

## ANALYSE D'IMPACT

### Traitements relatifs à l'usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions

#### Présentation générale

L'article 114 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale a autorisé, à titre expérimental, pour une durée de deux ans, l'utilisation de caméras mobiles par les agents de la police municipale dans les conditions prévues à l'article L. 241-1 du code de la sécurité intérieure.

Les modalités d'application de ce dispositif ont été précisées par le décret n° 2016-1861 du 23 décembre 2016 relatif aux conditions de l'expérimentation de l'usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions.

A l'issue de cette expérimentation, le ministère de l'intérieur a reçu des rapports relatifs à l'utilisation de ce dispositif de la part de 242 communes. Les rapports reçus tirent, de manière générale, un bilan particulièrement positif de cette expérimentation.

Dans un rapport d'évaluation du 7 juin 2018, le ministère de l'intérieur a conclu à la nécessité de pérenniser ce dispositif. Cette pérennisation a été permise par l'adoption de la loi n° 2018-697 du 3 août 2018 relative à l'harmonisation de l'utilisation des caméras mobiles par les autorités de sécurité publique.

En effet, l'article 3 de cette loi introduit un article L. 241-2 dans le code de la sécurité intérieure. Cet article autorise les agents de police municipale, dans l'exercice de leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens ainsi que de leurs missions de police judiciaire, à procéder en tous lieux, au moyen de caméras individuelles, à un enregistrement audiovisuel de leurs interventions lorsque se produit ou est susceptible de se produire un incident, eu égard aux circonstances de l'intervention ou au comportement des personnes concernées.

Le décret prévoit les modalités d'autorisation d'emploi de ces caméras par le représentant de l'Etat dans le département et de mise en œuvre par les communes des traitements de données à caractère personnel issues des enregistrements audiovisuels et notamment leurs finalités, les données enregistrées, les modalités et leur durée de conservation, les conditions d'accès aux enregistrements et les modalités d'exercice des droits des personnes concernées.

#### 1.1. Vue d'ensemble

##### 1.1.1. Traitements considérés

<b>Description des traitements</b>	Les agents de police municipale sont autorisés à procéder à un enregistrement audiovisuel au moyen de caméras individuelles dans le cadre de leurs interventions dans les conditions définies à l'article L. 241-2 du code de la sécurité intérieure. Ces enregistrements audiovisuels pourront alors permettre aux communes de mettre en œuvre des traitements de données à caractère personnel provenant des caméras individuelles fournies aux agents de police municipale au titre de l'équipement des personnels.
<b>Finalités des traitements</b>	Ces traitements ont pour finalités : <ol style="list-style-type: none"><li>1) La prévention des incidents au cours des interventions des agents de police municipale ;</li><li>2) Le constat des infractions et la poursuite de leurs auteurs par la collecte de preuves ;</li><li>3) La formation et la pédagogie des agents de police municipale.</li></ol>

<b>Enjeux des traitements</b>	Permettre de collecter des enregistrements audiovisuels afin d'éviter les incidents au cours des interventions des agents de police municipale, de poursuivre les auteurs d'infractions en cas d'incidents et de former les agents de police municipale à l'aide de mises en situation concrètes par le biais des enregistrements audiovisuels.
<b>Responsables des traitements</b>	Chaque responsable du service de la police municipale sera responsable du traitement dans la commune
<b>Sous-traitant(s)</b>	

*En cas de recours à un sous-traitant pour la mise en œuvre du traitement, veuillez préciser le nom et les coordonnées de ce dernier dans cette rubrique*

### 1.1.2. Textes applicables

Textes applicables au traitement	Modalité de prise en compte
Textes législatifs et réglementaires	
Article L. 241-2 du code de la sécurité intérieure	Décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés
Dispositions des II et IV de l'article 26 [31] et du chapitre XIII [titre III] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.	Décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et engagement de conformité transmis à la Commission nationale de l'informatique et des libertés préalablement à la mise en œuvre de chaque traitement
Décret n° 2019-140 du 27 février 2019 portant application de l'article L. 241-2 du code de la sécurité intérieure et relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des agents de la police municipale	Décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés et engagement de conformité transmis à la CNIL préalablement à la mise en œuvre de chaque traitement

## 1.2. Données, processus et supports

### 1.2.1. Description des données, destinataires et durées de conservation

Données	Destinataires	Durée de conservation
Images et sons captés par les caméras individuelles utilisées par les agents de police municipale dans les circonstances et pour les finalités prévues à l'article L. 241-2 du code de la sécurité intérieure	Dans la limite de leurs attributions respectives et de leur besoin d'en connaître ont seuls accès aux données les personnes suivantes : 1) Responsable du service de la police municipale ; 2) Agents de la police municipale individuellement désignés et habilités par le responsable du service.	Six mois à compter du jour de l'enregistrement des données. Lorsque les données ont été extraites ou

## Analyse d'impact relative à la protection des données

Jour et plages horaires d'enregistrement	<p>Dans la limite de leurs attributions respectives et de leur besoin d'en connaître dans le cadre d'une procédure judiciaire, administrative ou disciplinaire, ou dans le cadre d'une action de formation et de pédagogie, peuvent être destinataires de tout ou partie des données et informations enregistrées dans le traitement :</p> <ol style="list-style-type: none"> <li>1) Officiers et agents de police judiciaire de la police nationale et de la gendarmerie nationale ;</li> <li>2) Agents des services d'inspection générale de l'Etat, dans les conditions prévues à l'article L. 513-1 du code de la sécurité intérieure ;</li> <li>3) Le maire et le président de l'établissement public de coopération intercommunale en qualité d'autorité disciplinaire ainsi que les membres des instances disciplinaires et les agents en charge de l'instruction des dossiers présentés à ces instances ;</li> <li>4) Les agents chargés de la formation des personnels.</li> </ol>	transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, dans le délai de six mois, elles sont conservées selon les règles propres à chacune de ces procédures par l'autorité qui en a la charge
Identification de l'agent porteur de la caméra lors de l'enregistrement des données		
Lieu où ont été collectées les données		

### 1.2.2. Description des processus et supports

Processus	Description détaillée du processus	Supports des données concernés
Autorisation d'utilisation des caméras individuelles	<p>Afin de pouvoir équiper leurs agents de police municipale de caméras individuelles, le maire ou l'ensemble des maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes dans les conditions prévues au 1<sup>er</sup> alinéa de l'article L. 512-2 du code de la sécurité intérieure présentent au préfet de département et dans le département des Bouches-du-Rhône, au préfet de police des Bouches-du-Rhône, une demande d'autorisation, accompagnée des pièces suivantes :</p> <ol style="list-style-type: none"> <li>1° La convention de coordination des interventions de la police municipale et des forces de sécurité de l'Etat prévue à la section 2 du chapitre II du titre 1er du livre V du code de la sécurité intérieure ;</li> <li>2° Un dossier technique de présentation du traitement envisagé ;</li> <li>3° Le cas échéant, les éléments nécessités par les circonstances locales de mise en œuvre du traitement, complémentaires à l'analyse d'impact relative à la protection des données à caractère personnel adressée à la Commission nationale de l'informatique et des libertés par le ministère de l'intérieur avec la demande d'avis sur les dispositions de la section 2 du chapitre unique du titre IV du livre II du code de la sécurité intérieure ;</li> <li>4° L'engagement de conformité destiné à la CNIL faisant référence aux dispositions du décret et précisant le nombre de caméras et le service utilisateur ;</li> <li>5° Le cas échéant, une mention de la commune dans laquelle est installé le support informatique sécurisé mentionné à l'article R.241-11 du code de la sécurité intérieure lorsque la</li> </ol>	

Analyse d'impact relative à la protection des données

	<p>demande est présentée par l'ensemble des maires des communes concernées.</p> <p>L'enregistrement audiovisuel des interventions des agents de police municipale est autorisé par arrêté du préfet de département, et dans le département des Bouches-du-Rhône, du préfet de police des Bouches-du-Rhône. Cet arrêté précise le nombre de caméras, la ou les communes sur le territoire desquelles elles sont utilisées et, le cas échéant, la commune de l'établissement public de coopération intercommunale dans laquelle est installé le support informatique sécurisé.</p> <p>En application du IV de l'article 26 [31] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et du 4° du I de l'article R. 241-8 du code de la sécurité intérieure, le maire ou l'ensemble des maires des communes concernées envoie l'engagement de conformité à la CNIL.</p>	
Enregistrement audiovisuel	<p>Dans l'exercice de leurs missions de prévention des atteintes à l'ordre public et de protection de la sécurité des personnes et des biens ainsi que de leurs missions de police judiciaire, les agents de police municipale peuvent procéder au moyen de caméras individuelles à un enregistrement audiovisuel de leurs interventions lorsque se produit ou est susceptible de se produire un incident eu égard aux circonstances de l'intervention ou au comportement des personnes concernées.</p>	<p>Les enregistrements audiovisuels sont conservés dans les mémoires internes non amovibles des caméras des agents qui en sont dotés jusqu'au retour au service des agents.</p>
Transfert des données	<p>Lorsque les agents de police municipale ont procédé à l'enregistrement d'une intervention dans les conditions précisées ci-dessus, les données enregistrées par les caméras individuelles sont transférées sur un support informatique sécurisé dès leur retour au service.</p> <div data-bbox="638 1478 1037 1657" style="border: 1px solid black; background-color: yellow; border-radius: 15px; padding: 5px; display: inline-block; margin: 10px auto; width: fit-content;"> <p><i>Veillez sélectionner ici l'un de ces modes de déchargement de la caméra</i></p> </div>	<p>Les enregistrements sont intégralement transférés sur le support informatique sécurisé mis en place par la commune : le déchargement de la caméra s'opère <b>soit en plaçant la caméra sur une station de déchargement qui transfère directement les données sur le serveur sécurisé, soit en connectant la caméra au PC dédié via le cordon USB fourni par le système.</b> Les enregistrements sont conservés sur ce serveur dans un local aux accès limités doté d'un logiciel permettant l'effacement automatisé des informations après six mois et enregistrant la traçabilité des opérations. Les données transférées sont systématiquement effacées des mémoires de la caméra.</p>
Consultation des	<p>Les enregistrements effectués à l'aide des caméras individuelles ne peuvent être consultés qu'à l'issue de</p>	<p>Les enregistrements sont conservés sur un support</p>

données	l'intervention et après leur transfert sur un support informatique sécurisé. Aucun système de transmission permettant de visionner les images à distance en temps réel ne peut être mis en œuvre.	informatique sécurisé dans un local aux accès limités doté d'un logiciel permettant l'effacement automatisé des informations après six mois et enregistrant la traçabilité des opérations. La consultation ne peut être réalisée qu'un fois les données transférées et pendant une durée de six mois.
Extraction des données	Le responsable du service de la police municipale et les agents de police municipale individuellement désignés et habilités par le responsable du service peuvent seuls procéder à l'extraction des données et informations mentionnées à l'article R. 241-10 du code de la sécurité intérieure pour les besoins exclusifs d'une procédure judiciaire, administrative ou disciplinaire ou dans le cadre d'une action de formation et de pédagogie des agents.	Les copies des enregistrements qui ont fait l'objet d'une transmission à l'autorité judiciaire, administrative ou hiérarchique dans le cadre des procédures judiciaires, administratives ou disciplinaires sont conservées selon les règles et les modalités propres à chacune de ces procédures.

## 2. Principes fondamentaux

### 2.1. Mesures garantissant la proportionnalité et la nécessité des traitements

#### 2.1.1. Finalités

L'usage des caméras individuelles par les agents de police municipale vise à répondre à un besoin de sécurisation physique et juridique de ces derniers lors de leurs interventions.

Les traitements de données à caractère personnel provenant des caméras individuelles utilisées par les agents de police municipale au titre de l'équipement des personnels poursuivent trois finalités :

- 1) La prévention des incidents au cours de leurs interventions ;
- 2) Le constat des infractions et poursuite de leurs auteurs par la collecte de preuves ;
- 3) La formation et la pédagogie des agents de police municipale.

Finalités	Légitimité
Prévention des incidents au cours des interventions des agents de police municipale	Permettre de réduire le nombre d'incidents au cours des interventions des agents de police municipale et d'apaiser les relations entre les agents de police municipale et les concitoyens.
Constat des infractions et poursuite de leurs auteurs par la collecte de preuves	Permettre de constater puis de poursuivre les auteurs d'infractions commises au cours des interventions des agents de police municipale. Ainsi, aux termes du 2° de l'article 21 du code de procédure pénale, les agents de police municipale sont des agents de police judiciaire adjoints, qui ont pour mission de seconder, dans l'exercice de leurs fonctions, les

	<p>officiers de police judiciaire, de rendre compte à leurs chefs hiérarchiques de tous crimes, délits ou contraventions dont ils ont connaissance ainsi que de constater les infractions à la loi pénale et de recueillir tous les renseignements en vue de découvrir les auteurs de ces infractions. Récemment, la loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes les a autorisés à constater les contraventions prévues à l'article 621-1 du code pénal (outrage sexiste).</p> <p>En application du deuxième alinéa de l'article L. 511-1 du code de la sécurité intérieure, les agents de police municipale peuvent verbaliser les contraventions aux arrêtés de police du maire.</p> <p>En outre, ce même article permet aux agents de police municipale de constater par procès-verbaux les contraventions aux dispositions du code de la route dont la liste est fixée par décret en Conseil d'État (R. 130-2 du code de la route) ainsi que certaines contraventions mentionnées au livre VI du code pénal dont la liste est également fixée par décret en Conseil d'Etat (article R.15-33-29-3 du code de procédure pénale).</p> <p>Enfin, des textes spécifiques les rendent compétents pour relever des infractions dans un certain nombre de domaines (chiens dangereux, police de la conservation du domaine routier, police de l'environnement, nuisances sonores, accès aux parties communes d'immeuble à usage d'habitation...).</p>
Formation et pédagogie des agents de police municipale	<p>Permettre une mise en situation des agents de police municipale afin de mieux appréhender les risques encourus lors de leurs interventions.</p> <p>Les données utilisées pour ces finalités sont anonymisées.</p>

### 2.1.2. Fondement

Les traitements entrent dans le champ de la directive (UE) 2016/680 du 27 avril 2016, transposée au chapitre XIII [titre III] de la loi du 6 janvier 1978 susmentionnée, et se fondent sur les II et IV de l'article 26 [31] de la même loi. En effet, ces traitements ont une finalité de prévention, de recherche, de constatation ou de poursuite d'infractions pénales lors des interventions des agents de police municipale et sont mis en œuvre par des autorités compétentes pour le compte de l'Etat. Les traitements peuvent par ailleurs collecter des données de la nature de celles mentionnées au I de l'article 8 [6] de la même loi, qui peuvent être révélées dans les images et les sons captés.

### 2.1.3. Minimisation des données

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
Images et sons captés par les caméras individuelles utilisées par les agents de police	Données sensibles	Données indispensables en cas de procédure judiciaire, administrative ou disciplinaire car	- L'article L. 241-2 du code de la sécurité intérieure pose le principe selon lequel

Analyse d'impact relative à la protection des données

municipale dans les circonstances et pour les finalités prévues à l'article L. 241-2 du code de la sécurité intérieure		constitutives d'éléments de preuves	<p>l'enregistrement par le biais des caméras individuelles n'est pas permanent.</p> <ul style="list-style-type: none"> <li>- Les personnes filmées sont informées préalablement au déclenchement de l'enregistrement.</li> <li>- Lorsque ces données sont utilisées à des fins pédagogiques et de formation, elles font l'objet d'une anonymisation.</li> <li>- Les données sont effacées automatiquement à l'expiration d'un délai de six mois.</li> <li>- Il est interdit de sélectionner dans les traitements une catégorie particulière de personnes à partir des données relevant du I de l'article 8 [6] de la loi n° 78-17 du 6 janvier 1978</li> </ul>
Jour et plages horaires d'enregistrement	Données non sensibles	Données indispensables en cas de procédure judiciaire, administrative ou disciplinaire pour vérifier la date de l'enregistrement	
Identification de l'agent porteur de la caméra lors de l'enregistrement des données	Données non sensibles	Données indispensables en cas de procédure judiciaire, administrative ou disciplinaire pour vérifier la qualité de l'agent	
Lieu où ont été collectées les données	Données non sensibles	Données indispensables en cas de procédure judiciaire, administrative ou disciplinaire pour vérifier la location des faits	

2.1.4. Qualité des données

Mesures pour la qualité des données	Modalités de mise en œuvre
Intégrité des images et sons captés	<p>Les dispositifs techniques permettent d'empêcher les agents d'avoir accès aux enregistrements pris à l'aide de leur caméra et disponibles sur la mémoire interne de celle-ci. La consultation des enregistrements n'est possible qu'après transfert sur un support informatique sécurisé et par des personnes limitativement énumérées et habilitées. Ces garanties sont prévues aux articles L. 241-2, R. 241-11</p>

	et R. 241-12 du code de la sécurité intérieure. Il n'est pas possible de procéder à une rectification matérielle des images et sons, garantissant leur intégrité.
Horodatage et localisation des images et sons captés	La date et les plages horaires de l'enregistrement sont générées automatiquement par la caméra et ne peuvent être modifiées. <b>Les caméras disposant d'un GPS permettent une géolocalisation automatique lors de l'enregistrement. Dans le cas où le choix technique de la commune se porterait sur des caméras n'intégrant pas un GPS, l'agent porteur de la caméra doit consigner le lieu où les données ont été collectées à son retour de service.</b>
Port de la caméra au niveau du sternum afin de garantir une prise de vue grand angle et une stabilité des images	Les caméras peuvent être portées à l'épaule ou au niveau de la poitrine. Lors de leur formation, les agents de police municipale seront sensibilisés au fait que le port au niveau du thorax est préférable en raison du champ de vision offert.
Qualité infrarouge pour l'enregistrement des images nocturnes	<b>Même si toutes les caméras ne disposent pas de cette option, qui relève d'un choix technique, il sera recommandé d'opter pour des caméras infrarouges.</b>

*Veillez ici adapter ces mentions en fonction du choix effectué d'équiper ou non les agents de police municipale d'une caméra disposant d'un GPS*

*Veillez ici préciser si vous avez opté pour une caméra infrarouge*

2.1.5. 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 et sons captés par les caméras individuelles utilisées par les agents de police municipale dans les circonstances et pour les finalités prévues à l'article L. 241-2 du code de la sécurité intérieure	6 mois à compter du jour de l'enregistrement des données. Lorsque les données ont été extraites ou transmises pour les besoins d'une	Laisser un temps suffisant aux personnes filmées pour exercer, le cas échéant, un recours donnant lieu à une procédure judiciaire, administrative ou disciplinaire.  Permettre le traitement des enregistrements audiovisuels et la prise de décision d'une éventuelle extraction de données pour les besoins d'une procédure judiciaire, administrative ou disciplinaire.	Au terme du délai de 6 mois, les données sont effacées automatiquement des traitements.  Il s'agit d'une purge définitive des données du système.
Jour et plages horaires d'enregistrement	procédure judiciaire, administrative ou disciplinaire, dans	Conservation nécessaire en cas de poursuites dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.	
Identification de l'agent porteur de la caméra lors de l'enregistrement des données	le délai de six mois, elles sont conservées selon les règles propres à chacune de ces	Conservation nécessaire en cas de poursuites dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.	
Lieu où ont été	procédures par	Conservation nécessaire en cas de	

## Analyse d'impact relative à la protection des données

collectées les données	les	l'autorité qui en a la charge.	poursuites dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.	
------------------------	-----	--------------------------------	---	--

### 2.1.6. Evaluation des mesures

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable	Mesures correctives / préventives
Finalités : déterminées, explicites et légitimes Les finalités des traitements sont expressément définies à l'article L. 241-2 du code de la sécurité intérieure. Les données ne sont conservées qu'en vue de leur exploitation dans le cadre d'une procédure judiciaire, administrative ou disciplinaire.	Acceptable	
Fondement : licéité du traitement, interdiction du détournement de finalité Les traitements entrent dans le champ de la directive (UE) 2016/680 du 27 avril 2016, des II et IV de l'article 26 [31] et du chapitre XIII [titre III] de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés	Acceptable	Mesure préventive : un détournement des finalités des enregistrements et des traitements ou de l'utilisation des données peut être sanctionné dans le cadre d'une procédure judiciaire, administrative ou disciplinaire
Minimisation des données : adéquates, pertinentes et limitées L'article L. 241-2 du code de la sécurité intérieure précise que les agents de police municipale peuvent procéder à un enregistrement audiovisuel uniquement « <i>lorsque se produit ou est susceptible de se produire un incident eu égard aux circonstances de l'intervention ou au comportement des personnes concernées</i> ». et l'enregistrement n'est pas permanent	Acceptable	
Qualité des données : exactes et tenues à jour	Acceptable	
Durée de conservation : limitée à six mois	Acceptable	Mesure préventive : les données sont automatiquement et définitivement effacées à l'expiration du délai de six mois

## 2.2. Évaluation des mesures protectrices des droits des personnes concernées

### 2.2.1. Mesures pour l'information des personnes

Les agents de police municipale utilisateurs des caméras mobiles sont informés de la législation applicable à ces dispositifs et formés à leur utilisation.

L'article L. 241-2 du code de la sécurité intérieure dispose que « les caméras sont portées de façon apparente par les agents. Un signal visuel spécifique indique si la caméra enregistre. Le déclenchement de l'enregistrement fait l'objet d'une information des personnes filmées, sauf si les circonstances l'interdisent. Une information générale du public sur l'emploi de ces caméras est organisée par le ministre de l'intérieur. »

L'article R. 241-15 du code de la sécurité intérieure prévoit que « l'information générale du public sur l'emploi des caméras individuelles par la commune est délivrée sur le site internet de la commune ou, à défaut, par voie d'affichage en mairie ».

Les informations prévues à l'article 70-18 [104] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés sont mises à disposition par le maire ou l'ensemble des maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes.

Mesures pour le droit à l'information	Modalités de mise en œuvre et justifications
Présentation des conditions d'utilisation /confidentialité  <i>Veuillez adapter les cinq mentions du tableau en précisant les modalités d'information des personnes concernées : sur le site internet de votre commune ou par voie d'affichage en mairie</i>	Une information générale du public sur l'emploi de ces caméras est organisée par le ministre de l'intérieur, conformément au quatrième alinéa de l'article L. 241-2 du code de la sécurité intérieure. Cette information rappelle le cadre juridique, les modalités d'utilisation des caméras et de conservation des enregistrements ainsi que les droits des personnes concernées. Une information générale du public sur l'emploi des caméras individuelles par la commune est <b>délivrée sur le site internet de la commune ou, à défaut, par voie d'affichage en mairie.</b>
Possibilité d'accéder aux conditions d'utilisation/confidentialité	Sur le site internet du ministère de l'intérieur et <b>sur le site internet de la commune ou, à défaut, par voie d'affichage en mairie.</b>
Conditions lisibles et compréhensibles	Ces informations figurent sur <b>le site internet de chaque commune, ou à défaut, par voie d'affichage en mairie</b>
Existence de clauses spécifiques au dispositif	Non applicable
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)	Sur le site internet du ministère de l'intérieur et <b>sur le site internet de la commune ou, à défaut, par voie d'affichage en mairie.</b> Le dispositif ne comporte pas de croisement de données.
Présentation détaillée des données personnelles collectées	Les personnes concernées sont informées du déclenchement de l'enregistrement sauf si les circonstances l'interdisent. La liste des données est communiquée sur <b>le site internet de la commune ou, à défaut, par voie d'affichage en mairie.</b>
Présentation des éventuels accès à des identifiants de l'appareil, en précisant si ces identifiants sont communiqués à des tiers	Non applicable
Présentation des droits de la personne concernée (retrait du consentement, suppression de données, etc.)	Sur le site internet du ministère de l'intérieur <b>et sur le site internet de la commune ou, à défaut, par voie d'affichage en mairie.</b>
Information sur le mode de stockage sécurisé des données, notamment en cas d'externalisation	Non applicable

Modalités de contact de l'entreprise (identité et coordonnées) pour les questions de confidentialité	Non applicable
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité	Ce cas ne devrait pas se présenter.

#### 2.2.2. Mesures pour le recueil du consentement

Le consentement n'est pas applicable aux présents traitements qui relèvent de la directive (UE) 2016/680 du 27 avril 2016.

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

Le droit d'accès prévu à l'article 70-19 [105] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés s'exerce directement auprès du maire ou de l'ensemble des maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes.

Afin d'éviter de gêner des enquêtes et des procédures administratives ou judiciaires et d'éviter de nuire à la prévention ou la détection d'infractions pénales, aux enquêtes, aux poursuites en la matière, le droit d'accès peut faire l'objet de restrictions en application du 2° du II et du III de l'article 70-21 [107] de la même loi.

La personne concernée par ces restrictions exerce son droit auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 70-22 [108] de la même loi.

Le droit à la portabilité n'est pas applicable aux présents traitements qui relèvent de la directive (UE) 2016/680 du 27 avril 2016.

#### 2.2.4. Mesures pour les droits de rectification et d'effacement

Le droit de rectification n'est pas applicable aux traitements en ce qu'il constitue une formalité impossible. Les images et sons captés ne peuvent être matériellement rectifiés sauf à porter atteinte à leur intégrité. Les autres informations sont générées automatiquement par les caméras.

Le droit d'effacement prévu à l'article 70-20 [106] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés s'exerce directement auprès du maire ou de l'ensemble des maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes.

Afin d'éviter de gêner des enquêtes et des procédures administratives ou judiciaires et d'éviter de nuire à la prévention ou la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière, le droit d'effacement peut faire l'objet de restrictions en application du 3° du II de l'article 70-21 [107] de la même loi.

La personne concernée par ces restrictions exerce son droit auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 70-22 [108] de la même loi.

2.2.5. Mesures pour les droits de limitation du traitement et d'opposition

Le droit de limitation est garanti par les dispositions de l'article R. 241-13 du code de la sécurité intérieure qui prévoit que, lorsque les données ont, dans le délai de conservation de six mois, été extraites et transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, elles sont conservées selon les règles propres à chacune des procédures par l'autorité qui en a la charge.

Le droit d'opposition prévu à l'article 38 [110] de la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés ne s'applique pas en application du II de l'article R. 241-15 du code de la sécurité intérieure. Cette exclusion se justifie au regard des finalités des traitements.

*Veillez ici adapter ces mentions en fonction de votre choix de recourir ou non à un sous-traitant. Dans l'hypothèse d'un hébergement en cloud, il convient également de préciser les mesures protectrices des droits des personnes.*

2.2.6. Mesures pour la sous-traitance

La plupart des communes n'ont pas recours à des sous-traitants pour la mise en place du support informatique sécurisé. Toutefois, certains prestataires peuvent proposer un hébergement en cloud. Dans ce cas, ces prestataires ont la qualité de sous-traitants soumis à un contrat qui prévoit que seule l'administration aura accès aux données.

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

Le traitement n'implique pas de transfert de données en dehors de l'Union européenne.

2.2.8. Evaluation des mesures

Mesures protectrices des droits des personnes concernées	Acceptable / Améliorable ?	Mesures correctives
Information des personnes concernées (traitement loyal et transparent) : les caméras sont portées de façon apparente par les agents. Un signal visuel spécifique indique si la caméra enregistre. Les personnes sont préalablement informées du déclenchement de l'enregistrement.	Acceptable	
Recueil du consentement : Le principe du consentement n'est pas applicable pour les traitements qui relèvent du champ de la directive (UE) 2016/680 du 27 avril 2016	Non applicable	
Exercice des droits d'accès et à la portabilité : Le droit d'accès s'exerce directement auprès du maire ou de l'ensemble des	Acceptable pour droit d'accès ; non applicable pour la portabilité	

<p>maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes. Afin d'éviter de gêner des enquêtes et des procédures administratives ou judiciaires et 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 du 2° du II et du III de l'article 70-21 [107] de la même loi.</p> <p>Le droit à la portabilité n'est pas applicable aux traitements.</p>		
<p>Exercice des droits de rectification et d'effacement :</p> <p>Le droit de rectification n'est pas applicable aux traitements.</p> <p>Le droit d'effacement prévu à l'article 70-20 [106] de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés s'exerce directement auprès du maire ou de l'ensemble des maires des communes lorsque les agents susceptibles d'être équipés de caméras mobiles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes.</p> <p>Afin d'éviter de gêner des enquêtes et des procédures administratives ou judiciaires et d'éviter de nuire à la prévention ou la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière, le droit</p>	<p>Droit de rectification : non applicable</p> <p>Droit d'effacement : Acceptable</p>	

<p>d'effacement peut faire l'objet de restrictions en application du 3° du II de l'article 70-21 [107] de la même loi.</p>		
<p>Exercice des droits de limitation du traitement et d'opposition :</p> <p>Le droit de limitation est garanti par les dispositions de l'article R. 241-13 du code de la sécurité intérieure qui prévoit que, lorsque les données ont, dans le délai de conservation de six mois, été extraites et transmises pour les besoins d'une procédure judiciaire, administrative ou disciplinaire, elles sont conservées selon les règles propres à chacune des procédures par l'autorité qui en a la charge.</p> <p>Le droit d'opposition prévu à l'article 38 [110] de la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés ne s'applique pas en application du II de l'article R. 241-15 du code de la sécurité intérieure.</p>	<p>Droit d'opposition est exclu ; droit de limitation : acceptable</p>	
<p>Sous-traitance : Certains prestataires peuvent proposer un hébergement en cloud. Dans ce cas, ces prestataires ont la qualité de sous-traitant soumis à un contrat qui prévoit que seule l'administration a accès aux données.</p>		
<p>Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne</p>	<p>Non applicable</p>	

*En cas de recours à un sous-traitant pour la mise en œuvre du traitement, veuillez préciser le nom et les coordonnées de ce dernier dans cette rubrique et évaluer la mesure*

### 3. Etude des risques liés à la sécurité des données

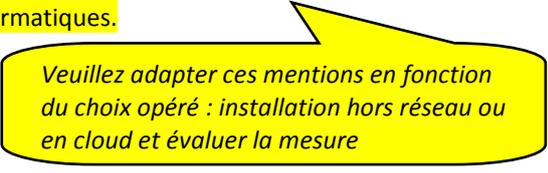
#### 3.1. Évaluation des mesures

##### 3.1.1. Mesures contribuant à traiter des risques liés à la sécurité des données

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Chiffrement	<p>Les systèmes commercialisés prévoient des enregistrements cryptés sur le disque dur de la station. Il existe plusieurs modes de cryptage en fonction du choix effectué par les communes mais qui proposent tous au minima un chiffrement. Seul l'administrateur du système a les clés du chiffrement pour les relectures et extractions.</p> <p><i>Veillez adapter ces mentions en précisant le mode de cryptage</i></p>	Acceptable	
Protection des sites web	<p>Pour la grande majorité des communes utilisatrices de caméras mobiles, le support informatique sécurisé est installé hors réseau Internet afin d'éviter tout piratage des informations collectées</p> <p>En cas d'hébergement cloud, les prestataires respectent les recommandations de la CNIL sur le sujet.</p> <p><i>Veillez adapter ces mentions en précisant si le support informatique sécurisé est installé hors réseau ou en hébergement cloud et évaluer la mesure</i></p>		
Cloisonnement des données (par rapport au reste du système d'information)	<p>Pour la grande majorité des communes utilisatrices de caméras mobiles, le support informatique sécurisé est installé hors réseau Internet afin d'éviter tout piratage des informations collectées</p> <p><i>Veillez adapter ces mentions en précisant si le support informatique sécurisé est installé hors réseau Internet. Dans le cas contraire, il convient de préciser les modalités de mise en œuvre intégrant des mesures de sécurité et évaluer la mesure</i></p>		
Sécurité physique	<p>Les locaux où sont entreposés les supports informatiques sécurisés des services de police municipale font l'objet d'un contrôle d'accès défini par le maire (soit accès par badge, par code ou clé conservée par le responsable, soit local sous alarme). Les locaux ne sont accessibles qu'aux agents du service de la police municipale qui y déposent leurs caméras</p> <p><i>Veillez sélectionner le mode d'accès choisi</i></p>	Acceptable	

	<p>après utilisation, et les personnes, assurant le cas échéant la maintenance, n'interviennent qu'en présence du responsable du service, désigné par le maire.</p>		
Contrôle des accès logiques	<p>Les systèmes de déchargement sont équipés d'un logiciel d'administration et de recherche, prévoyant deux profils :</p> <ul style="list-style-type: none"> <li>- l'administrateur technique qui crée les profils des utilisateurs « gestionnaires » désignés par le chef de service et paramètre les durées de conservations des enregistrements et des logs, par défaut respectivement 6 mois et 3 ans. Il peut effectuer les recherches dans les logs (log = toute action effectuée sur les profils, les enregistrements, les méta-données ou les logs eux-mêmes).</li> <li>- le gestionnaire : il effectue des recherches d'enregistrements sur la base des métadonnées (numéro de la caméra et du porteur, horodatage et données GPS), les consulte et les extrait dans le cadre prévu par les textes. Toutes les actions du gestionnaire sont enregistrées (logs).</li> </ul>	Acceptable	
Journalisation	<p>Chaque opération de consultation, d'extraction et d'effacement de données fait l'objet d'un enregistrement dans le traitement ou à défaut d'une consignation dans un registre spécialement ouvert à cet effet.</p> <div style="border: 1px solid black; border-radius: 15px; padding: 10px; background-color: yellow; margin: 10px 0;"> <p><i>Veuillez sélectionner ici la modalité d'enregistrement des opérations de consultation, d'extraction et d'effacement des données : par enregistrement dans le traitement ou par consignation dans un registre spécialement ouvert à cet effet</i></p> </div> <p>Cette consignation comprend :</p> <ul style="list-style-type: none"> <li>- Les matricules, nom, prénom et grade des agents procédant à l'opération de consultation, d'extraction et d'effacement ;</li> <li>- La date et l'heure de la consultation et de l'extraction ainsi que le motif judiciaire, administratif, disciplinaire ou pédagogique ;</li> <li>- Le service ou l'unité destinataire des données ;</li> <li>- L'identification des enregistrements audiovisuels extraits et de la caméra dont ils sont issus.</li> </ul> <p>Ces informations sont conservées pendant trois ans.</p>	Acceptable	

3.1.2. Mesures générales de sécurité

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Sécurité de l'exploitation	Les systèmes de déchargement sont équipés d'un logiciel d'administration et de recherche, prévoyant deux profils : - l'administrateur technique qui crée les profils des utilisateurs « gestionnaires » désignés par le chef de service et paramètre les durées de conservations des enregistrements et des logs, par défaut respectivement 6 mois et 3 ans. Il peut effectuer les recherches dans les logs (log = toute action effectuée sur les profils, les enregistrements, les méta-données ou les logs eux-mêmes). - le gestionnaire : il effectue des recherches d'enregistrements sur la base des métadonnées (numéro de la caméra et du porteur, horodatage et données GPS), les consulte et les extrait dans le cadre prévu par les textes. Toutes les actions du gestionnaire sont enregistrées (logs).	Acceptable	
Lutte contre les logiciels malveillants	La lutte contre les logiciels malveillants est garantie par le dispositif du support informatique hors réseau et d'un serveur dédié sécurisé. Dans l'hypothèse d'une prestation d'hébergement en cloud, le prestataire s'engage à garantir la confidentialité et l'intégrité des images.  	Acceptable	
Mot de passe	Mots de passe individualisés avec contrôle des logs de connexion	Améliorable	La doctrine de la CNIL concernant les mots de passe sera diffusée
Sécurité des sites web	Non applicable		
Sauvegardes	Programmation des conservations à six mois avec effacement automatique à échéance	Acceptable	
Maintenance	La maintenance est assurée par le fournisseur du dispositif pour remise en service du système en cas de panne, de dysfonctionnement des enregistrements.	Améliorable	
Sécurité des canaux informatiques (réseaux)	Il n'y a pas de raccordement réseau. Dans l'hypothèse d'une prestation d'hébergement en cloud, le prestataire s'engage à sécuriser les canaux informatiques.  		

Surveillance	Contrôle régulier par le responsable du journal automatique ou du registre	Acceptable	
Contrôle d'accès physique	Les locaux où sont entreposés les supports informatiques sécurisés des services de police municipale font l'objet d'un contrôle d'accès défini par le maire (soit accès par badge, par code ou clé conservée par le responsable, soit local sous alarme). Les locaux ne sont accessibles qu'aux agents du service de la police municipale et les personnes, assurant le cas échéant la maintenance, n'interviennent qu'en présence du responsable du service, désigné par le maire.	Acceptable	
Sécurité des matériels	Le serveur dédié est placé dans un local dédié sous contrôle d'accès physique.	Acceptable	
Éloignement des sources de risques	Le support informatique est installé hors réseau et les enregistrements sont cryptés sur le disque dur de la station.	Acceptable	
Protection contre les sources de risques non humaines	Les locaux des services de police municipale doivent prévoir des mesures de protections contre les risques.  <i>Veillez préciser les mesures de protection de vos locaux contre les risques non humains (détecteur sismique, incendie,...) et évaluer la mesure</i>		

3.1.3. Mesures organisationnelles (gouvernance)

Mesures générales de sécurité	Modalités de mise en œuvre	Acceptable / améliorable	Mesures correctives
Organisation	Chaque responsable du service de police municipale définit l'organisation : - l'administrateur détermine les accès ; - il procède à un contrôle régulier des informations de traçabilité ; - il s'assure de la conformité et de l'exécution du contrat de maintenance.  <i>Veillez adapter ces mentions en précisant l'organisation mise en place et évaluer la mesure</i>		Le règlement intérieur peut rappeler aux agents les modalités d'usage. Il peut être procédé à un contrôle ponctuel par les services d'inspection générale de l'Etat dans les conditions prévues à l'article L. 513-1 du code de la sécurité intérieure.
Politique (gestion des règles)	Formation, charte informatique, doctrine d'emploi  <i>Veillez adapter ces mentions en précisant si une formation, charte informatique ou doctrine d'emploi est ou va être mise en place et évaluer la mesure</i>		

Gestion des risques	<p>Traçabilité des connexions consultables sur le journal automatique ou sur le registre</p> <p><i>Veillez adapter ces mentions en précisant ici si la traçabilité est effectuée sur le journal automatique ou sur un registre</i></p>	Acceptable	
Gestion des projets	<p>Le choix des dispositifs relève du responsable du service de police municipale. Le représentant de l'Etat vérifie, préalablement à l'autorisation, la conformité du dispositif aux dispositions du code de la sécurité intérieure.</p> <p><i>Veillez apporter des précisions sur la justification du choix du dispositif et évaluer la mesure</i></p>		
Gestion des incidents et des violations de données	<p>Enregistrement au journal de la défaillance constatée et alerte les agents du dysfonctionnement constaté.</p> <p><i>Veillez apporter des précisions sur la procédure en cas d'incidents et évaluer la mesure</i></p>		
Gestion des personnels	<p>Les accès aux traitements sont restreints à un nombre limité d'agents qui sont individuellement désignés. Les agents sont formés aux usages et à l'emploi des caméras individuelles du déclenchement au transfert sur le support informatique sécurisé au retour du service.</p> <p><i>Veillez apporter des précisions sur la formation dispensée aux agents.</i></p>	Acceptable	
Relations avec les tiers	Non applicable	Acceptable	
Supervision	Le responsable du traitement (généralement l'administrateur qui crée les accès) veille par des contrôles aux connexions afin de détecter des accès anormaux mais aussi aux éventuels incidents (panne, sauvegarde défaillante, respect des procédures de déchargement).	Acceptable	

**3.2. Appréciation des risques : les atteintes potentielles aux droits et libertés**

3.2.1. Données essentielles

Données essentielles	Description
Images et sons captés par les caméras individuelles utilisées par les agents de police municipale dans les circonstances et pour les finalités prévues à l'article L. 241-2 du code de la sécurité intérieure	Lors de leurs interventions, en cas de déclenchement de l'enregistrement, les caméras individuelles peuvent enregistrées toute image et son, aussi bien dans des lieux publics que privés.

3.2.2. Analyse et estimation des risques

Risque	Principales sources de risques	Principales menaces	Principaux impacts potentiels	Principales mesures réduisant la gravité et la vraisemblance	Gravité	Vraisemblance
Accès illégitime à des données	Usurpation ou divulgation de mot de passe, Entourage d'un agent	Effacement des données Consultation et extraction des données collectées en vue d'une divulgation ou d'une utilisation illégale	Conséquences d'une communication d'informations sensibles (risque d'atteinte à la vie privée). Menaces et pressions sur la personne filmée ou sur l'agent porteur de la caméra Discrédit de l'usage du dispositif Perte de la confiance Accessoirement atteinte au secret dans le cadre d'une procédure judiciaire	Respect strict des règles de confidentialité des accès aux locaux, des mots de passes avec mesures de contrôles des logs, et accès aux données cryptées par le seul administrateur habilité.	Importante. Les enregistrements 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, mais également pour l'agent de police municipale	Limitée compte tenu des modalités de mise en œuvre qui responsabilisent les agents qui risquent une mise en cause, qui rappellent la politique des mots de passe et des sécurités physiques et numériques

*Veillez préciser les mesures locales mises en œuvre aux fins de réduire le risque d'accès illégitime aux données*

Analyse d'impact relative à la protection des données

<p>Modification non désirées de données</p>	<p>Introduction dans le système</p>	<p>Modification des informations collectées ne permettant plus d'utiliser celles ci à l'appui d'une procédure</p>	<p>Impossibilité d'exploiter les informations et de les utiliser dans le cadre d'une procédure judiciaire, administrative ou disciplinaire en tant que preuves</p> <p><i>Veillez préciser les mesures mises en œuvre aux fins de réduire le risque de modification non désirée des données</i></p>	<p>Procédures de contrôle, implication des agents, contrôles des logs, maintenance</p> <p>L'administrateur est en charge de ces contrôles.</p> <p>Les procédures varient toutefois en fonction des communes utilisatrices des caméras mobiles.</p>	<p>limitée.</p> <p>Une modification des images et des sons captés serait nécessairement détectée car portant atteinte à l'intégrité de la donnée. Une modification pourrait nuire aux enquêtes car les enregistrements ne pourraient être extraits et utilisés comme mode de preuve. Toutefois, en l'absence d'obligation de procéder à un enregistrement, ne serait pas de nature à vicier les procédures engagées.</p>	<p>Très limitée en raison du cloisonnement du système et de son installation hors réseau</p>
<p>Disparition de données</p>	<p>Introduction usurpée et frauduleuse dans le système d'hébergement de conservation</p> <p>Et source non humaine (cas de force majeure : incendie, inondation)</p>	<p>dysfonctionnement du stockage, erreur de manipulation de l'agent, problème de maintenance ou défaillance technique</p>	<p>Impossibilité d'exploiter les informations et de les utiliser dans le cadre d'une procédure judiciaire, administrative ou disciplinaire en tant que preuves</p> <p><i>Veillez préciser les mesures mises en œuvre aux fins de réduire le risque de disparation des données</i></p>	<p>Maintenance, contrôles réguliers du dispositif et des connexions</p> <p>Certaines communes peuvent mettre en place une sauvegarde distante des données. Cela a notamment été le cas pour certaines grandes collectivités lors de l'expérimentation.</p>	<p>limitée</p> <p>Une suppression des données serait détectée via les informations de traçabilité. Une disparition des données pourrait nuire aux enquêtes car les enregistrements ne pourraient être extraits et utilisés comme mode de preuve. Toutefois, en l'absence d'obligation de procéder à un enregistrement, ne serait pas de nature à vicier les procédures engagées.</p>	<p>limitée en raison du cloisonnement du système et de son installation hors réseau et de la sécurisation des locaux</p>

## 4. Validation de l'analyse d'impact

### 4.1. Eléments utiles à la validation

#### 4.1.1. Synthèse relative à la conformité au RGPD

Finalités	Evaluation
<b>Mesures garantissant la proportionnalité et la nécessité du traitement</b>	
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
<b>Mesures protectrices des droits des personnes des personnes concernées</b>	
Information des personnes concernées (traitement loyal et transparent)	Acceptable
Recueil du consentement	Non applicable
Exercice des droits d'accès et à la portabilité	Acceptable
Exercice des droits de rectification et d'effacement	Acceptable
Exercice des droits de limitation du traitement et d'opposition	Acceptable
Sous-traitance : identifiée et contractualisée	Acceptable
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	Non applicable

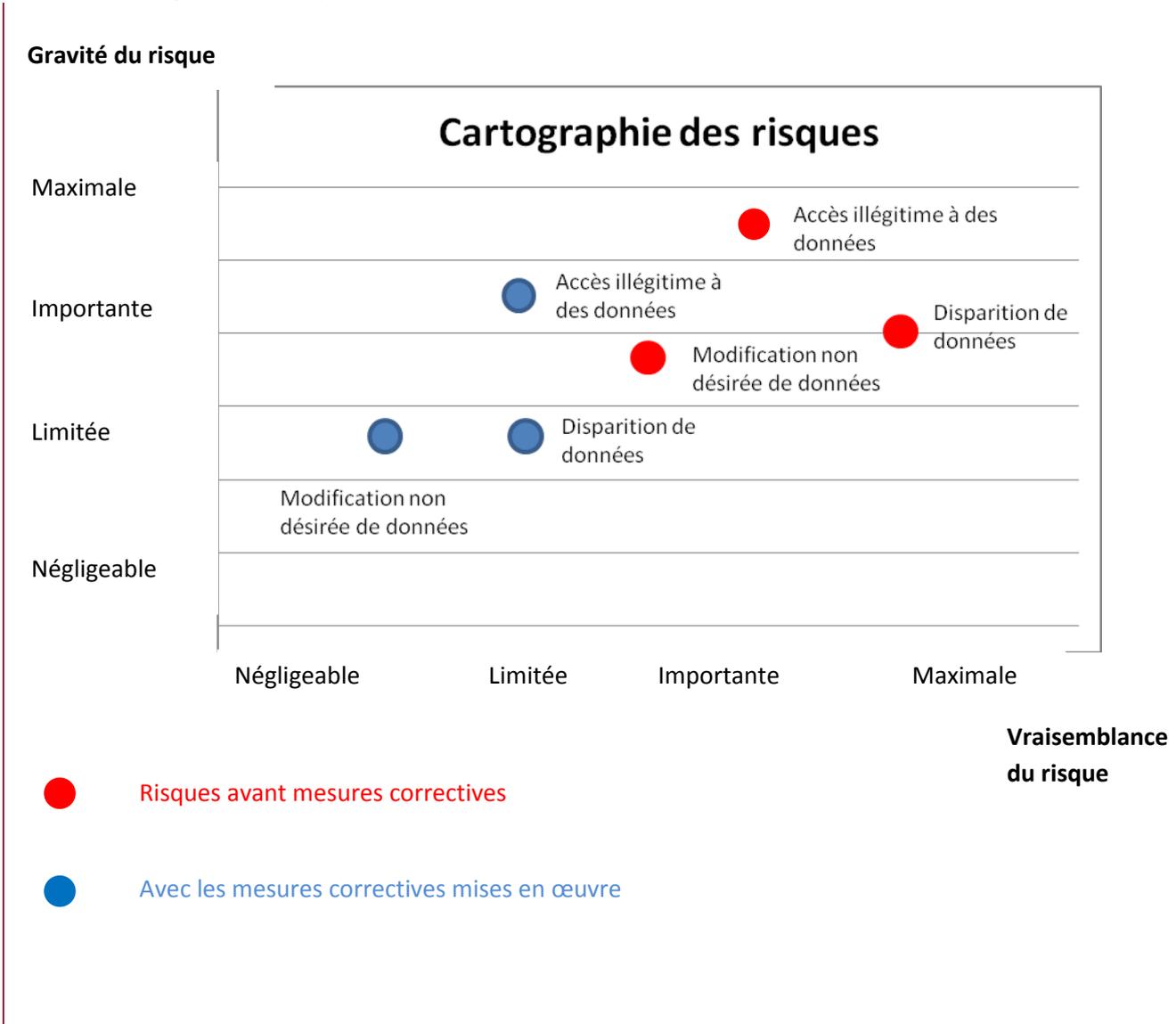
#### 4.1.2. Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données

Finalités	Evaluation
<b>Mesures portant spécifiquement sur les données du traitement</b>	
Chiffrement	Acceptable
Anonymisation	Acceptable
Cloisonnement des données (par rapport au reste du système d'information)	Acceptable
Contrôle des accès logiques des utilisateurs	Acceptable
Traçabilité (journalisation)	Acceptable
Contrôle d'intégrité	Acceptable
Archivage	Acceptable
Sécurité des documents papier	Non applicable
<b>Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre</b>	

Analyse d'impact relative à la protection des données

Sécurité de l'exploitation	Acceptable
Lutte contre les logiciels malveillants	Acceptable
Gestion des postes de travail	Améliorable
Sécurité des sites web	Non applicable
Sauvegardes	Acceptable
Maintenance	Améliorable
Sécurité des canaux informatiques (réseaux)	Non applicable
Surveillance	Acceptable
Contrôle d'accès physique	Acceptable
Sécurité des matériels	Acceptable
Éloignement des sources de risques	Acceptable
Protection contre les sources de risques non humaines	Acceptable
<b>Mesures organisationnelles (gouvernance)</b>	
Organisation	Acceptable
Politique (gestion des règles)	Acceptable
Gestion des risques	Acceptable
Gestion des projets	Acceptable
Gestion des incidents et des violations de données	Acceptable
Gestion des personnels	Acceptable
Relations avec les tiers	Non applicable
Supervision	Acceptable

4.1.3. Cartographie des risques liés à la sécurité des données



**Avis du délégué à la protection des données de la commune**

---

*Avis à compléter par le délégué à la protection des données désigné par le maire ou l'ensemble des maires*

## 5. Annexes

Echelles d'analyse des risques :

- Echelle de gravité (cf. partie 5.1)
- Echelle de vraisemblance (cf. partie 5.2)

5.1. Echelle de gravité

• Niveaux	• Descriptions génériques des impacts (directs et indirects)	• Exemples d'impacts corporels	• Exemples d'impacts matériels	• Exemples d'impacts moraux
<p><b>1. Négligeable</b></p>	<ul style="list-style-type: none"> <li>• Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté.</li> </ul>	<ul style="list-style-type: none"> <li>• Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle)</li> <li>• Maux de tête passagers</li> </ul>	<ul style="list-style-type: none"> <li>• Perte de temps pour réitérer des démarches ou pour attendre de les réaliser</li> <li>• Réception de courriers non sollicités (ex. : spams)</li> <li>• Réutilisation de données publiées sur des sites Internet à des fins de publicité ciblée (information des réseaux sociaux réutilisation pour un mailing papier)</li> <li>• Publicité ciblée pour des produits de consommation courants</li> </ul>	<ul style="list-style-type: none"> <li>• Simple contrariété par rapport à l'information reçue ou demandée</li> <li>• Peur de perdre le contrôle de ses données</li> <li>• Sentiment d'atteinte à la vie privée sans préjudice réel ni objectif (ex : intrusion commerciale)</li> <li>• Perte de temps pour paramétrer ses données</li> <li>• 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)</li> </ul>

<p><b>2. Limitée</b></p>	<ul style="list-style-type: none"> <li>• Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés</li> </ul>	<ul style="list-style-type: none"> <li>• Affection physique mineure (ex. : maladie bénigne suite au non- respect de contre-indications)</li> <li>• Absence de prise en charge causant un préjudice minime mais réel (ex : handicap)</li> <li>• Diffamation donnant lieu à des représailles physiques ou psychiques</li> </ul>	<ul style="list-style-type: none"> <li>• Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement</li> <li>• Refus d'accès à des services administratifs ou prestations commerciales</li> <li>• Opportunités de confort perdues (ex. : annulation de loisirs, d'achats, de vacances, fermeture d'un compte en ligne)</li> <li>• Promotion professionnelle manquée</li> <li>• Compte à des services en ligne bloqué (ex. : jeux, administration)</li> <li>• Réception de courriers ciblés non sollicités susceptible de nuire à la réputation des personnes concernées</li> <li>• Élévation de coûts (ex. : augmentation du prix d'assurance)</li> <li>• Données non mises à jour (ex. : poste antérieurement occupé)</li> <li>• Traitement de données erronées créant par exemple des dysfonctionnements de comptes (bancaires, clients, auprès d'organismes sociaux, etc.)</li> <li>• Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique)</li> <li>• Profilage imprécis ou abusif</li> </ul>	<ul style="list-style-type: none"> <li>• Refus de continuer à utiliser les systèmes d'information (<i>whistleblowing</i>, réseaux sociaux)</li> <li>• Affection psychologique mineure mais objective (diffamation, réputation)</li> <li>• Difficultés relationnelles avec l'entourage personnel ou professionnel (ex. : image, réputation ternie, perte de reconnaissance)</li> <li>• Sentiment d'atteinte à la vie privée sans préjudice irrémédiable</li> <li>• Intimidation sur les réseaux sociaux</li> </ul>
--------------------------	---	---	---	---

Analyse d'impact relative à la protection des données

<p><b>3. Importante</b></p>	<ul style="list-style-type: none"> <li>Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives.</li> </ul>	<ul style="list-style-type: none"> <li>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)</li> <li>Altération de l'intégrité corporelle par exemple à la suite d'une agression, d'un accident domestique, de travail, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Détournements d'argent non indemnisé</li> <li>Difficultés financières non temporaires (ex. : obligation de contracter un prêt)</li> <li>Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d'études, de stages ou d'emploi, interdiction d'examen)</li> <li>Interdiction bancaire</li> <li>Dégradation de biens</li> <li>Perte de logement</li> <li>Perte d'emploi</li> <li>Séparation ou divorce</li> <li>Perte financière à la suite d'une escroquerie (ex. : après une tentative d'hameçonnage / <i>phishing</i>)</li> <li>Bloqué à l'étranger</li> <li>Perte de données clientèle</li> </ul>	<ul style="list-style-type: none"> <li>Affection psychologique grave (ex. : dépression, développement d'une phobie)</li> <li>Sentiment d'atteinte à la vie privée et de préjudice irrémédiable</li> <li>Sentiment de vulnérabilité à la suite d'une assignation en justice</li> <li>Sentiment d'atteinte aux droits fondamentaux (ex. : discrimination, liberté d'expression)</li> <li>Victime de chantage - <i>Cyberbullying</i> et harcèlement moral</li> </ul>
<p><b>4. Maximale</b></p>	<ul style="list-style-type: none"> <li>Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter</li> </ul>	<ul style="list-style-type: none"> <li>Affection physique de longue durée ou permanente (ex. : suite au non-respect d'une contre-indication)</li> <li>Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l'intégrité physique</li> </ul>	<ul style="list-style-type: none"> <li>Péril financier</li> <li>Dettes importantes</li> <li>Impossibilité de travailler</li> <li>Impossibilité de se reloger</li> <li>Perte de preuves dans le cadre d'un contentieux</li> <li>Perte d'accès à une infrastructure vitale (eau, électricité)</li> </ul>	<ul style="list-style-type: none"> <li>Affection psychologique de longue durée ou permanente</li> <li>Sanction pénale</li> <li>Enlèvement</li> <li>Perte de lien familial</li> <li>Impossibilité d'ester en justice</li> <li>Changement de statut administratif et/ou perte d'autonomie juridique (tutelle)</li> </ul>

## 5.2. Echelle de vraisemblance

• Niveaux de vraisemblance	• Description générique du niveau de vraisemblance d'une menace donnée
1. <b>Négligeable</b>	• 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. <b>Limité</b>	• 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. <b>Important</b>	• 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. <b>Maximal</b>	• 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).