**ANNEXE**

**ANALYSE D’IMPACT RELATIVE À LA PROTECTION DES DONNEES**

**Traitements de données à caractère personnel relatifs à l’usage de caméras individuelles par les agents de police municipale dans le cadre de leurs interventions**

## Responsable du traitement

Veuillez préciser le responsable du traitement et son adresse postale.

Responsable du traitement : Adresse :

# Table des matières

[Table des matières 11](#_TOC_250027)

[Présentation 13](#_TOC_250026)

* 1. Présentation générale 13
  2. Vue d’ensemble 14
     1. [*Traitements considérés* 14](#_TOC_250025)
     2. [*Textes applicables* 14](#_TOC_250024)
  3. Données, processus et supports 15
     1. [*Description des données, accédants, destinataires et durées de conservation* 15](#_TOC_250023)
     2. [*Données sensibles ou relatives aux condamnations pénales, infractions ou mesures de sûreté* 17](#_TOC_250022)
     3. [*Description des processus et supports* 18](#_TOC_250021)

1. [Principes fondamentaux 21](#_TOC_250020)
   1. Mesures garantissant la proportionnalité et la nécessité des traitements 21
      1. [*Finalités* 21](#_TOC_250019)
      2. [*Fondement* 23](#_TOC_250018)
      3. [*Minimisation des données* 23](#_TOC_250017)
      4. [*Qualité des données* 24](#_TOC_250016)
      5. [*Durées de conservation* 25](#_TOC_250015)
      6. [*Évaluation des mesures* 26](#_TOC_250014)
   2. Évaluation des mesures protectrices des droits des personnes concernées 26
      1. [*Mesures pour l’information des personnes* 26](#_TOC_250013)
      2. [*Mesures pour le recueil du consentement* 28](#_TOC_250012)
      3. [*Mesures pour les droits d’accès* 28](#_TOC_250011)
      4. *Mesures pour le droit à la portabilité* 28
      5. *Mesures pour les droits de rectification et d’effacement* 28
      6. *Mesures pour les droits à la limitation du traitement et d’opposition* 29
      7. *Mesures pour la sous-traitance* 30
2. [Etude des risques liés à la sécurité des données 31](#_TOC_250010)
   1. Évaluation des mesures 31
      1. [*Mesures contribuant à traiter des risques liés à la sécurité des données* 31](#_TOC_250009)
      2. [*Mesures générales de sécurité* 33](#_TOC_250008)
      3. [*Mesures organisationnelles (gouvernance)* 36](#_TOC_250007)
   2. Appréciation des risques : les atteintes potentielles aux droits et libertés 38
      1. [*Données essentielles* 38](#_TOC_250006)
      2. [*Analyse et estimation des risques* 38](#_TOC_250005)
3. [Validation de l’analyse d’impact 40](#_TOC_250004)
   1. Eléments utiles à la validation 40
      1. [*Synthèse relative à la conformité au RGPD* 40](#_TOC_250003)
      2. [*Synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques* liés à la sécurité des données 40](#_TOC_250002)
   2. [Avis du délégué à la protection des données de la commune 43](#_TOC_250001)
4. [Annexes 43](#_TOC_250000)
   1. Echelle de gravité 44
   2. Echelle de vraisemblance 48
   3. Modèle de mention d’information s’agissant des traitements relevant de la directive

dite « police-justice » (titre III de la loi n° 78-17 du 6 janvier 1978) 49

## Présentation

**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.

À 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’utili- sation 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.

En application de l’article L. 241-2 du code de la sécurité intérieure précité, le décret n° 2019-140 du 27 février 2019 précise 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 notam- ment leurs finalités, les données enregistrées, les modalités et leur durée de conservation, les conditions d’accès aux enre- gistrements et les modalités d’exercice des droits des personnes concernées.

L’article 45 de la loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés a modifié les articles

L. 241-1 et L. 241-2 du code de la sécurité intérieure relatifs à l’usage des caméras individuelles, autorisant désormais, d’une part, un accès direct aux images captées par les agents de police municipale ayant procédé à l’enregistrement au moyen de leur caméra individuelle afin de faciliter la recherche d’auteurs d’infractions, la prévention d’atteintes imminentes à l’ordre public, le secours aux personnes ou l’établissement fidèle des faits lors des comptes rendus d’interventions. D’autre part, la loi permet une transmission en temps réel des images en salle de commandement et aux agents impliqués dans la conduite et l’exécution de l’intervention, lorsque la sécurité des agents ou la sécurité des biens et personnes est menacée.

Tout en préservant les droits et intérêts de la population et des agents, ces dispositifs garantiront aussi une meilleure ges- tion et contextualisation des éventuelles accusations de fautes qui seraient commises par les agents et des infractions commises à l’encontre des agents de police municipale. Dans une démarche de rapprochement entre les forces de sécurité intérieure et la population, les caméras individuelles ainsi encadrées et assorties de garanties fortes pour les droits des personnes permettront en effet de retracer la vérité des faits et de rétablir une confiance partagée.

Enfin, le décret n° 2022-1409 du 7 novembre 2022 portant diverses dispositions relatives à la sécurité intérieure modifie les modalités d’enregistrement des images lors de l’utilisation de pistolet à impulsion électrique (PIE) en permettant désor- mais que celui-ci soit opéré par la caméra individuelle dont l’agent porteur de l’arme est doté, en plus de la possibilité

préexistante de dispositif d’enregistrement directement intégré au PIE. Le déclenchement de cet enregistrement est dé- sormais automatique. Cette utilisation des caméras individuelles est inclue dans les finalités énumérées à l’article R.241-9 du code de la sécurité intérieure et développées dans la présente AIPD.

**1.2.**

**Vue d’ensemble**

#### *Traitements considérés*

|  |  |
| --- | --- |
| **Description des traitements** | 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. |
| **Finalités des traitements** | Ces traitements ont pour finalités :   1. La prévention des incidents au cours des interventions des agents de police municipale ; 2. Le constat des infractions et la poursuite de leurs auteurs par la collecte de   preuves. |
| **Enjeux des traitements** | Dans un objectif de sécurité globale les traitements permettent une meilleure compréhension de la situation en cours de déroulement. En outre, les traitements permettent 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. |
| **Responsables des traitements** | Chaque responsable du service de la police municipale, maire ou président de l’établissement public de coopération intercommunale dans le cadre de l'autorité prévue au V de l'article L. 5211-9-2 du code général des collectivités territoriales sera responsable du traitement dans la commune |
| **Sous-traitant(s)** |  |

#### *Textes applicables*

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. En outre, il conviendra de conclure avec ce-dernier un contrat de sous-traitance conformément à l’article 96 de la loi du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.

|  |  |
| --- | --- |
| **Textes applicables au traitement** | **Modalité de prise en compte** |
| **Textes législatifs et réglementaires** | |
| Article L. 241-2 du code de la sécurité intérieure modifié | Décret en Conseil d’État, pris après avis de la  Commission nationale de l’informatique et des libertés |
| Dispositions générales de la loi n° 78-17 du 6 janvier 1978 relative à  l'informatique, aux fichiers et aux libertés | Toujours applicable |
| Titre III de la loi du 6 janvier 1978 | Le traitement (ou la partie de traitement)  poursuit des fins de protection contre les |

|  |  |
| --- | --- |
|  | menaces pour la sécurité publique et la  prévention de telles menaces |
| Article 31-I 1° ou II (sécurité publique) de la loi du 6 janvier 1978 | Le traitement intéresse la sécurité publique |
| Article 31-I 2° ou II (prévention, recherche, constatation, poursuite des infractions pénales ou exécution des condamnations ou des mesures de sûreté) de la loi du 6 janvier 1978 | Le traitement a pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de  sûreté |

**1.3.**

**Données, processus et supports**

#### *Description des données, accédants, destinataires et durées de conservation*

|  |  |  |  |
| --- | --- | --- | --- |
| **Données** | **Accédants et destinataires** | **Durée de**  **conservation** | **Justification** |
| Images et sons captés par les caméras individuelles utilisées par les agents de police municipale | Dans la limite de leurs attributions respectives et de leur besoin d’en connaître, peuvent êtres accédants de tout ou partie des données et informations enregistrées dans les traitements, les personnes suivantes :   1. Le maire ou le président de l’établissement public de coopération intercommunale lorsque les agents de la police municipale agissent sous son autorité dans le cadre prévu au V de l'article L. 5211 9 2 du CGCT ; 2. le responsable du service de la police municipale; 3. les agents de la police municipale individuellement désignés et habilités par le maire ou le président de l’établissement public de coopération intercommunale ; 4. L’agent auquel la caméra individuelle est fournie, dans les conditions définies au II de l’article R. 241-11 du code de la sécurité intérieure pour les seules données mentionnées au 1° de l’article R. 241-10 du même code.   Peuvent recevoir communication dans les conditions prévues au I de l’article R. 241-11 du code de la sécurité intérieure, à raison de leur attribution et dans la limite, des données mentionnées au 1° de l’article R. 241-10 du même code :   * 1. Les agents de police municipale affectés dans les salles de commandement ;   2. Les autorités administratives et judiciaires dont la présence est | Un mois à compter du jour de l’enregistrement des données. Lorsque les données ont été extraites ou transmises pour les besoins d’une procédure judiciaire, administrative ou disciplinaire, dans le délai de un mois, elles sont  conservées selon  les règles propres à chacune de ces procédures par l’autorité qui en a la charge | La collecte de ces données est nécessaire à la prévention des incidents au cours des interventions des agents, en permettant de replacer dans un contexte objectif les circonstances des interventions concernées.  Elle permet également la collecte de preuves dans le cadre du constat des infractions et la poursuite de leurs auteurs, en  permettant de confirmer l’identification des personnes concernées et le déroulements des faits auxquels auraient assisté les agents porteurs de  la caméra. |
| Jour et plages horaires d’enregistrement | Besoin de  traçabilité sur  l’emploi des caméras par les agents porteurs. |

|  |  |  |  |
| --- | --- | --- | --- |
| Identification de l’agent porteur de la caméra lors de l’enregistrement des données | requise dans les postes de commandement ;   1. Les agents de police municipale impliqués dans la conduite et l’exécution de l’intervention.   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 :   * 1. Les officiers et agents de police judiciaire de la police nationale et de la gendarmerie nationale ;   2. les 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 ;   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 ;   4. Les agents chargés de la formation des personnels. |  | La collecte de ces données est  nécessaire à l’identification des agents porteurs des caméras.  Elles permettent notamment de garantir le suivi des enregistrements effectués par les agents porteurs.  Lorsque les caméras individuelles ne  permettent pas d’enregistrer, en même temps que les images et les sons, l’identité de l’agent porteur de la caméra ou le lieu où ont été  collectées les  données, les personnes mentionnées au 1°,  2° et 3° du I de  l’article R. 241-12 doivent être en mesure de justifier de ces  informations. |
| Lieu où ont été collectées les données |  | Besoin de traçabilité sur l’emploi des caméras par les agents porteurs. |
| Identifiant de l’auteur, date, | 1. Responsable du service de la police municipale ; 2. Le maire ou le président de l’établissement public de coopération intercommunale dans le cadre de l’autorité prévue au V de l’article L. 5211- 9-2 du code général des collectivités territoriales ainsi que les membres des instances disciplinaires et les agents en | Trois ans à compter | Les données de |
| heure et motif de | du jour de | traçabilité des |
| l’opération de collecte, de | l’opération de | opérations de |
| modification, de | collecte, de | consultation et |
| consultation, de | modification, de | d’extraction sont |
| communication et | consultation, de | utilisées |
| d’effacement des données à | communication et | exclusivement dans |
| caractère personnel et | d’effacement des | le cadre d’une |
| informations, et, le cas | données à | enquête judiciaire, |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| échéant, | destinataire | des | charge de l’instruction des dossiers présentés à ces instances ;   1. Officiers et agents de police judiciaire de la police nationale et de la gendarmerie nationale ; 2. Agents des services d’inspection générale de l’État, dans les conditions prévues à l’article L. 513-1 du code de la sécurité intérieure. | caractère personnel | administrative ou |
| données |  |  | et informations. | d’une procédure |
|  |  |  |  | disciplinaire. Une |
|  |  |  |  | durée de |
|  |  |  |  | conservation de |
|  |  |  |  | trois ans permet de |
|  |  |  |  | bénéficier d’un |
|  |  |  |  | délai suffisant pour |
|  |  |  |  | permettre de |
|  |  |  |  | déceler des |
|  |  |  |  | anomalies ou |
|  |  |  |  | comportements |
|  |  |  |  | qui s’inscrivent |
|  |  |  |  | dans la durée. |

#### *Données sensibles ou relatives aux condamnations pénales, infractions ou* mesures de sûreté

|  |  |  |
| --- | --- | --- |
| **Catégorie** | **Collecte dans le traitement (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 et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : injures subies à raison de la couleur lors d’une manifestation sportive, récréative ou culturelle à laquelle l’agent est affecté. |
| Les opinions politiques | Oui | L’enregistrement de ces données n’est pas réalisé à dessein, mais de telles données peuvent être collectées à partir des faits visibles et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : affectation à la sécurité d’une manifestation sportive, récréative ou culturelle au cours de laquelle survient une scène des dégradations (tags politisés) |
| Les convictions religieuses | Oui | L’enregistrement de ces données n’est pas réalisé à dessein, mais de telles données peuvent être collectées à partir des faits visibles et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : intervention à proximité de lieux de culte où des dégradations sont commises (tags antisémites, anti-musulmans, anti-chrétiens) dont les convictions religieuses peuvent concerner la victime ou l’auteur présumé. |
| Les convictions philosophiques | Oui | L’enregistrement de ces données n’est pas réalisé à dessein, mais de telles données peuvent être collectées à partir des faits visibles et/ou audibles |

|  |  |  |
| --- | --- | --- |
|  |  | enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : affectation à la sécurité d’une manifestation sportive, récréative ou culturelle au cours de laquelle des participants font acte de dégradations au nom de leurs convictions philosophiques. |
| L’appartenance syndicale | Oui | L’enregistrement de ces données n’est pas réalisé à dessein, mais de telles données peuvent être collectées à partir des faits visibles et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : constat d’occupation en réunion d’espaces communs d’immeubles collectifs d’habitation par des manifestants syndiqués ou des délégués syndicaux. |
| La santé | Oui | L’enregistrement de ces données n’est pas réalisé à dessein, mais de telles données peuvent être collectées à partir des faits visibles et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : au cours de l’intervention, les images captées peuvent révéler l’état d’invalidité d’une personne (fauteuil roulant, matériel médical…). |
| 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 à partir des faits visibles et/ou audibles enregistrés dans le fichier vidéo, en ce qu’ils font partie des circonstances de l’intervention de l’agent porteur de la caméra.  *Exemple* : intervention suite à des menaces ou à une agression homophobe, les propos de l’auteur étant rapportés par la victime. |
| 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 | Oui | L’enregistrement audiovisuel pourra faire apparaître, directement ou indirectement, des échanges entre usagers et les agents de police municipale évoquant des condamnations pénales d’un ou plusieurs protagonistes. |
| Les infractions | Oui | L’enregistrement audiovisuel pourra faire apparaître, directement ou indirectement, des échanges entre usagers et les agents de police municipale évoquant des infractions commises par un ou plusieurs protagonistes. Les agents de police municipale peuvent également être témoins directs de la commission d’une infraction constatée par l’enregistrement vidéo. |
| Les mesures de sûreté | Oui | L’enregistrement audiovisuel pourra faire apparaître, directement ou indirectement, des échanges entre usagers et les agents de police municipale évoquant des mesures de sûreté dont faisait l’objet un ou plusieurs protagonistes au moment de l’incident. |

#### *Description des processus et supports*

|  |  |  |
| --- | --- | --- |
| **Processus** | **Description détaillée du processus** | **Supports des données concernés** |

|  |  |  |
| --- | --- | --- |
|  | 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 1er 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 : |  |
|  | 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 ; |
|  | 2° Un dossier technique de présentation du traitement envisagé ; |
| Autorisation d’utilisation des | 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 de la partie  réglementaire du code de la sécurité intérieure |
| caméras  individuelles | 4°L’engagement de conformité destiné à la CNIL faisant référence aux dispositions de la section 2 du chapitre unique du titre IV du livre II de la partie réglementaire du code de la sécurité intérieure et précisant le nombre de caméras et le service utilisateur ; |
|  | 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 demande est présentée par l’ensemble des maires des communes concernées. |
|  | L’enregistrement audiovisuel des interventions des agents de police municipale est autorisé par arrêté du préfet de département, à Paris, par le préfet de police, 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. En application du IV de l’article 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. |
| Enregistrement audiovisuel | 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 | Les enregistrements audiovisuels sont conservés dans les mémoires internes non amovibles des caméras des agents qui en |

|  |  |  |
| --- | --- | --- |
|  | 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. | sont dotés jusqu’au retour au service des agents.  En cas de transmission en temps réel des données au poste de commandement du |
|  | service concerné ou aux personnels |
|  | impliqués dans la conduite et l’exécution |
|  | de l’intervention, le flux est transmis en |
|  | streaming et ne fait pas l’objet d’un |
|  | enregistrement au sein d’un serveur en |
|  | salle de commandement. Aucun |
|  | déclenchement de la transmission en |
|  | temps réel des images d’une ou plusieurs |
|  | caméras n’est opérée à distance. |
|  | 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. | Les enregistrements sont intégralement transférés sur le support informatique sécurisé mis en place par la commune : le déchargement de la caméra s’opère   * 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. Les enregistrements sont conservés sur ce serveur dans un local aux accès limités doté d’un logiciel permettant l’effacement automatisé des informations après un mois et enregistrant la traçabilité des opérations. Les données transférées sont systématiquement effacées des mémoires de la caméra.  Veuillez sélectionner ici l’un de ces modes de déchargement de la caméra. |
| Transfert des données | Lorsque la sécurité des agents ou la sécurité des biens et des personnes est menacée, les images captées peuvent être transmises en temps réel au poste de commandement du service concerné et aux personnels impliqués dans la conduite et l’exécution de l’intervention. La sécurité des agents, des biens ou des personnes est réputée menacée lorsqu’il existe un risque immédiat d’atteinte à leur intégrité. À titre d’exemples, de telles circonstances se rapportent à des situations telles que l’intervention des agents peut susciter des réactions agressives ou hostiles ; d’autre part, des situations où il est possible de matérialiser les infractions (à l’instar d’une atteinte au domaine public) ; des situations où il est requis d’assurer la sécurité des rassemblements de personnes sur la voie publique ou dans les lieux ouverts au public (manifestations sportives, récréatives et culturelles, notamment). La transmission en temps réel permet donc de rendre compte de la situation et d’adapter les effectifs et les moyens à engager. |
| Consultation des données | Les enregistrements effectués à l’aide des caméras indivi- duelles peuvent être consultés à l’issue de l’intervention, après leur transfert sur un support informatique sécurisé, par les seuls accédants aux traitements. La consultation des images après l’intervention apporte une aide aux agents inter- pellateurs lors de la rédaction du procès-verbal pour corriger des imprécisions éventuelles. | Les enregistrements sont conservés sur un support informatique sécurisé dans un local aux accès limités doté d’un logiciel permettant l’effacement automatisé des informations après un mois et enregistrant la traçabilité des opérations. |

|  |  |  |
| --- | --- | --- |
|  | Les images captées au moyen de caméras individuelles peuvent également être consultées en temps réel au poste de commandement du service concerné et aux personnels impliqués dans la conduite et l’exécution de l’intervention, lorsque la sécurité des agents ou la sécurité des biens et des personnes est menacée.  Enfin, dans le cadre d’une procédure judiciaire ou d’une intervention, les agents auxquels les caméras individuelles sont fournies peuvent avoir accès directement aux enregistrements auxquels ils procèdent afin de faciliter la recherche d’auteurs d’infractions, la prévention d’atteintes imminentes à l’ordre public, le secours aux personnes ou l’établissement fidèle des faits lors des comptes rendus d’intervention. À titre d’exemples, la consultation en intervention permet le signalement d’une personne ayant pris la fuite lors d’un contrôle ou de s’assurer du modèle d’un véhicule ou d’un numéro d’immatriculation lors d’un refus d’obtempérer. |  |
| Extraction des données | Le responsable du service de la police municipale, le maire ou le président de l’établissement public de coopération intercommunale dans le cadre de l'autorité prévue au V de l'article L. 5211-9-2 du code général des collectivités territoriales et les agents de police municipale individuellement désignés et habilités par responsable du service de la police municipale, le maire ou le président de l’établissement public de coopération intercommunale 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. |

## Principes fondamentaux

**2.1.**

**Mesures garantissant la proportionnalité et la nécessité des traitements**

#### *Finalités*

|  |  |
| --- | --- |
| **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 pé- nale, les agents de police municipale sont des agents de police ju-  diciaire adjoints, qui ont pour mission de seconder, dans l’exercice |

Veuillez préciser les modalités d’anonymisation des données à caractère personnel utilisées à cette fin ainsi que la fréquence de ces formations

|  |  |
| --- | --- |
|  | de leurs fonctions, les officiers de police judiciaire, de rendre compte à leurs chefs hiérarchiques de tous crimes, délits ou con- traventions dont ils ont connaissance ainsi que de constater les in- fractions à la loi pénale et de recueillir tous les renseignements en vue de découvrir les auteurs de ces infractions. 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).  En application du deuxième alinéa de l’article L. 511-1 du code de la sécurité intérieure, les agents de police municipale peuvent ver- baliser les contraventions aux arrêtés de police du maire.  En outre, ce même article permet aux agents de police municipale de constater par procès-verbaux les contraventions aux disposi- tions du code de la route dont la liste est fixée par décret en Con- seil d’État (R. 130-2 du code de la route) ainsi que certaines con- traventions 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).  Enfin, des textes spécifiques les rendent compétents pour relever des infractions dans un certain nombre de domaines (chiens dan- gereux, police de la conservation du domaine routier, police de l’environnement, nuisances sonores, accès aux parties communes  d’immeuble à usage d’habitation...). |
| Formation et pédagogie des agents de police municipale | Permettre une mise en situation des agents de police municipale afin de mieux appréhender les risques encourus lors de leurs interventions.  Les données utilisées pour ces finalités sont anonymisées. |

#### *Fondement*

Les traitements, mis en œuvre par les autorités compétentes pour le compte de l’État et ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales lors des interventions des agents de police municipale. À ce titre, ces traitements relèvent des dispositions du titre III de la loi du 6 janvier 1978.

Eu égard aux finalités poursuivies et à la nature des données potentiellement collectées, les traitements relèvent également du I et II de l’article 31 de la même loi. Les traitements sont donc autorisés par un décret en Conseil d’État après avis de la CNIL.

Il est proposé de faire de ce décret un acte cadre permettant aux différentes communes concernées de mettre en œuvre de tels traitements par engagement de conformité, transmis à la CNIL en application du IV de l’article 31 de la loi n° 78-17 du 6 janvier 1978 et de l’article R.241-16 du code de la sécurité intérieure.

#### *Minimisation des données*

|  |  |  |  |
| --- | --- | --- | --- |
| **Détail des données traitées** | **Catégories** | **Justification du besoin et de la pertinence des données** | **Mesures de minimisation** |
|  |  |  | - L’article L. 241-2 du code de la sécurité intérieure pose le principe selon lequel l’enregistrement par le biais des caméras individuelles n’est pas permanent. |
|  |  |  | - Les personnes filmées sont informées préalablement au déclenchement de l’enregistrement. |
| Images et sons captés par les caméras individuelles utilisées par les agents de police municipale | Données sensibles | Données indispensables en cas de procédure judiciaire, administrative ou disciplinaire car constitutives d’éléments de preuves | * Les agents de police municipale utilisateurs des caméras mobiles individuelles sont informés de la législation applicable à ces dispositifs et formés à leur utilisation. Lorsque ces données sont utilisées à des fins pédagogiques et de formation, elles font l’objet d’une anonymisation. * Les données sont effacées automatiquement à l’expiration d’un délai d’un mois. |
|  |  |  | - Il est interdit de sélectionner dans les traitements une catégorie particulière de personnes à partir des données relevant du I de l’article 6 de la loi n° 78-17 du 6 janvier 1978 |
|  |  |  | - Lorsque les enregistrements font l’objet d’une transmission en temps réel dans les conditions prévues au I de l’article R. 241- 11 du code la sécurité intérieure, ils ne peuvent faire l’objet d’un enregistrement |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  |  | par le poste de commandement du service concerné et par les personnels impliqués dans la conduite et l’exécution de  l’intervention. |
|  |  |  | Données indispensables en cas |  |
| Jour et plages d’enregistrement | horaires | Données non  sensibles | de procédure judiciaire, administrative ou disciplinaire  pour vérifier la date de | Veuillez compléter ces trois rubriques |
|  |  |  | l’enregistrement |  |
|  | | Données | Données indispensables en cas |  |
| Identification de l’agent porteur de la caméra lors de l’enregistrement des données | | non sensibles | 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 | Le cas échéant, la géolocalisation permet de garantir la fiabilité de ces données. |

#### *Qualité des données*

##### Mesures pour la qualité des données

Intégrité des images et sons captés

Horodatage et localisation des images et sons captés

Veuillez adapter ces mentions en fonction du choix effectué d’équiper ou non les agents de police municipale d’une caméra disposant d’un GPS.

##### Modalités de mise en œuvre

Les données collectées sont exclusivement tirées des enregistrements audiovisuels. Il n’est pas possible de procéder à une rectification matérielle des images et sons, ou de supprimer ces données avant la fin de leur durée légale de conservation dans le logiciel.

Il est recommandé aux communes de se doter d’un dispositif permettant d’horodater et de localiser automatiquement les images enregistrées. Les caméras disposant d’un GPS permettent une géolocalisation automatique lors de l’enregistrement. Néanmoins, 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 et les personnes mentionnées aux 1°, 2° et 3° du I de l’article R.241-12 CSI doivent être en mesure de justifier de ces informations.

Port de la caméra au niveau du sternum afin de garantir une prise de vue grand angle et une stabilité des images

Qualité infrarouge pour l’enregistrement des images nocturnes

Veuillez ici préciser si vous avez

opté pour une caméra infrarouge.

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.

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.

#### *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 | 1 mois à compter du jour de  l’enregistrement des données.  Lorsque les données ont été extraites ou transmises pour les besoins d’une procédure judiciaire, administrative ou disciplinaire, dans le délai d’un mois, elles sont  conservées selon les règles propres à chacune de ces procédures par l’autorité qui en a la charge. | 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. La conservation des données est nécessaire à l’exercice des missions de police judiciaire et aux fins de consultation par les services d’enquête et les autorités de contrôles. | Au terme du délai de 1 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 | 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 | Conservation nécessaire en cas de poursuites dans le cadre d’une procédure judiciaire, administrative ou disciplinaire. |
| Lieu où ont été collectées les données |  | Conservation nécessaire en cas de poursuites dans le cadre d’une procédure judiciaire, administrative  ou disciplinaire. |  |
| Identifiant de | Trois ans à compter | Les données de traçabilité des |  |
| l’auteur, date, heure | du jour de | opérations de consultation et |
| et motif de | l’opération de | d’extraction sont utilisées |
| l’opération de | collecte, de | exclusivement dans le cadre d’une |
| collecte, de | modification, de | enquête judiciaire, administrative ou |
| modification, de | consultation, de | d’une procédure disciplinaire. Une |
| consultation, de | communication et | durée de conservation de trois an |
| communication et | d’effacement des | permet de bénéficier d’un délai |
| d’effacement des | données à caractère | suffisant pour permettre de déceler |
| données à caractère | personnel et | des anomalies ou comportements qui |
| personnel et | informations. | s’inscrivent dans la durée. |
| informations, et, le |  |  |
| cas échéant, |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| destinataire des  données |  |  |  |

#### *Évaluation 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 31 et du 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  « *lorsque se produit ou est susceptible de se produire un incident eu égard aux circonstances de l’intervention ou au comportement des personnes concernées* ». et  l’enregistrement n’est pas permanent | Acceptable |  |
| Qualité des données : exactes et tenues à jour | Acceptable |  |
| Durée de conservation : limitée à un mois | Acceptable | Mesure préventive : les données sont  automatiquement et définitivement effacées à l’expiration du délai d’un mois |

**2.2.**

**Évaluation des mesures protectrices des droits des personnes concernées**

#### *Mesures pour l’information des personnes*

À titre liminaire, les traitements relevant du I et du II de l’article 31 et du titre III de la loi du 6 janvier 1978, ils seront autorisés par un décret en Conseil d’État qui sera publié au *Journal officiel*.

Les agents de police municipale utilisateurs des caméras individuelles 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 fournies par le service et 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 ».*

Il est à noter que si, dans ce cas, le déclenchement de l'enregistrement peut, par exception, ne pas faire l'objet de cette information lorsque « les circonstances l'interdisent », ces circonstances recouvrent les seuls cas où cette information est rendue impossible pour des raisons purement matérielles et indépendantes des motifs de l'intervention.

Aussi, ces exceptions respectent les principes de nécessité et de proportionnalité. Si l’exception est caractérisée, l’information de la personne enregistrée peut être faite de manière différée, dès lors que les circonstances interdisant l’information immédiate des personnes filmées ont cessé et au plus tard, à l’issue de l’intervention.

L’article L. 241-2 du code de la sécurité intérieure dispose par ailleurs qu’« *une information générale du public sur l’emploi de ces caméras est organisée par le maire de chaque commune sur le territoire de laquelle ces agents sont affectés.* »

En outre, 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* ».

Enfin, les informations prévues à l’article 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 | Une information générale du public sur l’emploi de ces caméras est |
| /confidentialité | organisée par le maire de chaque commune sur le territoire de laquelle |
|  | ces agents sont affectés, conformément au quatrième alinéa de l’article |
|  | L. 241-2 du code de la sécurité intérieure ainsi qu’à l’article R.241-15 du |
| Veuillez adapter les mentions surlignées ci-  contre en précisant les modalités d’information des personnes concernées : sur le site internet de votre commune ou par voie d’affichage en mairie. | même code. 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 délivrée sur le site internet de la |
|  | commune ou, à défaut, par voie d’affichage en mairie. |
| Possibilité d’accéder aux conditions  d’utilisation/confidentialité | Sur le site internet de la commune ou, à défaut, par voie d’affichage en  mairie. |
| Conditions lisibles et compréhensibles | Ces informations figurent sur le site internet de chaque commune, ou  à défaut, par voie d’affichage en mairie |
| Existence de clauses spécifiques au dispositif | Non applicable |
| Présentation détaillée des finalités des | Sur le site internet de la commune ou, à défaut, par voie d’affichage en |
| traitements de données (objectifs précis, | mairie. Le dispositif ne comporte pas de croisement de données. |
| croisements de données s’il y a lieu, etc.) |  |
| Présentation détaillée des données | Les personnes concernées sont informées du déclenchement de |
| personnelles collectées | l’enregistrement sauf si les circonstances l’interdisent. |
|  | La liste des données est communiquée sur le site internet de la |
|  | commune ou, à défaut, par voie d’affichage en mairie. |
| 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 | Sur le site internet de la commune ou, à défaut, par voie d’affichage |
| concernée (retrait du consentement, | en mairie. |
| suppression de données, etc.) |  |

|  |  |
| --- | --- |
| 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  Ce cas ne devrait pas se présenter. |
| Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de  confidentialité |

#### *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 et du titre III de la loi n°78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers, et aux libertés.

#### *Mesures pour les droits d’accès*

Le droit d’accès prévu à l’article 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 individuelles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes, dans les conditions prévues au premier alinéa de l’article L. 512-2 du code de la sécurité intérieure.

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 107 de la même loi.

À titre d’exemple, une restriction au droit d’accès ne peut avoir lieu si la demande est excessive ou infondée. De même, la demande ne pourra aboutir si le délai de 1 mois est dépassé, les images ayant été détruites. Enfin, si les images prises par la caméra individuelle ont été intégrées à une procédure judiciaire, l’accès à celles-ci est régi par le code de procédure pénale.

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 108 de la même loi.

* + 1. *Mesures pour le droit à la portabilité*

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

* + 1. *Mesures pour les droits de rectification et d’effacement*

Le droit de rectification s’exerce directement auprès du maire ou de l’ensemble des maires des communes lorsque les agents susceptibles d’être équipés de caméras individuelles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes, dans les conditions prévues au premier alinéa de l’article

L. 512-2 du code de la sécurité intérieure.

Le droit de rectification est applicable aux traitements, celui-ci ne pourra consister à matériellement modifier les images et/ou le son captés dès lors que cela porterait atteinte à leur intégrité.

Le droit d’effacement prévu à l’article 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 individuelles sont employés par un établissement public de coopération intercommunale et mis à disposition de plusieurs communes, dans les conditions prévues au premier alinéa de l’article L. 512-2 du code de la sécurité intérieure.

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, les droits de rectification et d’effacement peuvent 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 restrictions 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.

* + 1. *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 s’exerce directement auprès du maire ou de l’ensemble des maires des communes lorsque les agents susceptibles d’être équipés de caméras individuelles 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 à la limitation 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.

Le droit d’opposition prévu à l’article 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 au présent traitement.

Cette exclusion se justifie au regard des finalités des traitements et figure dans l’acte réglementaire les autorisant.

* + 1. *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.

Veuillez 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.

* + 1. *Mesures pour le transfert de données en dehors de l’Union européenne*

Les données enregistrées dans le traitement peuvent faire l’objet d’un transfert de données en dehors de l’Union européenne, en cas de recours à un sous-traitant étranger, lorsque celui-ci garantit un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux des personnes à l’égard du traitement dont ces données font l’objet ou peuvent faire l’objet.

En tout état de cause, le recours à un sous-traitant étranger, impliqué dans un transfert de données à caractère personnel en dehors de l’Union européenne, devra respecter les règles et, le cas échéant, les garanties appropriées prévues 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 (Articles 112 à 114) » de la loi n° 78-17 du 6 janvier 1978 modifiée dite « informatique et libertés ».

## Etude des risques liés à la sécurité des données

**Évaluation des mesures**

#### *Mesures contribuant à traiter des risques liés à la sécurité des données*

##### Mesures générales de sécurité

Chiffrement

##### Modalités de mise en œuvre

Les systèmes commercialisés prévoient des enregistre- ments chiffrés sur le disque dur de la station. Il existe plu- sieurs modes de cryptage en fonction du choix effectué par les communes mais la commune devra prévoir *a mi- nima* un chiffrement conforme à l’état de l’art. Seul l’ad- ministrateur du système a les clefs du chiffrement pour les relectures et extractions. Chaque commune 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.

##### Acceptable / améliorable

Acceptable

##### Mesures correctives

Veuillez adapter ces mentions en précisant le mode de

Un cryptage *via* au moins un procédé de chiffrement de-

vra être effectué sur les données transmises en temps

réel vers le poste de commandement du service con- cerné et aux personnels impliqués dans la conduite et l’exécution de l’intervention est prévu.

Protection des sites web

Pour la grande majorité des communes utilisatrices de caméras individuelles, le support informatique sécurisé est installé hors réseau Internet afin d’éviter tout piratage des informations collectées. Les communes ont également la possibilité de recourir à un hébergement *cloud* en cas de nécessité.

Veuillez adapter ces mentions en précisant si le support informatique sécurisé est installé hors réseau ou en hébergement cloud

Cloisonnement des données (par rapport au reste

données de l'organisme et les données de ses autres clients, en définissant très précisément les lieux dans lesquels les données sont susceptibles d'être stockées, et les pays depuis lesquels les données stockées dans le *cloud* sont susceptibles d'être accessibles.

Pour la grande majorité des communes utilisatrices de caméras individuelles, le support informatique sécurisé

services *cloud* une séparation *a minima* logique entre les

*cloud* notamment en imposant au fournisseur de

vigilance particulière lors du recours à un hébergeur

particulier, chaque commune devra faire preuve d’une

les recommandations de la CNIL1 sur le sujet. En

En cas d’hébergement *cloud*, les prestataires respectent

Veuillez 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.

1 *Cf.* Recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud computing* disponibles à l’adresse sui- vante : https[://w](http://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_sous-)ww[.c](http://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_sous-)n[il.fr/sites/default/files/typo/document/Recommandations\_pour\_les\_entreprises\_qui\_envisagent\_de\_sous-](http://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_sous-) crire\_a\_des\_services\_de\_Cloud.pdf

du système d’information)

installé hors réseau Internet afin d’éviter tout piratage des informations collectées.

Sécurité physique

Contrôle des accès logiques et sécurité des transferts de données

Les locaux où sont entreposés les supports informatiques sécurisés des services de police municipale et la salle de commandement vers laquelle sont transmis les enregistrements en temps réel 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 après utilisation, et les personnes, assurant le cas échéant la maintenance, n’interviennent qu’en présence du responsable du service, désigné par le maire.

Il n’est possible d’accéder aux données qu’après une authentification.

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 1 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).

Les enregistrements sont intégralement transférés sur le support informatique sécurisé mis en place par la commune : le déchargement de la caméra s’opère 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. Les enregistrements sont conservés sur ce serveur dans un local aux accès limités doté d’un logiciel permettant l’effacement automatisé des informations après un mois et enregistrant la traçabilité des opérations. Les données transférées sont systématiquement effacées des mémoires de la caméra.

Acceptable

Acceptable

Veuillez sélectionner le mode

d’ è

Veuillez sélectionner ici l’un de ces modes de déchargement de la caméra.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Chaque commune fera son possible pour mettre en place des mesures destinées à alerter en cas de modification non désirée ou de disparition de données à caractère personnel (fonction de hachage, signature électronique, prévenir des injections SQL, etc.) lors du déchargement de la caméra et de la conservation des enregistrements. Ces mesures devront appropriées et suffisamment robustes afin d’être adaptées par rapport au risque. Une attention particulière devra être portée sur la restriction des droits des agents utilisateurs afin de lutter contre les risques de suppression des données avant échéance. |  |  |
| Journalisation | Chaque opération de collecte, de modification, de consultation, de communication et d’effacement de données fait l’objet d’un enregistrement dans le traitement, y compris lorsque la consultation des données a lieu dans le cadre de l’intervention. Cette consignation comprend :   * les matricules, nom, prénom et grade des agents procédant à l’opération de consultation, d’extraction et d’effacement ; * la date et l’heure de la consultation et de l’extraction ainsi que le motif judiciaire, administratif, disciplinaire ou pédagogique ; * le service ou l’unité destinataire des données ; * l’identification des enregistrements audiovisuels extraits et de la caméra dont ils sont issus.   Ces informations sont conservées pendant trois ans. | Acceptable |  |
| Association des métadonnées et des flux vidéo | Dans la mesure du possible, chaque commune  s’efforcera de rechercher la mise en place de solutions A compléter le cas  techniques permettant de garantir la bonne association échéant. des métadonnées aux flux vidéo captés (identification de  l’agent porteur lors de la captation, horodatage,  localisation, …). | | |

#### *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 1 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

dispositif du support informatique hors réseau et d’un

La lutte contre les logiciels malveillants est garantie par le

serveur dédié sécurisé.

|  |
| --- |
| 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 permettant de filtrer les flux |
| entrants/sortants du réseau (firewall, proxy, etc.) et de |
| faire remonter les événements de sécurité de l'antivirus |

sur un serveur centralisé pour analyse statistique et gestion des problèmes *a posteriori* (dans le but de détecter un serveur infecté, un virus détecté et non éradiqué par l'antivirus, etc.).

Veuillez adapter ces mentions en fonction du choix opéré : installation hors réseau ou en cloud et évaluer la mesure

Il est également recommandé d’installer un programme de lutte contre les logiciels espions (anti-spyware) sur les postes de travail, le configurer et le tenir à jour.

Dans l’hypothèse d’une prestation d’hébergement en cloud, le prestataire s’engage à garantir la confidentialité et l’intégrité des images ainsi qu’à suivre les mêmes indications et recommandations visées au sein de la mesure précitée « Protection des sites web » au 3.1.1.

Mot de passe

Il n’est possible d’accéder aux données qu’après une authentification.

Cette authentification s’effectue par le biais de mots de passe individualisés avec contrôle des logs de connexion

Améliorable

La doctrine de la CNIL prévue aux termes de sa délibération n° 2022-100 du 21 juillet

2022 portant

adoption d'une

Veuillez préciser cela par la doctrine retenue au serin

### 34

de la commune en matière de mots de passe

d

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | | | |  | recommandation relative aux mots de passe et autres secrets partagés et abrogeant la délibération n° 2017-  012 du 19 janvier  2017 sera diffusée. |
| Sécurité des sites web | Il est fait en sorte que les caractéristiques des sites web ne soient pas exploitées pour porter atteinte aux données à caractère personnel (référentiel général de sécurité, chiffrement TLS des flux, politique de dépôt de cookies, audits de sécurité, etc.). En particulier, il est recommandé que le chiffrement des flux soit garanti par le protocole TLS ; le serveur web sera ainsi configuré de sorte à ce qu’il n'accepte que ce type de protocole (sera exclu notamment le protocole SSL). | | | | Acceptable |  |
| Sauvegardes | Chaque commune devra faire son possible pour garantir et rétablir la disponibilité des données à caractère personnel (réalisation régulière de sauvegardes régulière, de tests de restauration, etc.). Programmation des conservations à un 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) |  | Dans l’hypothèse d’une transmission en temps réel | | Veuillez adapter ces mesures de sécurité en fonction des choix techniques opérés :   * Transmission en temps réel ou non (mesure à évaluer) ; * Installation hors réseau | | |
| d’images et sons au poste de commandement et du | |
| service concerné et aux personnels impliqués dans la | |
| conduite et l’exécution de l’intervention, il est nécessaire | |
| que chaque caméra dispose d’une carte SIM lui | |
| permettant d’accéder au réseau Internet ou soit équipé | |
| d’un système Bluetooth pour procéder à une telle | |
| transmission. La sécurisation de cette transmission par | |
| Internet *via* les réseaux radio disponibles nécessite de | |
| programmer un protocole de reconnaissance et | |
| d’échanges réciproque entre le serveur du centre de | |
| commandement et chaque caméra. Ce protocole est | |
| paramétrable avant la mise en service de l’outil. | | ou hébergement en clou | | |
| Dans l’hypothèse d’une prestation d’hébergement en | | (mesure à évaluer). | | |
| cloud, le prestataire s’engage à sécuriser les canaux | |
| informatiques et pour ce faire à suivre les mêmes | |
| indications et recommandations en matière | |
| d’hébergement *cloud* visées au sein de la mesure précitée | |
| « Protection des sites web » au 3.1.1. |  |
| 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 | |  | Acceptable |  |
| sécurisés des services de police municipale et la salle de | |

### 35

Veuillez sélectionner le mode d’accès choisi.

Protection contre les sources de risques non humaines

Acceptable

Le support informatique est installé hors réseau et les en- registrements sont cryptés sur le disque dur de la station.

Éloignement des sources de risques

Acceptable

Le serveur dédié est placé dans un local dédié sous con- trôle d’accès physique.

Sécurité des matériels

commandement vers laquelle sont transmis les enregistrements en temps réel 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.

Les locaux des services de police municipale doivent prévoir des mesures de protections contre les risques.

Veuillez préciser les mesures de protection de vos locaux contre les risques non humains (détecteur sismique, incendie…) et évaluer la mesure

#### *Mesures organisationnelles (gouvernance)*

##### Mesures générales de sécurité

Organisation

Politique (gestion des règles)

##### Modalités de mise en œuvre

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.

Veuillez adapter ces mentions en précisant l’organisation mise en place et évaluer la mesure

Formation, charte informatique, doctrine d’emploi

##### Acceptable / améliorable

##### Mesures correctives

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.

Veuillez 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.

Gestion des risques Gestion des projets

Traçabilité des connexions consultables sur le journal automatique

Le choix des dispositifs relève du responsable du service de police municipale. Le représentant de l’Etat vérifie, préalablement à l’autorisation, la conformité

Acceptable

Veuillez apporter des précisions sur la justification du choix du dispositif et évaluer la mesure

### 36

Veuillez apporter des précisions sur la procédure en cas d’incidents et évaluer la mesure.

la

|  |  |  |  |
| --- | --- | --- | --- |
|  | du dispositif aux dispositions du code de la sécurité  intérieure. |  |  |
| Gestion des incidents et des violations de  données | Enregistrement au journal de la défaillance constatée et alerte les agents du dysfonctionnement constaté. |  |  |
| Gestion des personnels | Les accès aux traitements sont restreints à un nombre Acceptable limité d’agents qui sont individuellement désignés. Les  agents sont formés aux usages et à l’emploi des Veuillez apporter des précisions sur caméras individuelles du déclenchement au transfert formation dispensée aux agents. sur le support informatique sécurisé au retour du  service. | | |
| Relations avec les tiers | Non applicable |  |  |
| 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 |  |

37

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

#### *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, en tous lieux.  Les images captées peuvent être transmises en temps réel au poste de commandement du service concerné et aux personnels impliqués dans la conduite et l’exécution de l’intervention lorsque la sécurité des agents ou la sécurité des biens et des personnes est menacée. |

#### *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 |  | 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 | Importante.  Les enregistrements permettent d’identifier des personnes physiques et, le cas échéant, leur associer des  comportements. Un  accès illégitime pourrait | | 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 |
|  | habilité.  Veuillez préciser les mesures locales mises en œuvre aux fins de réduire le risque d’accès illégitime aux données. | 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 | |
|  |  |  | Perte de la confiance |  |
|  |  |  | Accessoirement atteinte au secret dans le cadre d’une procédure judiciaire |  |

Modification non désirées de données

Introduction dans le

système

Modification des informations collectées ne

permettant plus d’utiliser celles-ci à l’appui d’une procédure

Impossibilité d’exploiter les informations et de les utiliser dans le cadre d’une procédure judiciaire, administrative ou disciplinaire en tant que preuves

Procédures de contrôle, implication des agents, contrôles des logs, maintenance

L’administrateur est en charge de ces contrôles.

Les procédures varient toutefois en fonction des communes utilisatrices des caméras mobiles.

Limitée.

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

Très limitée en raison du cloisonnement du système et de son installation hors réseau

Veuillez préciser les mesures mises en œuvre afin de réduire le risque de modification non désirée des données.

procéder à un enregistrement, ne serait pas de nature à vicier les procédures engagées.

Disparition de données

Introduction usurpée et frauduleuse dans le

système d’hébergement de conservation

Et source non humaine (cas de force

Dysfonctionnement du stockage, erreur de manipulation de l’agent, problème de maintenance ou défaillance technique

Impossibilité d’exploiter les informations et de les utiliser dans le cadre d’une procédure judiciaire, administrative ou disciplinaire en tant que preuves

Maintenance, contrôles réguliers du dispositif et des connexions

Certaines communes peuvent mettre en place une sauvegarde distante des données. Cela a notamment été le cas pour certaines grandes collectivités.

Limitée.

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

Limitée en raison du cloisonnement du système et de son installation hors réseau et de la sécurisation des locaux

majeure :

incendie, inondation)

Veuillez préciser les mesures mises en œuvre afin de réduire le risque de disparation des données.

l’absence d’obligation de procéder à un enregistrement, ne serait pas de nature à vicier les procédures engagées.

## Validation de l’analyse d’impact

**Eléments utiles à la validation**

#### *Synthèse relative à la conformité au RGPD*

|  |  |
| --- | --- |
| **Finalités** | **Evaluation** |
| **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 | 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 | Acceptable |

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

|  |  |
| --- | --- |
| **Finalités** | **Evaluation** |
| **Mesures portant spécifiquement sur les données du traitement** | |
| Chiffrement | Acceptable |
| Anonymisation | Acceptable |
| Pseudonymisation | Non applicable |
| Cloisonnement des données (par rapport au reste du système d’information) |  |
| Contrôle des accès logiques des utilisateurs | Acceptable |
| Traçabilité (journalisation) | Acceptable |
| Contrôle d’intégrité | Acceptable |
| Archivage | Acceptable |
| Sécurité des documents papier | Non applicable |
| **Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre** | |
| Sécurité de l’exploitation | Acceptable |

En cas de recours à un sous-traitant, veuillez adapter la mention.

|  |  |
| --- | --- |
| Lutte contre les logiciels malveillants |  |
| Gestion des postes de travail | Améliorable |
| Sécurité des sites web Il convient d’adapter cette mention en Sauvegardes fonction du choix opéré : installation hors  réseau ou en cloud et évaluer la mesure.  Maintenance  Sécurité des canaux informatiques (réseaux) | Non applicable |
| Acceptable |
| Améliorable |
| Non applicable / Acceptable |
| 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 |  |
| **Mesures organisationnelles (gouvernance)** | |
| Organisation |  |
| Politique (gestion des règles) |  |
| Gestion des risques | Acceptable |
| Gestion des projets |  |
| Gestion des incidents et des violations de données |  |
| Gestion des personnels | Acceptable |
| Relations avec les tiers | Non applicable / Acceptable |
| Supervision | Acceptable |

* + 1. *Cartographie des risques liés à la sécurité des données*

Cartographie à adapter par chacune des communes au regard des éléments présentés *supra*.

## Gravité du risque



### Maximale

**Cartographie des risques**

Accès illégitime à des données

Importante

Limitée

Négligeable

Modification non désirée de données

Accès illégitime à des données

Modification non désirée de données

Disparition de données

Disparition de données

Négligeable Limitée Importante Maximale **Vraisemblance**

## du risque

### Risques avant mesures correctives

Avec les mesures correctives mises en œuvre

##### 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.

## Annexes

Echelles d’analyse des risques :

* + Echelle de gravité (cf. partie 0.1.) ;
  + Echelle de vraisemblance (cf. partie 5.2.) ;
  + Modèle de mentions d’information (cf. partie 5.3).

**Echelle de gravité**

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

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

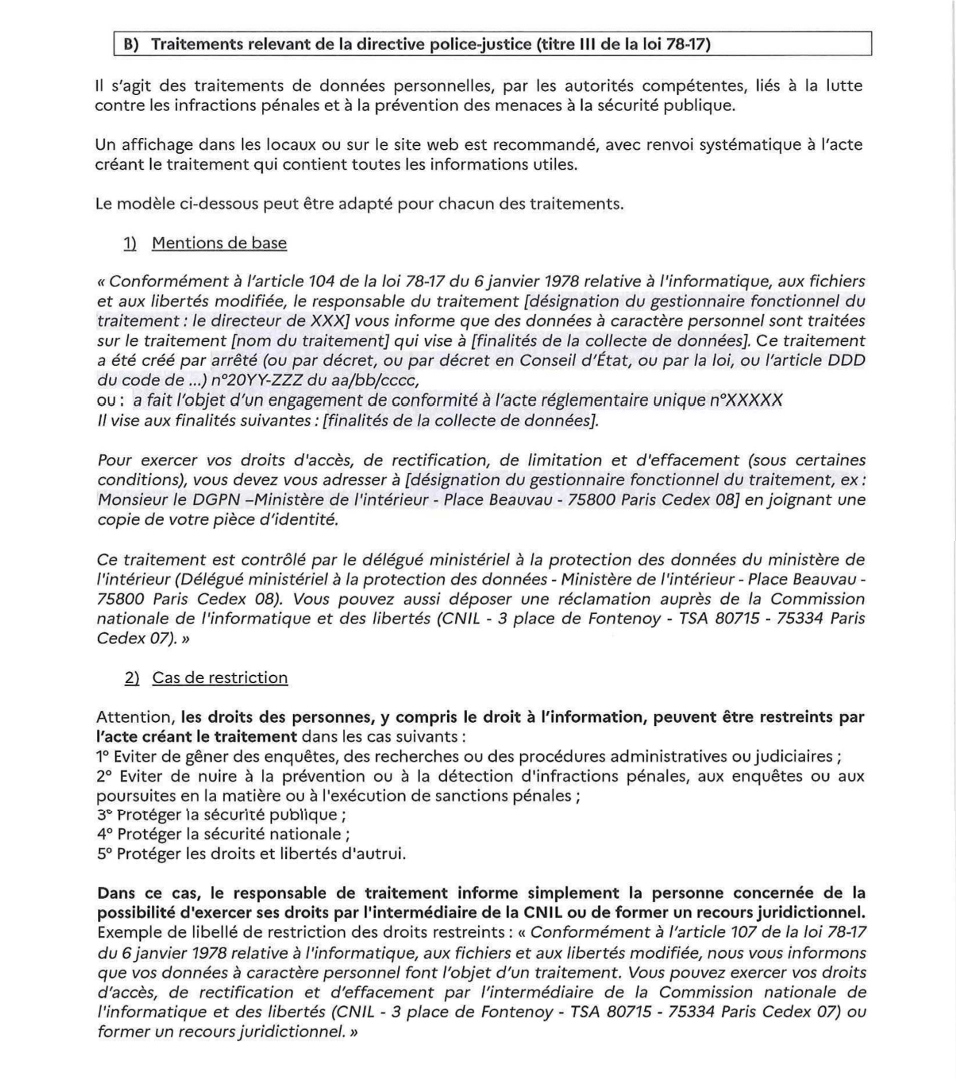
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | auprès d’organismes sociaux, etc.)   * Publicité ciblée en ligne sur un aspect vie privée que la personne souhaitait garder confidentiel (ex : publicité grossesse, traitement pharmaceutique) * Profilage imprécis ou abusif |  |
| **3. Importante** | * Les personnes concernées pourraient connaître des conséquences significatives, qu’elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives. | * Affection physique grave causant un préjudice à long terme (ex. : aggravation de l’état de santé suite à une mauvaise prise en charge, ou au non- respect de contre- indications) * Altération de l’intégrité corporelle par exemple à la suite d’une agression, d’un accident domestique, de travail, etc. | * Détournements d’argent non indemnisé * Difficultés financières non temporaires (ex. : obligation de contracter un prêt) * Opportunités ciblées, uniques et non récurrentes, perdues (ex. : prêt immobilier, refus d’études, de stages ou d’emploi, interdiction d’examen) * Interdiction bancaire * Dégradation de biens * Perte de logement * Perte d’emploi * Séparation ou divorce * Perte financière à la suite d’une escroquerie (ex. : après une tentative d’hameçonnage / *phishing*) * Bloqué à l’étranger * Perte de données clientèle | * Affection psychologique grave (ex. : dépression, développement d’une phobie) * Sentiment d’atteinte à la vie privée et de préjudice irrémédiable * Sentiment de vulnérabilité à la suite d’une assignation en justice * Sentiment d’atteinte aux droits fondamentaux (ex.   : discrimination, liberté d’expression)   * Victime de chantage - *Cyberbullying* et harcèlement moral |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **4. Maximale** | * Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu’elles pourraient ne pas surmonter | * Affection physique de longue durée ou permanente (ex. : suite au non- respect d’une contre-indication) * Décès (ex. : meurtre, suicide, accident mortel) - Altération définitive de l’intégrité   physique | * Péril financier * Dettes importantes * Impossibilité de travailler * Impossibilité de se reloger * Perte de preuves dans le cadre d’un contentieux * Perte d’accès à une infrastructure vitale (eau, électricité) | * Affection psychologique de longue durée ou permanente * Sanction pénale * Enlèvement * Perte de lien familial * Impossibilité d’ester en justice * Changement de statut administratif et/ou perte d’autonomie juridique (tutelle) |

**Echelle de vraisemblance**

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

**Modèle de mention d’information s’agissant des traitements relevant de la directive dite « police-justice » (titre III de la loi n° 78-17 du 6 janvier 1978)**



Ces mentions doivent permettre aux personnes concernées par les traitements de données à caractère personnel (citoyens, agents, usagers, mis en cause…) d’être informées des caractéristiques de ces traitements. Elles sont spécifiques à chaque traitement.