadre des contrôles qu'elle exerce de sa propre initiative ou sur saisine de toute personne intéressée, la commission départementale de vidéoprotection peut déléguer un de ses membres pour collecter, notamment auprès du responsable du système, les informations utiles relatives aux conditions de fonctionnement d'un système de vidéoprotection et visant à vérifier le respect des obligations de destruction des enregistrements ou la conformité du système à son autorisation.

La commission départementale de vidéoprotection peut être réunie à l'initiative de son président pour examiner les résultats des contrôles et émettre, le cas échéant, des recommandations et proposer au préfet la suspension ou la suppression d'un système de vidéoprotection lorsqu'elle constate qu'il n'est pas autorisé ou qu'il en est fait un usage anormal ou non conforme à son autorisation.

La commission départementale de vidéoprotection exerce sa mission de contrôle dans les conditions prévues par l'article L. 253-3 du code de la sécurité intérieure.

II. Le contrôle de la CNIL

Avant l'entrée en vigueur de la loi du 19 mai 2023, les pouvoirs de la CNIL étaient déterminés par le code de la sécurité intérieure. Désormais, elle exerce ses prérogatives conformément à la loi « informatique et libertés ».

La CNIL peut contrôler tout responsable de traitement à la suite de plaintes qu'elle reçoit, de signalements qui lui sont faits, ou sur simple auto-saisine. Ces contrôles peuvent avoir lieu sur place, en ligne ou constituer une audition sur convocation.

En cas de manquements constatés lors du contrôle, le président de la CNIL peut décider d'une mise en demeure ou la formation restreinte peut prononcer différentes mesures ou sanctions.

III. Le contrôle du préfet

Le préfet peut faire procéder, par les services de police ou de gendarmerie, à des contrôles de vérification des prescriptions émises dans les autorisations préfectorales. Le contrôle peut également porter sur l'existence de systèmes non autorisés et sur la conformité du système aux normes techniques définies par arrêté en application de l'article L. 252-4 du code de la sécurité intérieure.

L'article R. 252-17 du code de la sécurité intérieure impose au responsable du système de tenir le préfet informé des événements importants qui affectent l'exploitation du système de vidéoprotection mis en œuvre. Doivent à ce titre lui être signalés la mise en service effective des caméras, ainsi que la localisation des caméras à l'intérieur du périmètre d'installation du système de vidéoprotection préalablement à leur installation et, le cas échéant, à leur déplacement.

IV. Les sanctions

A. La suspension de l'autorisation

A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la commission départementale de vidéoprotection peut, après en avoir informé le maire, proposer au préfet la suspension de l'autorisation d'installation, en application de l'article L. 253-1 du code de la sécurité intérieure.

L'interruption provisoire de la mise en œuvre du traitement peut être prononcée pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du titre III lorsqu'ils sont mis en œuvre pour le compte de l'Etat. Concernant le cas spécifique de ces derniers, la CNIL peut informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée. Le Premier ministre fait alors connaître à la formation restreinte de la CNIL les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

B. Le retrait de l'autorisation

A l'issue du contrôle qu'elle peut exercer sur les systèmes de vidéoprotection, la commission départementale de vidéoprotection peut, après en avoir informé le maire, proposer au préfet le retrait de l'autorisation d'installation, en cas de manquement à la loi ou de modification des conditions au vu desquelles elle a été délivrée.

C. La fermeture administrative de l'établissement

Le maintien d'un système de vidéoprotection sans autorisation peut entraîner, après mise en demeure du préfet, la fermeture administrative de l'établissement pour une durée de trois mois, par décision du préfet, à la demande de cette commission ou de sa propre initiative, en application de l'article L. 253-4 du code de la sécurité intérieure. A l'issue de cette période de trois mois, si l'établissement n'a pas régularisé sa situation, le préfet peut lui enjoindre de démonter ledit système et, s'il ne donne pas suite à cette injonction, prononcer une nouvelle mesure de fermeture de trois mois.

D. Sanction pénale

La mise en œuvre d'un système de vidéoprotection fixant, enregistrant ou transmettant l'image d'une personne dans un lieu privé constitue un délit en application de l'article 226-1 du code pénal, puni d'un an d'emprisonnement et de 45 000 euros d'amende.

La mise en œuvre d'un système de vidéoprotection sur la voie publique ou dans un espace ouvert au public sans autorisation préalable constitue un délit en application de l'article 226-16 du code pénal, ce qui peut fonder une saisine du parquet compétent au titre de l'article 40 du code de procédure pénale. Ainsi, les personnes déclarées responsables pénalement d'un tel délit encourent cinq ans d'emprisonnement et 300 000 euros d'amende. Aussi, s'agissant des personnes morales, lorsqu'elles sont déclarées responsables pénalement d'un tel délit, elles encourent les peines auxquelles il est fait référence à l'article 226-24 du code pénal¹⁰.

¹⁰ Il s'agit des peines suivantes : l'amende au quintuple ; l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ; le placement, pour une durée de cinq ans au plus, sous surveillance judiciaire ; la fermeture définitive ou pour une durée de cinq ans au plus des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ; l'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le

Ainsi, les personnes déclarées responsables pénalement d'un tel délit encourrent un an d'emprisonnement et 45 000 euros d'amende. De même, s'agissant des personnes morales, lorsqu'elles sont déclarées responsables pénalement d'un tel délit, elles encourrent les peines prévues à l'article 226-7 de ce même code¹¹.

retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ; la peine de confiscation, dans les conditions et selon les modalités prévues à l'article 131-21 ; l'affichage de la décision prononcée ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

¹¹ Il s'agit des peines suivantes : l'amende au quintuple ; l'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ; l'affichage ou la diffusion de la décision prononcée, dans les conditions prévues par l'article 131-35.

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	3
2. Présentation du traitement des images.....	4
2.1 Vue d'ensemble	4
2.2. Données, processus et supports	6
2.1.1 Description des données.....	6
2.1.2. Accédants	7
2.1.3. Destinataires	9
2.1.4. Données sensibles ou relatives aux condamnations pénales, infractions ou mesures de sûreté.....	9
2.1.5. Description des traitements de données et supports.....	10
3. Principes fondamentaux.....	11
3.1. Mesures garantissant la proportionnalité et la nécessité du traitement	11
3.1.1. Finalités	11
3.1.2. Fondement juridique et base légale	11
3.1.3. Minimisation des données.....	11
3.1.4. Qualité des données	12
3.1.5. Durées de conservation	12
3.1.6. Evaluation des mesures	13
3.2. Évaluation des mesures protectrices des droits des personnes concernées	13
3.2.1. Mesures pour l'information des personnes.....	13
3.2.2 Mesures pour le recueil du consentement.....	14
3.2.3. Mesures pour les droits d'accès et à la portabilité	14

3.2.4. Mesures pour les droits de rectification et d'effacement	14
3.2.5. Mesures pour les droits à la limitation du traitement et d'opposition	15
3.2.6. Mesures pour la sous-traitance	15
3.2.7. Evaluation des mesures	15
4. Etude des risques liés à la sécurité des données	16
4.1. Évaluation des mesures	16
4.1.1. Mesures générales de sécurité	16
4.1.2. Mesures organisationnelles (gouvernance).....	18
4.2. Appréciation des risques : les atteintes potentielles aux droits et libertés des personnes physiques	20
4.2.1. Analyse et estimation des risques.....	20
5. Validation de l'analyse d'impact	23
5.1. Eléments utiles à la validation.....	23
5.1.1. Synthèse relative à la conformité au RGPD	23
5.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données.....	23
5.1.3. Cartographie des risques liés à la sécurité des données.....	24
5.1.3. Plan d'actions (si mesures correctives prévues) :	27
5.2. Validation formelle.....	27
6. Annexes	28

1. PRESENTATION GENERALE

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. PRESENTATION DU TRAITEMENT DES IMAGES

2.1 Vue d'ensemble

Finalités	<input type="checkbox"/>	La protection des bâtiments et installations publics et de leurs abords
	<input type="checkbox"/>	La sauvegarde des installations utiles à la défense nationale
	<input type="checkbox"/>	La régulation des flux de transport
	<input type="checkbox"/>	La constatation des infractions aux règles de la circulation
	<input type="checkbox"/>	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
	<input type="checkbox"/>	La prévention d'actes de terrorisme, dans les conditions prévues au chapitre III du titre II du présent livre
	<input type="checkbox"/>	La prévention des risques naturels ou technologiques
	<input type="checkbox"/>	Le secours aux personnes et la défense contre l'incendie
	<input type="checkbox"/>	La sécurité des installations accueillant du public dans les parcs d'attraction
	<input type="checkbox"/>	Le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile
	<input type="checkbox"/>	La prévention et la constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets
	<input type="checkbox"/>	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 responsable du 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)	<input type="checkbox"/>	Titre II et RGD
	<input type="checkbox"/>	Titre III
	<input type="checkbox"/>	Titre IV
Enjeux du traitement	<p>[Description concrète du besoin de recourir à un système de vidéoprotection].</p> <ul style="list-style-type: none"> ▪ Dissuader <p>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...</p> <ul style="list-style-type: none"> ▪ Surveiller <p>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</p>	

	<p>procédures judiciaires, Surveillance constante à distance de quartiers éloignés, difficiles d'accès ou très sensibles Protection des établissements sensibles.</p> <ul style="list-style-type: none"> Assurer la gestion des événements de voie publique <p>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</p> <p>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.</p> <ul style="list-style-type: none"> Identifier des auteurs d'infraction <p>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.</p> <p>Dans le cadre d'une intervention, l'opérateur suit et guide, le cas échéant, l'unité d'intervention.</p> <p>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.</p>
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
<p>Règlement général relatif à la protection des données</p> <p>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</p> <p>Loi informatique et libertés, [préciser : son/ses titre II, III et/ou IV]</p> <p>Arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure</p> <p>Arrêté préfectoral d'autorisation [renseigner les références de l'arrêté]</p>

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

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	[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	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

son système de vidéoprotection	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	[choisir oui ou non]	[A compléter]	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 ou mesures de sûreté

Catégorie	Enregistrement	Justification de la collecte
-----------	----------------	------------------------------

	(oui / non)	
Données sensibles de l'article 6 de la loi du 6 janvier 1978		
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
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	<p>[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 :</p> <ul style="list-style-type: none"> - Nombre et lieu d'implantation des caméras ; - Centre de supervision ; 	[A compléter]

et transmission des images	<ul style="list-style-type: none"> - Système analogique ou numérique ; - Caméras fixes ou orientables, caméras dômes, caméras PTZ, caméras mégapixel, plan large ou plan étroit, résolution des images, standards vidéo, 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.	[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)]
Jour et plages horaires d'enregistrement.	
Lieu où ont été collectées les données.	

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 modifiées
[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	[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.
Jour et plages horaires d'enregistrement.			

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 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 [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 panneaux 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'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 {[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 LIES A LA SECURITE DES DONNEES

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/a méliorable	
Archivage	<p>[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.)]</p> <p>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</p>	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	<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	
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	
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	

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/a méliorable	
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 / amélioré	Si amélioré, 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/a méliorable	
Politique (gestion des règles)	Formation, charte informatique, règles de gestion des habilitations des administrateur, agents habilités et leurs profils	Acceptable	
Gestion des risques	Tracabilité 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/a méliorable	
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. [Des mesures	Acceptable	

	<p>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.</p> <p>Un enregistrement au journal de la défaillance constatée et une alerte des agents du dysfonctionnement constaté peut être mis en place.]</p>		
Gestion des personnels	<p>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.</p>	Acceptable	
Relations avec les tiers	<p>[Préciser : convention, relation avec la police, les pompiers etc.]</p>	Acceptable/a méliorable	
Supervision	<p>Le responsable de traitement veille par des contrôles aux connexions afin de détecter des accès anormaux mais aussi aux éventuels incidents.</p>	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	<p>Usurpation ou divulgation de mot de passe</p> <p>Action interne par un personnel</p> <p>Cyberattaque automatisée (virus) ou volontaire par ingénierie sociale.</p> <p>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</p> <p>Vol du matériel par un tiers</p>	<p>Mauvaise gouvernance</p> <p>Intégrité et confidentialité des données.</p> <p>Effacement des données</p> <p>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</p> <p>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</p> <p>Discrédit de l'usage du dispositif</p> <p>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>

Analyse d'impact relative à la protection des données

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.	<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.</p> <p>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</p> <p>Risque de dégradations de biens en représailles ou de violence pour une personne injustement mise en cause</p> <p>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.</p> <p>Information des personnels sur la gestion de données critiques.</p> <p>Sauvegarde des données</p>	Importante mais une modification des images captées serait nécessairement détectée car portant atteinte à l'intégrité de la donnée.	Limitée
---	---	---	--	---	---	---------

Analyse d'impact relative à la protection des données

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>	<p>Limitée</p>
-------------------------------	---	---	---	---	---	----------------

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

Analyse d'impact relative à la protection des 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	<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"> Paielements 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.) 	<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
-------------------	---	---	--	---

			<ul style="list-style-type: none"> • Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) • Profilage imprécis ou abusif 	
3. Importante	<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 irrémissible • 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 irrémediables, 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).

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 personnes morales de droit privé

Responsable du traitement :

Identité : [A COMPLETER]

Adresse : [A COMPLETER]

Service gestionnaire :

Direction : [A COMPLETER]

Adresse : [A COMPLETER]

TABLE DES MATIERES

1. Présentation générale	3
2. Présentation du traitement des images.....	4
2.1 Vue d'ensemble	4
2.2. Données, processus et supports	6
2.1.1 Description des données.....	6
2.1.2. Accédants	7
2.1.3. Destinataires	9
2.1.4. Données sensibles ou relatives aux condamnations pénales, infractions ou mesures de sûreté.....	9
2.1.5. Description des traitements de données et supports.....	10
3. Principes fondamentaux.....	11
3.1. Mesures garantissant la proportionnalité et la nécessité du traitement	11
3.1.1. Finalités	11
3.1.2. Fondement juridique et base légale	11
3.1.3. Minimisation des données.....	11
3.1.4. Qualité des données	12
3.1.5. Durées de conservation	12
3.1.6. Evaluation des mesures	13
3.2. Évaluation des mesures protectrices des droits des personnes concernées	13
3.2.1. Mesures pour l'information des personnes.....	13
3.2.2 Mesures pour le recueil du consentement.....	14
3.2.3. Mesures pour les droits d'accès et à la portabilité	14

3.2.4. Mesures pour les droits de rectification et d'effacement	14
3.2.5. Mesures pour les droits à la limitation du traitement et d'opposition	15
3.2.6. Mesures pour la sous-traitance	15
3.2.7. Evaluation des mesures	15
4. Etude des risques liés à la sécurité des données	16
4.1. Évaluation des mesures	16
4.1.1. Mesures générales de sécurité	16
4.1.2. Mesures organisationnelles (gouvernance).....	18
4.2. Appréciation des risques : les atteintes potentielles aux droits et libertés des personnes physiques	20
4.2.1. Analyse et estimation des risques.....	20
5. Validation de l'analyse d'impact	23
5.1. Eléments utiles à la validation.....	23
5.1.1. Synthèse relative à la conformité au RGPD	23
5.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données.....	23
5.1.3. Cartographie des risques liés à la sécurité des données.....	24
5.1.3. Plan d'actions (si mesures correctives prévues) :	27
5.2. Validation formelle.....	27
6. Annexes	28

1. PRESENTATION GENERALE

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 ainsi qu'à l'article L. 223-1 du code de la sécurité intérieure.

Les personnes morales de droit privées, y compris les commerçants, peuvent mettre en œuvre de tels systèmes pour les finalités suivantes :

- La protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme ;
- La sécurité des personnes et des biens dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol ;
- La sécurité des personnes et des biens dans les lieux et établissements ouverts au public susceptibles d'être exposés à des actes de terrorisme.

Par ailleurs, les commerçants uniquement peuvent mettre en œuvre de tels systèmes pour assurer la protection des abords immédiats de leurs bâtiments et des installations dans les lieux particulièrement exposés à des risques d'agression ou de vol. Ces bâtiments et installations sont :

- les lieux ouverts au public où se déroulent les opérations de vente de biens ou de services ;
- les lieux où sont entreposés lesdits biens ou marchandises destinés à ces opérations de vente.

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 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.

L'installation des systèmes de vidéoprotection est subordonnée à une autorisation préfectorale donnée après avis d'une commission départementale.

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

2. PRESENTATION DU TRAITEMENT DES IMAGES

2.1 Vue d'ensemble

Finalités	<input type="checkbox"/>	La protection des abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme
	<input type="checkbox"/>	La sécurité des personnes et des biens dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol
	<input type="checkbox"/>	La sécurité des personnes et des biens dans les lieux et établissements ouverts au public susceptibles d'être exposés à des actes de terrorisme
	<input type="checkbox"/>	La protection des abords immédiats des bâtiments et des installations des commerçants dans les lieux particulièrement exposés à des risques d'agression ou de vol.
Identité et coordonnées du responsable de traitement	[Dénomination de la personne morale de droit privée + adresses postale et électronique].	
Le cas échéant, identité et coordonnées du Délégué à la protection des données	[A compléter]	
Régime juridique applicable	Titre II du RGPD	
Enjeux du traitement	<p>[Description concrète du besoin de recourir à un système de vidéoprotection].</p> <p>Les systèmes de vidéoprotection permettent aux personnes privées de sécuriser les abords ainsi que l'intérieur de leurs bâtiments et installations.</p> <p>En effet, la présence visible de caméras dans les lieux exposés à des risques d'agression ou de vol a un effet dissuasif. De plus, lorsque l'opérateur détecte un événement en direct, il peut en aviser immédiatement les autorités compétentes qui jugent de la suite à donner aux faits observés.</p> <p>Par ailleurs, de manière très circonscrite par la loi, de tels systèmes permettent également aux autorités publiques d'exercer leurs missions de surveillance et d'identification des auteurs d'infraction. En effet, les services de police peuvent être amenés à solliciter les opérateurs pour l'identification de personnes recherchées ou de véhicules impliqués dans des procédures judiciaires. 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.</p>	
Nombre de caméras	[Nombre de caméras]	
Sous-traitant(s)	[Dénomination + siège social des sous-traitants + objet du contrat (ex : maintenance/exploitation)]	

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, titre II Arrêté définissant les normes techniques prévu à l'article L. 252-4 du code de la sécurité intérieure

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

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 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 sur les abords immédiats des bâtiments et installations des personnes morales de droit privé, y compris les commerçants, pour les seules images issues de leur système de vidéoprotection			
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	[choisir oui ou non]	[A compléter]	Les images prises sur la voie publique
S'agissant des accédants visionnant des images prises sur la voie publique sur les abords immédiats des bâtiments et installations des commerçants			
Les agents des services de police nationale ; Les agents des unités de la gendarmerie nationale ; Les agents de police municipale ; Les agents de la ville de Paris chargés d'un service de police, agréés par le procureur de la République et assermentés, mentionnés aux articles L. 531-1, L. 532-1 et L. 533-1.	[choisir oui ou non]	[A compléter]	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, 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 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 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	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 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
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	<p>[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 :</p> <ul style="list-style-type: none"> - 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, 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...] <p>[Indiquer si le système est supervisé ou non, les plages horaires].</p>	[A compléter]
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 : Sécurité des personnes et des biens dans les lieux et établissements particulièrement exposés à des risques d'agression ou de vol]	[Par exemple : agression ou vols 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.

La détermination de la base de licéité des traitements d'images dépend de leur finalité et de la qualité du responsable du système. Ainsi, 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, soit le f 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.	[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)]
Jour et plages horaires d'enregistrement.	
Lieu où ont été collectées les données.	

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	[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.
Jour et plages horaires d'enregistrement.			
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 panneaux comportant un pictogramme représentant une caméra.

Les informations prévues à l'article 14 du règlement (UE) 2016/679 du 27 avril 2016 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 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 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 15 du règlement (UE) 2016/679 du 27 avril 2016 s'exerce directement auprès du responsable de traitement.

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

Les droits de rectification et d'effacement prévus aux articles 16 et 17 du règlement (UE) 2016/679 du 27 avril 2016 s'exercent directement auprès du responsable de traitement.

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

Le droit à la limitation prévu à l'article 18 du règlement (UE) 2016/679 du 27 avril 2016 s'exerce directement auprès du responsable de traitement.

Conformément 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 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

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

4. ETUDE DES RISQUES LIES A LA SECURITE DES DONNEES

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	<p>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.</p> <p>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.</p>	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/a 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/a améliorable	

Archivage	<p>[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.)]</p> <p>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</p>	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	<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	
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	
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	
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/a méliorable	
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	Acceptable	

	PC ou équipements se connectant à cet équipement. Les logs des firewalls sont conservés trois ans.		
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/a améliorable	
Politique (gestion des règles)	Formation, charte informatique, règles de gestion des habilitations des administrateur, agents habilités et leurs profils	Acceptable	
Gestion des risques	Tracabilité 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/a améliorable	
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. 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.]	Acceptable	
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/a méliorable	
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	<p>Usurpation ou divulgation de mot de passe</p> <p>Action interne par un personnel</p> <p>Cyberattaque automatisée (virus) ou volontaire par ingénierie sociale.</p> <p>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</p> <p>Vol du matériel par un tiers</p>	<p>Mauvaise gouvernance</p> <p>Intégrité et confidentialité des données.</p> <p>Effacement des données</p> <p>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</p> <p>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</p> <p>Discrédit de l'usage du dispositif</p> <p>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>

Analyse d'impact relative à la protection des données

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.	<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.</p> <p>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</p> <p>Risque de dégradations de biens en représailles ou de violence pour une personne injustement mise en cause</p> <p>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.</p> <p>Information des personnels sur la gestion de données critiques.</p> <p>Sauvegarde des données</p>	Importante mais une modification des images captées serait nécessairement détectée car portant atteinte à l'intégrité de la donnée.	Limitée
---	---	---	--	---	---	---------

Analyse d'impact relative à la protection des données

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>	<p>Limitée</p>
-------------------------------	---	---	---	---	---	----------------

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

Analyse d'impact relative à la protection des données

	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	<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.) 	<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
-------------------	---	---	--	---

			<ul style="list-style-type: none"> Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) Profilage imprécis ou abusif 	
3. Importante	<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 irrémissible 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 irréremédiables, 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).

DÉCLARATION SIMPLIFIÉE

ENGAGEMENT DE CONFORMITÉ

(Articles 24-I, 25-II, 26-IV et 27-III de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004)

1 Déclarant

- ☐ Vous êtes un organisme (personne morale)
☐ Vous êtes une personne physique

* Champs obligatoires

Nom et prénom ou raison sociale*

Signature (facultatif)

N° SIRET*

Service

Adresse*

Code postal*

Ville*

Adresse électronique*

Code APE*

Téléphone*

Fax

Personne destinataire du récépissé et contact au sein de l'organisme déclarant si un complément d'information doit être demandé :

Nom et prénom*

Adresse électronique*

2 Texte de référence*

Vous déclarez par la présente que votre traitement est strictement conforme aux règles énoncées dans le texte de référence. Veuillez sélectionner la case correspondant à votre situation (plusieurs choix sont possibles) et préciser le n° de référence du texte :

Nature du texte	N° de référence	N° de référence	N° de référence	N° de référence	N° de référence
<input type="checkbox"/> Norme simplifiée	NS - [] [] [] []	NS - [] [] [] []	NS - [] [] [] []	NS - [] [] [] []	NS - [] [] [] []
<input type="checkbox"/> Autorisation unique	AU - [] [] [] []	AU - [] [] [] []	AU - [] [] [] []	AU - [] [] [] []	AU - [] [] [] []
<input type="checkbox"/> Acte réglementaire unique	RU - [] [] [] []	RU - [] [] [] []	RU - [] [] [] []	RU - [] [] [] []	RU - [] [] [] []
<input type="checkbox"/> Méthodologie de référence	MR - [] [] [] []	MR - [] [] [] []	MR - [] [] [] []	MR - [] [] [] []	MR - [] [] [] []
<input type="checkbox"/> Autorisation unique - BCR	BCR - [] [] [] []	BCR - [] [] [] []	BCR - [] [] [] []	BCR - [] [] [] []	BCR - [] [] [] []

3 Transferts de données hors de l'Union Européenne*

Vous transférez tout ou partie des données enregistrées dans votre traitement vers organisme (filiale, maison mère, prestataire de service, etc.) qui se trouve dans un pays situé hors de l'Union Européenne :

- ☐ Non ☐ Oui

4 Signature

Personne responsable de l'organisme déclarant :

Nom et prénom*

Date* / /

Fonction

Signature

Adresse électronique*

Les informations recueillies font l'objet d'un traitement informatique destiné à permettre à la CNIL l'instruction des déclarations qu'elle reçoit. Elles sont destinées aux membres et services de la CNIL. Certaines données figurant dans ce formulaire sont mises à disposition du public en application de l'article 31 de la loi du 6 janvier 1978 modifiée. Vous pouvez exercer votre droit d'accès et de rectification aux informations qui vous concernent en vous adressant à la CNIL : 3 Place de Fontenoy - TSA 80715 - 75334 PARIS Cedex 07.



DEMANDE D'AUTORISATION D'UN SYSTÈME DE VIDÉOPROTECTION

13806*04

Articles L.223-1 à L.223-9, L.251-1 à L.255-1, L.613-13 et R.223-1 à R.223-2, R.251-1 à R.254-2 du code de la sécurité intérieure

Veuillez indiquer dans la case ci-après le numéro du département de la préfecture compétente (il s'agit du département dans lequel vous souhaitez installer votre système de vidéoprotection sauf s'il s'agit d'un système en réseau couvrant plusieurs départements auquel cas vous devez saisir la préfecture du département où est installé le siège social).		PARTIE RESERVEE A L'ADMINISTRATION	
1 - NATURE DE LA DEMANDE			
<input type="checkbox"/> Demande d'autorisation d'un nouveau système		DATE D'ARRIVEE :	
<input type="checkbox"/> Modification d'un système autorisé	N° de dossier	RECEPISSE DELIVRE LE :	
<input type="checkbox"/> Demande de renouvellement d'un système autorisé	N° de dossier	DATE DE LA DECISION :	

2 - IDENTITÉ DU DÉCLARANT ET DU RESPONSABLE DU SYSTÈME

Nom de naissance :
Prénom : Fonction :
Dénomination de la collectivité territoriale ou la raison sociale de l'établissement ou de l'entreprise :
Eventuellement nom usuel ou sigle (si différent de la raison sociale) :
Activité :
Adresse : Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie
Code postal : Commune :
Téléphone : Mail :
Nom de la personne à contacter pour la mise à disposition des images aux forces de l'ordre :
Téléphone :

3 - INFORMATIONS GÉNÉRALES ET FINALITÉ DU SYSTÈME DE VIDÉOPROTECTION (Attention les personnes de droit privé ne peuvent poursuivre que les finalités de prévention à la sécurité des personnes et des biens, ainsi que de protection des abords immédiats de leurs bâtiments et installation dans les lieux et établissements particulièrement exposés à des risques d'agressions et de vol ou susceptibles d'être exposés à des actes de terrorisme)

a) Informations générales

Horaires d'ouverture (pour les établissements ouverts au public) :

A préciser le cas échéant, (descriptions des éventuelles agressions survenues ou risques à prendre en compte) :

b) Finalité(s) du système (veuillez cocher la ou les cases correspondantes) :

- | | |
|--|---|
| <input type="checkbox"/> Protection des bâtiments et installations publics et de leurs abords | <input type="checkbox"/> Prévention d'actes de terrorisme |
| <input type="checkbox"/> Sauvegarde des installations utiles à la défense nationale | <input type="checkbox"/> Prévention des risques naturels ou technologiques |
| <input type="checkbox"/> Régulation des flux transport | <input type="checkbox"/> Secours aux personnes et la défense contre l'incendie |
| <input type="checkbox"/> Constatation des infractions aux règles de la circulation | <input type="checkbox"/> Sécurité des installations accueillant du public dans les parcs d'attraction |
| <input type="checkbox"/> Prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression et de vol ou de trafic de stupéfiant | |
| <input type="checkbox"/> Prévention des fraudes douanières prévues par le dernier alinéa de l'article 414 du code des douanes dans des zones particulièrement exposées à ces infractions | |
| <input type="checkbox"/> Obligation d'être couvert par une assurance pour faire circuler un véhicule terrestre à moteur (responsabilité civile) | |
| <input type="checkbox"/> Prévention et constatation des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets | |
| <input type="checkbox"/> Prévention des atteintes à la sécurité des personnes et des biens dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol | |
| <input type="checkbox"/> Protection des abords immédiats des bâtiments et des installations de lieux et établissements relevant d'une personne morale de droit privé exposés à des actes de terrorisme | |
| <input type="checkbox"/> Protection des abords immédiats des bâtiments et des installations des commerçants dans des lieux exposés à des risques d'agression et de vol | |
| <input type="checkbox"/> Autre (préciser) : | |

4 - LOCALISATION DU SYSTÈME DE VIDÉOPROTECTION (Veuillez renseigner uniquement une des deux rubriques ci-dessous)

4-1) LIEU D'INSTALLATION ET NOMBRE DE CAMÉRAS (cette rubrique n'est pas à renseigner pour les demandes portant sur un périmètre vidéoprotégé, dans ce cas vous ne devez renseigner que la rubrique 4-2)

Adresse : Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie Code postal Commune

.....

Nombre de caméras intérieures:

Il s'agit des caméras installées à l'intérieur d'un établissement :
joindre le cas échéant le plan de détail et le plan de masse

Nombre de caméras extérieures:

Il s'agit des caméras installées dans un lieu ouvert au public non couvert ou sur un bâtiment et qui ne visionnent pas la voie publique : joindre le cas échéant le plan de détail et le plan de masse (cf notice)

Le cas échéant, nombre de caméras visionnant la voie publique:

Pour les systèmes de moins de 8 caméras installées à l'intérieur d'un établissement ouvert au public, veuillez indiquer ci après la superficie de l'établissement :m²

4-2) DEMANDE PORTANT SUR UN PÉRIMÈTRE VIDÉOPROTÉGÉ (cette rubrique ne doit être renseignée que si vous souhaitez avoir recours à la notion de périmètre vidéoprotégé)

Si au moins une des caméras que vous souhaitez installer doit visualiser la voie publique, veuillez cocher la case ci-après ☐

Délimitation du périmètre : pour délimiter ce périmètre, veuillez indiquer ci-après les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre.

Adresse : Numéro de voie	Extension (bis, ter...)	Type de voie (rue, av...)	Nom de la voie	Code postal	Commune
.....
.....
.....
.....
.....
.....
.....

5 - CARACTÉRISTIQUES DU SYSTÈME

Délai de conservation des images (exprimé en jours) : (Indiquez un nombre compris entre 0 et 30)
(la durée maximale est de 30 jours)

Existence d'un système de retransmission des images : ☐ oui ☐ non

si oui, veuillez cocher la case correspondante ci-dessous

Retransmission en temps réel :

☐

Retransmission en temps différé :

☐

Le système de vidéoprotection est-il mis en place par un installateur certifié ? ☐ oui ☐ non

si oui, veuillez indiquer ci-dessous le nom de cet installateur ou de cette société d'installation ainsi que son numéro de certification.

Nom de l'installateur ou de la société : Numéro de certification:.....

Cet installateur vous a-t-il remis une attestation de conformité aux normes techniques définies par l'arrêté mentionné à l'article R.252-3, 11° du Code de la sécurité intérieur ☐ oui ☐ non

Si l'installateur n'est pas certifié, veuillez joindre un questionnaire précisant les caractéristiques techniques du dispositif et sa conformité aux normes techniques définies par l'arrêté mentionné à l'article R.252-3, 11° du Code de la sécurité intérieur

6 - PERSONNES HABILITÉES A ACCÉDER AUX IMAGES :

NOM :Prénom :Fonctions :

NOM :Prénom :Fonctions :

NOM :Prénom :Fonctions :

NOM :Prénom :Fonctions :

Une de ces personnes habilitées relève-t-elle d'une société privée délégataire : ☐ oui ☐ non

si plus de quatre personnes, vous pouvez adresser (par courrier ou sous forme électronique) une liste complémentaire.

7 - EXPLOITATION DES IMAGES (cette rubrique n'est à renseigner que si les images font l'objet d'un traitement dans un lieu différent de celui de l'implantation du système et/ou par une personne autre que le responsable du système)

Adresse du lieu de traitement à renseigner ci-après :

Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie Code postal Commune

.....

Si ce traitement est effectué par un service, veuillez indiquer ci-après le nom du service :

Si ce traitement est effectué par une personne, veuillez indiquer ci-après ses noms et prénoms :

8 - SÉCURITÉ ET CONFIDENTIALITÉ

(nous vous remercions de décrire ci-dessous les mesures adoptées pour assurer la confidentialité des images)

Mesures prises pour contrôler l'accès au poste central de surveillance (par exemple code d'accès, porte blindée, accès contrôlé...) :

.....

Si existence d'un système d'enregistrement :

Mesures pour la sauvegarde et la protection de ces enregistrements :

.....

Modalités de destructions des enregistrements :

.....

9 - MODALITÉS D'INFORMATION DU PUBLIC

Veuillez indiquer ci-après le nombre d'affiches ou de panonceaux d'information :

Précisez la (ou les) localisation(s) de cet affichage :

10 - SERVICE (OU PERSONNE) AUPRÈS DUQUEL S'EXERCE LE DROIT D'ACCÈS

Nom :Prénom : Fonction de cette personne :

ou service responsable : Téléphone :

Veuillez renseigner ci-après l'adresse de cette personne ou de ce service :

Numéro de voie Extension (bis, ter...) Type de voie (rue, av...) Nom de la voie Code postal Commune

Fonction habilitant le déclarant à signer :

Le signataire s'engage à se conformer aux articles du code de la sécurité intérieure relatifs à la vidéoprotection

SIGNATURE ET CACHET :

Date :

Conformément aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le demandeur est informé que les renseignements qu'il doit fournir pour satisfaire sa demande font l'objet d'un traitement automatisé par la préfecture du lieu de dépôt de son dossier. Le droit d'accès et de rectification s'exercera auprès de cette préfecture..

NOTICE D'INFORMATION

relative au formulaire CERFA n° 13806*03 et 14095*02

Demande d'autorisation d'un système de vidéoprotection

A) Informations générales

A-1) L'encadrement juridique :

L'usage de la vidéoprotection est régi par **les articles L.223-1 à L.223-9, L.251-1 à L.255-1 et L.613-13 du code de la sécurité intérieure et par le décret d'application n°96-926 du 17 octobre 1996**. Les conditions d'application de ces textes sont explicitées par les circulaires : **INTD9600124C du 22 octobre 1996, INTD0600096C du 26 octobre 2006 et INTK0930018J du 2 février 2009**.

Dans les lieux privatifs ou les locaux à usage exclusivement professionnel qui n'accueillent pas de public au sens de la loi, la réglementation de la vidéoprotection mentionnée ci-dessus n'est pas applicable. La mise en place éventuelle de caméras doit cependant s'effectuer dans le respect de la vie privée et sans visionner la voie publique.

Les dispositions générales du code civil sur le droit à l'image (article 9) ou des réglementations particulières, telle que celle du code du travail (**3^{ème} alinéa de l'article L. 2223-32 et articles L. 1222-4 et L.1221-9**) sont alors applicables.

L'article 226-1 du code pénal punit d'un an d'emprisonnement et de 45 000 € d'amende toute personne ayant volontairement porté atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant l'image d'une personne se trouvant dans un lieu privé, c'est-à-dire, selon la jurisprudence, un lieu qui n'est ouvert à personne sauf autorisation de celui qui l'occupe d'une manière permanente ou temporaire.

Dans les cas très rares où le système de vidéoprotection est relié à un traitement de données automatisées (fichier de données à caractère personnel), la loi « informatique et libertés » n°78-17 du 6 janvier 1978 est alors applicable. Dans ce cas précis, vous devez adresser une déclaration spécifique à la CNIL. (En cas de doute n'hésitez pas à poser votre question à l'adresse ci-après, une réponse vous sera adressée en retour dans les 10 jours : videoprotection@interieur.gouv.fr. Vous pouvez également prendre contact avec l'accueil de la préfecture qui instruira votre demande).

A-2) Dans quels cas devez vous déposer une demande d'autorisation ?

➤ **DANS LE CAS D'UN SYSTÈME VISÉ PAR LA LOI INSTALLÉ EN VOIE PUBLIQUE OU DANS UN LIEU OU UN ÉTABLISSEMENT OUVERT AU PUBLIC :**

1) Quel système est visé par la loi ?

Il y a une vidéoprotection toutes les fois que sont mis en œuvre au moins une caméra et un moniteur, c'est-à-dire un écran permettant la visualisation des images, même s'ils ne sont pas situés dans le même local, et lorsque les caméras, fixes ou mobiles, fonctionnent de manière permanente ou non, prennent des images, éventuellement de manière séquentielle ou aléatoire, qui peuvent être visionnées, en temps réel ou en différé, sur place ou dans un lieu distant, sur un écran de type télévision ou sur un écran d'ordinateur.

Ainsi, la prise de photographies n'est pas un système de vidéoprotection et ce, quelque soit la technique utilisée (appareil numérique). Par contre, un dispositif dans lequel des images sont enregistrées à l'occasion d'une intrusion ayant déclenché le fonctionnement de caméras, dans un poste de contrôle éloigné, correspond bien à la définition de la vidéoprotection. Dans ce cas, le dispositif participe en outre des activités dites de télésurveillance régies par les dispositions du livre VI du CSI.

La loi ne se prononce pas sur la technologie utilisée. Elle définit seulement les principales modalités de fonctionnement des systèmes et fixe des normes techniques (par arrêté du 3 août 2007- annexes techniques publiées au JO du 25 août 2007). Cette absence de détermination précise des caractéristiques des dispositifs de vidéoprotection a permis d'accompagner le développement des nouvelles technologies et d'appliquer la réglementation à des cas auxquels le législateur ne pouvait penser en 1995 (ex : utilisation des webcams).

Ainsi, les systèmes de vidéoprotection numériques dont les images sont transmises par internet et consultées, à distance, par les personnes responsables du système entrent dans le champ des dispositions du CSI. Le procédé numérique doit permettre le respect des garanties imposées par la loi.

Par contre, la diffusion sur internet d'images issues de webcams ne constitue pas un dispositif de vidéoprotection dans la mesure où il n'y a pas « visionnage » des images sur un écran appartenant au propriétaire de la webcam mais transmission directe sur internet.

2) Les lieux visés par la Loi :

Les dispositions du CSI relatives à la vidéoprotection déterminent les lieux dans lesquels un dispositif de vidéoprotection peut être installé. Il s'agit de :

- l'intérieur des **lieux et établissements ouverts au public** ;
- la **voie publique** limitée géographiquement :
- aux abords des bâtiments et installations publics ;
- aux abords immédiats des bâtiments et installations appartenant à des personnes physiques ou morales de droit privé en cas de risque d'attentat terroriste ;
- aux voies de circulation.

Concernant la voie publique, la vidéoprotection peut être mise en œuvre :

- par une personne publique, pour assurer soit la protection des bâtiments et installations publics et de leurs abords ; soit la sauvegarde des installations utiles à la défense nationale ; soit la régulation des flux de transport ; soit la constatation des infractions aux règles de la circulation ; soit 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 second 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 ; soit la prévention d'actes de terrorisme ; soit la prévention des risques naturels ou technologiques ; soit le secours aux personnes et la défense contre l'incendie ; soit la sécurité des installations accueillant du public dans les parcs d'attraction.

- par une personne physique ou morale de droit privé pour visionner les abords immédiats de ses bâtiments ou installations (article L 223-1 du CSI) au titre de la finalité de prévention d'actes de terrorisme ;

- dans certains lieux revêtant une dimension ou une complexité particulières, le préfet peut autoriser qu'un périmètre de voie publique ou compris dans un établissement ou un lieu ouvert au public puisse être vidéoprotégé, dans les limites et le cadre des finalités imposées par la loi. Cette notion répond à une nécessité opérationnelle d'adaptation de la vidéoprotection puisqu'elle recouvre l'espace susceptible d'être situé dans le champ d'une ou plusieurs caméras.

Sont visées par la notion d'ensemble immobilier ou foncier complexe les lieux ouverts au public dans des zones à forte concentration urbaine ou touristique ou dont la configuration géographique et architecturale rend difficile l'intervention des services de sécurité ou de secours mais également dans des zones utilisées dans le cadre de manifestations exceptionnelles. Pourraient entrer dans ce champ, à titre d'exemple : la place de la Concorde, une cité composée de plusieurs immeubles à usage d'habitation, une zone rurale utilisée dans le cadre d'une manifestation d'une ampleur exceptionnelle, comme une rave-party.

A-3) Quels documents devez-vous joindre à votre demande et dans quels cas ?

1) Les documents constitutifs d'une demande d'autorisation :

L'ensemble des documents décrits ci-dessous ne sont pas exigibles dans tous les cas. Veuillez vous reporter au 2) afin d'identifier précisément la nature de votre demande.

- Le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires le CERFA n° 14095*02 ;

- Le rapport de présentation : il s'agit d'un rapport spécial expliquant les finalités du projet au regard des objectifs définis par la loi et les techniques mises en œuvre, eu égard à la nature de l'activité exercée, aux risques d'agression ou de vol présentés par le lieu ou l'établissement à protéger ;

- Le plan de masse : Il s'agit d'un plan des lieux montrant les bâtiments du demandeur et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures ;

- Le plan de détail : Il s'agit d'un plan à une échelle suffisante montrant le nombre, le positionnement des caméras ainsi que les zones couvertes par celles-ci ;

- Un plan du périmètre : Il s'agit d'un document qui peut se substituer au plan de détails et au plan de masse, montrant l'espace susceptible d'être situé dans le champ de vision d'une ou plusieurs caméras dans le cas d'une demande portant sur un périmètre à vidéoprotéger ;

- La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images : théoriquement ces informations sont indiquées dans les parties 5, 7 et 8 du formulaire mais en cas de dispositif élaboré notamment en cas de traitement par une société extérieure, un document expliquant le fonctionnement du système peut-être demandé.

- La désignation des personnes susceptibles d'accéder aux images (rubrique 6 du formulaire) : il s'agit de toute personne habilitée par le responsable à accéder aux images et donc susceptible de les visionner (il peut s'agir bien sûr du responsable lui-même mais aussi du technicien de maintenance par exemple). Ce n'est que dans l'hypothèse où plus de 4 personnes sont habilitées à accéder aux images qu'il convient de joindre une liste complémentaire au formulaire de demande.

Dans l'hypothèse où une des personnes habilitée à accéder aux images relève d'une société privée agissant par délégation, il convient de joindre l'agrément de ce prestataire

- Modèle de l'affiche ou du panneau d'information du public : les panneaux destinés à informer d'un système sur la voie publique doivent comporter un pictogramme (dessin) représentant une caméra. Si les affiches ou panneaux sont placés dans les lieux et établissements ouverts au public, le nom ou la qualité, ainsi que le numéro de téléphone du responsable auprès duquel toute personne intéressée peut s'adresser pour exercer son droit d'accès doivent y figurer.

Attestation de la conformité du système aux normes techniques définies par l'arrêté du 3 août 2007 : deux cas de figure se présentent. En fonction de l'installateur auquel vous aurez recouru vous devrez produire un des documents prévus à cet effet :

- 1) Si vous avez fait appel à un installateur certifié : une attestation de conformité établie par ce dernier suffit.
- 2) Si votre installateur n'est pas certifié : il vous faut produire un questionnaire précisant les caractéristiques techniques du dispositif et sa conformité aux normes techniques (voir modèle joint en Annexe 1).

2) Les documents à fournir en fonction des différents cas suivants :

Vidéoprotection de la voie publique avec désignation du nombre de caméras : veuillez joindre à votre dossier tous les documents énumérés en 1) (sauf le plan du périmètre qui ne concerne que les cas de vidéoprotection d'un périmètre).

Vidéoprotection d'un périmètre (en voie publique ou dans un lieu ouvert au public) : veuillez fournir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n° 14095*02, le rapport de présentation, le modèle d'affiche et/ou de panneau d'information du public, le plan du périmètre, le justificatif de la conformité aux normes techniques (attestation de conformité par un installateur certifié ou questionnaire dans l'autre cas), description du dispositif (dans ce cas de figure ce descriptif sera limité aux techniques employées et aux modes de visionnage et d'exploitation des images **le nombre de caméras et leur emplacement n'auront pas à être indiqués**). Eventuellement la liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéoprotection dans un lieu ou un établissement ouvert au public et 7 caméras maximum : le dossier dans ce cas est très simplifié : veuillez fournir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n° 14095*02, l'affiche d'information et le justificatif de conformité si l'installateur n'est pas certifié (si vous avez fait appel à un installateur certifié, vous devez pouvoir produire son attestation en cas de contrôle mais n'êtes pas obligé de la transmettre dans le cas où vous effectuez votre déclaration par téléprocédure), éventuellement liste complémentaire des personnes habilitées à accéder aux images si la partie 6 du formulaire ne suffit pas.

Vidéoprotection dans un lieu ou un établissement ouvert au public et 8 caméras minimum : veuillez fournir le formulaire CERFA n° 13806*03 ou, pour les établissements bancaires, le CERFA n° 14095*02, le rapport de présentation, le plan de détail, l'affiche d'information du public et le justificatif de conformité, éventuellement la liste complémentaire des personnes habilitées à accéder aux images si la rubrique 6 du formulaire ne suffit pas.

A-4) A qui devez-vous adresser votre dossier ?

A la préfecture du département dans lequel vous souhaitez installer le dispositif (par exemple pour une société dont le déclarant est à Paris mais qui veut installer un dispositif dans une de ses succursales située en Gironde, il faut adresser votre déclaration à la préfecture de Bordeaux). Dans le cas d'un dispositif qui concernerait plusieurs départements (exemple : réseau autoroutier), le dossier doit être déposé à la préfecture du siège de l'établissement demandeur.

Ce dossier peut être transmis soit sous forme papier par voie postale ou déposé à l'accueil de la préfecture qui instruira votre demande, soit par téléprocédure disponible sur le site «videoprotection.interieur.gouv.fr» qui propose par ailleurs un ensemble d'informations ou d'actualités sur le sujet de la vidéo protection.

B) Comment remplir le formulaire de demande d'autorisation ?

Vous devez indiquer le numéro du département où se trouve la préfecture compétente en complétant par trois chiffres la case prévue à cet effet en haut du formulaire CERFA (par exemple pour PARIS renseigner 075, pour Marseille indiquer 013).

Rubrique 1 - Nature de la demande

Veuillez cocher obligatoirement une des trois cases proposées correspondant à la nature de votre demande (par exemple s'il s'agit d'une première demande vous cocherez «demande initiale»).

En cas de demande de modification d'un dispositif existant ou de demande de renouvellement, préciser le numéro de dossier sous lequel il a été enregistré dans la partie prévue à cet effet.

La modification peut concerner par exemple l'augmentation du nombre de caméras ou la localisation de celles-ci, sauf, si l'autorisation obtenue portait sur un périmètre vidéoprotégé. Dans ce dernier cas vous devez simplement déclarer au préfet compétent soit par courrier soit par téléprocédure (sur le site «videoprotection.interieur.gouv.fr» à la rubrique «TELE-VIDEOPROTECTION» dans le menu «déclaration de mise en service») le nouveau positionnement de vos caméras. Si vous souhaitez, en revanche, modifier la définition du périmètre (changement de l'environnement de celui-ci), vous devez adresser une demande de modification complétée des documents nécessaires.

Rubriques 2 et 10 - Identité et fonction du déclarant

L'autorisation de mise en œuvre d'un système de vidéoprotection est délivrée à la personne responsable du système, c'est-à-dire à celle qui, ayant la capacité juridique pour ce faire, estime nécessaire de recourir à la vidéoprotection. L'obligation de déclaration des systèmes entrant dans le champ d'application des dispositions du CSI incombe à l'exploitant des lieux où sont installées les caméras, qu'il soit ou non le propriétaire des lieux et même lorsque le système de vidéoprotection n'est installé que pour une durée limitée. Le responsable n'est donc pas l'installateur.

Vous devez par conséquent impérativement compléter les informations relatives au nom, prénom et fonction du déclarant (la fonction se trouve à la rubrique 10 en fin de formulaire) **(Si par la suite, le responsable du système change, par exemple suite à une mutation ou un départ à la retraite, il faudra en aviser la préfecture, dans certains cas ce changement peut nécessiter une nouvelle demande d'autorisation ; la préfecture vous le précisera).**

Veillez ensuite renseigner la dénomination (il peut s'agir d'une collectivité exemple : commune de XXX, d'une entreprise exemple : – SARL XXX- , d'un établissement privé ou public exemple : bibliothèque municipale de XXX ; ou institut XXX)

S'il existe un nom usuel différent de ce que vous avez indiqué, il est recommandé de l'indiquer à la ligne suivante qui reste une information facultative.

Concernant l'activité, elle doit être impérativement renseignée si la demande concerne une entreprise ou un lieu ouvert au public (exemple : musée, commerce de vêtements...).

Vous complèterez ensuite l'adresse de la collectivité, de l'établissement ou de l'entreprise (veuillez renseigner le plus précisément possible cette adresse en complétant toutes les rubriques proposées).

L'adresse électronique reste facultative, il est conseillé toutefois de la mentionner afin de faciliter les échanges le cas échéant, entre l'administration et le demandeur.

Rubrique 3 - Informations générales et finalité(s) du système de vidéoprotection

a) les informations générales :

Dans cette rubrique, vous devez compléter la partie relative aux horaires d'ouverture **sauf en cas de vidéoprotection sur la voie publique** (par exemple si vous déposez un dossier pour un commerce, cette information peut vous être réclamée en complément si vous ne la renseignez pas dès le départ).

De même, vous êtes invité à signaler les éventuelles agressions déjà survenues sur le lieu que vous souhaitez protéger ou les risques particuliers auxquels vous l'estimez exposé (délinquance de proximité, commerce recevant beaucoup de liquidités).

b) la ou les finalité(s) du système :

Veillez cocher obligatoirement au moins l'une des cases proposées. Vous pouvez en cocher plusieurs, la finalité du système n'étant pas nécessairement unique. Si vous cochez la case «autre», vous devez préciser sur la ligne suivante le but que vous recherchez en installant un système de vidéoprotection.

Rubrique 4 - Localisation du système de vidéoprotection

Veillez compléter soit la rubrique 4-1, soit la rubrique 4-2. En aucun cas vous ne pouvez compléter les deux rubriques en même temps (la rubrique 4-2 concerne uniquement les ensembles immobiliers ou fonciers de dimension importante ou complexes).

4-1 Lieu d'installation et nombre de caméras

Veillez compléter le plus précisément possible l'adresse du lieu d'installation du dispositif (en cas d'installation sur la voie publique de plusieurs caméras réparties sur une certaine distance, veuillez indiquer au moins le nom de la voie).

Pour les dispositifs de 7 caméras maximum installées à l'intérieur d'un établissement, vous préciserez impérativement la superficie de cet espace intérieur.

4-2 Demande portant sur un périmètre

Il est possible, lorsque l'installation de vidéoprotection est prévue sur un ensemble foncier ou immobilier de dimension importante ou complexe, de recourir à la notion de périmètre vidéo protégé.

Cette formule présente l'avantage de vous dispenser du dépôt de demande de modification pour déplacer les caméras ou en augmenter le nombre à l'intérieur du périmètre.

Si vous souhaitez obtenir une autorisation au titre d'un périmètre vidéo protégé, veuillez préciser les différentes adresses (8 au maximum) qui constituent l'environnement de ce périmètre (par exemple si vous souhaitez une autorisation pour protéger une gare, vous préciserez à la rubrique 2 l'activité « gare » et indiquerez toutes les adresses permettant de délimiter le périmètre géographique dans lequel se trouve située cette gare).

Dans cette hypothèse c'est au moment où vous informerez le préfet de la mise en service des caméras que vous lui en préciserez la localisation.

Rubrique 5 - Caractéristiques du système

Vous devez préciser impérativement le nombre de jours pendant lesquels seront conservées les images. Ce chiffre (de 00 à 30 jours, délai de conservation maximum autorisé par la loi) sera reporté dans la case correspondante.

Vous répondrez ensuite à la question «existence d'un système de retransmission». Si vous cochez non, vous pouvez passer à la question relative à l'installateur. Si vous répondez oui, vous devrez cocher obligatoirement une des deux cases suivantes : retransmission en temps réel ou retransmission en temps différé.

Veillez ensuite préciser, en cochant la case correspondante, si l'installateur auquel vous avez fait appel est certifié.

Si vous avez coché la case «oui» et que cet installateur est certifié par l'AFNOR-CNPP ou par un mécanisme de certification équivalent, Il faut mentionner le nom de cet installateur (ou de cette société d'installation) et son numéro de certification. Vous répondrez également à la question suivante en cochant «oui» ou «non». Si l'installateur vous a remis une attestation, vous n'êtes pas obligé de la joindre à votre dossier (pour les dispositifs importants de plus de 7 caméras ou en voie publique, il est toutefois conseillé de la joindre ; pour les petits dispositifs hors voie publique de 7 caméras maximum, vous n'êtes pas obligé de joindre au dossier cette attestation mais elle peut vous être réclamée en cas de contrôle a posteriori).

Si l'installateur n'est pas certifié, vous joindrez au dossier le questionnaire (dont le modèle figure, en annexe 1) précisant les caractéristiques du système.

Rubrique 6 - Personnes habilitées à accéder aux images

Il s'agit de mentionner le nom et prénoms des personnes qui seront en charge de visionner les images ou qui peuvent y accéder (s'il s'agit du responsable-déclarant de la demande d'autorisation lui-même, il convient de le préciser en réécrivant ses nom, prénoms et fonction qui devront dans ce cas correspondre aux informations contenues à la rubrique 2 et 10. De même, le ou les techniciens susceptibles d'intervenir sur le système au titre de la maintenance doivent être mentionnés dans cette liste. S'il y a plus de quatre personnes, il convient de joindre une liste complémentaire).

Si la ou les personnes habilitées à accéder aux images relèvent d'une société privée agissant par délégation, vous devez impérativement cocher la case « oui » prévue à cet effet.

En cas de modification de la liste des personnes habilitées, le signataire informera l'autorité préfectorale (soit par courrier, soit par « téléprocédure »).

Rubrique 7 - Traitement des images

Cette rubrique doit être renseignée dans le cas où les images font l'objet d'un traitement dans un lieu différent de celui de l'implantation des caméras et/ou par une personne autre que les responsables du système. Si ce n'est pas le cas, vous devez passer à la rubrique 8.

Rubrique 8 - Sécurité et confidentialité

La première ligne de cette rubrique doit impérativement être renseignée, il s'agit de décrire les mesures prises pour contrôler l'accès au poste central (code d'accès, porte blindée, badge d'accès, accès contrôlé).

Si vous avez coché la réponse «oui» à la question «existence d'un système d'enregistrement» en rubrique 5, veuillez répondre aux deux questions suivantes en décrivant 1) les mesures pour la sauvegarde et la protection des enregistrements (par exemple : armoire blindée) et 2) les modalités de destruction de ces enregistrements (par exemple : écrasement).

Rubrique 9 - Modalités d'information du public

Les textes en vigueur prévoyant l'obligation d'informer le public susceptible d'être filmé, vous préciserez les mesures prévues à cet effet.

Vous devez par conséquent compléter les deux lignes prévues dans cette rubrique.

Par ailleurs l'information sur l'existence d'un système de vidéoprotection devant être apportée au moyen de panoneaux comportant un pictogramme représentant une caméra (dans les cas de vidéoprotection sur la voie publique) et au moyen d'affiches ou de panoneaux (au choix en cas de vidéoprotection dans un lieu ou établissement recevant du public), n'oubliez pas de joindre à votre dossier le modèle d'affiche ou de panonceau.

Rubrique 10 - Service (ou personne) auprès duquel s'exerce le droit d'accès

L'article L.253-5 du code de la sécurité intérieure énonce :

«Toute personne intéressée peut s'adresser au responsable d'un système de vidéoprotection afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit. Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers.»

Il s'agit de préciser auprès de quelle personne ou de quel service doit s'adresser une personne ayant été filmée par le dispositif que vous souhaitez installer pour vérifier les images.

Il vous appartient par conséquent de renseigner cette rubrique en indiquant soit le nom, prénom et fonction de la personne auprès de laquelle s'exerce ce droit d'accès aux images, soit le nom du service.

Vous pouvez compléter éventuellement ces quatre informations (nom, prénom, fonction, service auquel appartient cette personne).

Vous indiquerez ensuite l'adresse de cette personne et/ou de ce service (cela peut être la même personne que le déclarant-responsable du système).

La signature du formulaire

Veuillez, une fois les rubriques complétées, indiquer la fonction du signataire-déclarant (rubrique 2 du formulaire, page 4 de la présente notice), dater votre document et le signer en apposant, le cas échéant le cachet de la collectivité, de l'établissement ou de l'entreprise.

Si vous effectuez votre déclaration par téléprocédure, vous complèterez simplement la mention relative à la fonction du déclarant.

Questionnaire de conformité d'un système de vidéoprotection à l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéoprotection.

Je soussigné(e)....., certifie par la présente que le système de vidéoprotection pour lequel j'ai sollicité une autorisation en date du....., installé par (nom et adresse de l'installateur).... est conforme aux dispositions de l'arrêté du 3 août 2007.

Fait à, le

Caractéristiques du système (veuillez cocher les cases appropriées) :

1

Caractéristiques générales :

a. Nombre de caméras :

- ☐ moins de 8 caméras ☐ 8 caméras ou plus

b. Mode de fonctionnement du système :

- ☐ Le système comporte des caméras à plan large (destinées à une compréhension des situations) et des caméras à plan étroit (susceptibles de permettre une reconnaissance des individus)
- ☐ Le système ne comporte que des caméras à plan large
- ☐ Le système ne comporte que des caméras à plan étroit

2

Mode d'enregistrement des images :

a. Le stockage des images est-il ?

- Analogique ☐ Numérique ☐

b. Possibilité de déterminer la caméra ayant filmé une scène :

- Possible sur les enregistrements eux mêmes ☐
- Possible grâce à un journal ☐
- Non prévu ☐

c. Existe-t-il un journal gardant la trace des opérations effectuées sur les flux vidéo (export, modification, suppression)

- Oui, journal manuel ☐
- Oui, journal généré automatiquement sous forme électronique ☐
- Non ☐

3

Questions relatives à la qualité des images :

a. La résolution des images en plan étroit (à l'exclusion de celles de régulation du trafic routier) est-elle toujours supérieure ou égale à 4 CIF (704 x 576 pixels) et le nombre d'images supérieur ou égal à 12 images/s

- ☐ Oui ☐ Non

b. La résolution des autres images est-elle toujours supérieure ou égale à 1CIF (352 x 288 pixels) et le nombre d'images supérieur ou égal à 6 images/s ?

- ☐ Oui ☐ Non

4

Transmission des images aux forces de police :

a. Les images peuvent-elles être exportées sans dégradation de leur qualité ?

- Oui ☐ Non ☐

b. Dans le cas de systèmes numériques, si le format de codage des images n'est pas standard et libre de droits, le titulaire a-t-il prévu de fournir gratuitement à l'administration en cas de réquisition judiciaire, un système de lecture (ou une licence si le produit peut être installé) sur un PC standard permettant de lire les enregistrements et d'effectuer les principales opérations de visualisation

- Oui ☐ Non ☐