RÉPUBLIQUE FRANÇAISE
Liberté – Égalité – Fraternité

Département du Val-de-Marne
Canton d'Orly
Commune d'Orly

Ville d'Orly

N°A- IVP-2024/ 176

ARRÊTÉ DE LA MAIRE

Registre des arrêtés du Maire

Objet : APPROBATION DE L'ANALYSE D'IMPACT A LA PROTECTION DES DONNEES RELATIVES À LA VIDEOPROTECTION A LA VILLE D'ORLY

LA MAIRE D'ORLY,

VU le Code général des collectivités territoriales ;

VU le Règlement 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 ;

VU la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

VU le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

VU l'analyse d'impact relative à la protection des données (AIPD) annexée au présent arrêté ;

CONSIDERANT que les traitements de données à caractère personnel susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées implique la réalisation d'analyses d'impact ;

CONSIDERANT que la ville d'Orly dispose d'un traitement de données à caractère personnel dont l'objet est la vidéoprotection, pour lequel une analyse d'impact à la protection des données a été réalisée ;

CONSIDERANT que le responsable du traitement est la Ville d'Orly dont le représentant est Madame la Maire ;

ARRÊTE:

ARTICLE 1 : DIT que la ville d'Orly dispose d'un traitement automatisé de données à caractère personnel dont l'objet est la vidéoprotection nécessitant la réalisation d'une analyse d'impact.

ARTICLE 2 : APPROUVE l'analyse d'impact à la protection des données relative à la vidéoprotection. Le service en charge de la mise en œuvre du traitement ainsi que du plan d'actions et des mesures correctives prévus dans l'analyse d'impact susvisée est le service de la Police municipale.

ARTICLE 3 : DIT que les finalités du traitement cité à l'article 1 sont de proposer aux administrés une meilleure sécurisation des lieux publics et de permettre de constater des infractions aux règles de circulation

(vidéoverbalisation), réguler les flux de transport et protéger des bâtiments, installations publiques et leurs abords, les finalités de traitement qui sont en cohérence avec la législation en vigueur. Le détail des finalités de traitement est contenu dans l'analyse d'impact relative à la protection des données (AIPD) en annexe au présent arrêté.

ARTICLE 4 : PRECISE que l'analyse d'impact à la protection des données relatives à la vidéoprotection, telle qu'annexée au présent arrêté, énumère le type de données à caractère personnel et information enregistrées.

ARTICLE 5 : PRECISE que dans le cadre de ces traitements, les données sont accessibles au service de la Police municipale. L'analyse d'impact à la protection des données relatives à la vidéoprotection, telle qu'annexée au présent arrêté, précise les personnels compétents ayant accès aux données à caractère personnel utilisées par le présent traitement automatisé de données.

ARTICLE 6 : PRECISE que les personnes concernées sont informées à propos du traitement par le biais des panneaux d'affichage indiquant le numéro de téléphone à contacter pour l'exercice de leurs droits, notamment le droit d'accès.
Les droits d'accès, rectification et de suppression s'exercent auprès du délégué à la protection des données, à l'adresse suivante :

- rgpd@mairie-orly.fr.

ARTICLE 7 : DIT qu'ampliation du présent arrêté sera adressée à Madame la Préfète du Val-de-Marne.

ARTICLE 8 : DIT que la Directrice générale des services de la mairie d'Orly est chargée de l'exécution du présent arrêté.

ARTICLE 9 : DIT que le présent arrêté peut faire l'objet d'un recours pour excès de pouvoir devant le Tribunal administratif de Melun dans un délai de 2 mois à compter de sa publication.

Fait à Orly, le 13 JUIN 2024

Imène SOUID

Maire,
Conseillère départementale du Val de Marne

Accusé de réception en préfecture
094-219400546-20240603-AIVP2024176-AR
Date de télétransmission : 03/06/2024
Date de réception préfecture : 03/06/2024

PIA

Analyse d'impact sur la protection des données
Privacy impact assessment

VIDÉOPROTECTION

AESATIS

Ville d'Orly

Présentation

Description de l'analyse

Aperçu de l'analyse

INFORMATIONS GÉNÉRALES

Statut : Validation simple

Saisie : Damien AULANIER
Évaluation : Célia CAMPANA
Validation : Bernadette LEROY

L'analyse est basée sur :

- Une analyse documentaire ;
- Un ensemble d'entretiens et d'échanges, avec :
  - Le service concerné ;
  - Le service informatique de la ville d'Orly ;
  - Le sous-traitant principal ;

LISTE DES ANNEXES À L'ANALYSE

- Article L251-2 du code de la sécurité intérieure (CSI) ;
- Article L.241- du CSI ;
- Plan d'actions.

Présentation

Sommaire de l'analyse

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?

Le traitement faisant l'objet de l'étude est la gestion de la vidéoprotection sur la voie publique. Ce traitement est mis en place par la Ville d'Orly pour assurer la sécurité des biens et des personnes.

Quelles sont les responsabilités liées au traitement ?

Le responsable du traitement est la Ville d'Orly, représentée par Madame le Maire.

Le service en charge de la mise en œuvre du traitement est le Service Technique et Environnement.

Le prestataire intervenant dans le cadre du traitement est la société INEO/EQUANS, qui met à disposition le logiciel de gestion des caméras de vidéoprotection GENETEC.

Quels sont les référentiels applicables ?

Les référentiels applicables sont :

- Code de la sécurité intérieure (Articles L.223-1, L.223-9, L.251-1 à L.255-1 et L.613-13 et R.251-1 à R.253-4) et décret n° 96-926 du 17 octobre 1996 modifié.
- Publication de la CNIL : vidéoprotection sur la voie publique.

Évaluation : Acceptable

Contexte

Données, processus et supports

Quelles sont les données traitées ?

Les données traitées sont des images vidéos de la ville d'Orly. Dans ce cadre, on retrouve deux catégories de données, dont :

- **Données d'identification** : images des personnes ;
- **Données de localisation** : horaire et lieu de passage des personnes sur les zones filmées.

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

Les images sont enregistrées à travers les caméras installées dans différents lieux de la ville. Les images sont conservées sur un serveur dédié, pour une durée de 30 jours si aucune procédure n'est engagée.

En interne, seuls les agents de surveillance de la voie publique ont un accès aux images enregistrées, via le logiciel GENETEC. Une liste nominative de ces derniers a été établie et déclarée à la préfecture.

En externe, les agents des forces de l'ordre peuvent avoir un accès aux images enregistrées, sur demande, sur constat d'une infraction, ou sur réquisition judiciaire.

Quels sont les supports des données ?

Les images sont conservées en format numérique, sur un serveur dédié.

Évaluation : Acceptable

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

La finalité du traitement est déterminée, explicite et légitime.

La vidéoprotection permet de proposer aux administrés une meilleure sécurisation des lieux publics. Ces dispositifs peuvent également permettre de constater des infractions aux règles de circulation (vidéoverbalisation), réguler les flux de transport et protéger des bâtiments, installations publiques et leurs abords.
Les personnes sont informées sur le traitement à travers des panneaux d'affichage en permanence au niveau des zones concernées. La ville respecte, dans le cadre de ce traitement, la réglementation liée à la vidéoprotection : les déclarations en préfecture sont bien réalisées et une traçabilité de l'ensemble des actions effectuées sur les images (enregistrements, transferts, modifications, destructions) est assurée via le logiciel GENETEC.

Évaluation : Acceptable

Quel(s) est (sont) le(s) fondement(s) qui rend(ent) votre traitement licite ?

Le fondement sur lequel repose le traitement est la mission d'intérêt public. Il permet d'assurer la protection des personnes et des biens dans les lieux publics de la ville. De plus, il participe à la lutte contre les infractions aux règles de circulation, permet de réguler les flux de transport et aide à la protection des bâtiments, installations publiques et leurs abords.

Évaluation : Acceptable

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Au regard des finalités du traitement, les images vidéos enregistrées sont toutes adéquates, minimisées et nécessaires. En effet, les caméras filment seulement des zones précises et ne permettent pas de visualiser l'intérieur des bâtiments, conformément à la réglementation en matière de vidéoprotection.

Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les images sont exactes et tenues à jour. Les images sont enregistrées en permanence et supprimées automatiquement au bout de 30 jours.

Évaluation : Acceptable

Quelle est la durée de conservation des données ?

La durée de conservation définie est de 30 jours. En effet, sur le logiciel GENETEC, les images sont paramétrées pour être supprimées automatiquement tous les 30 jours.
En cas de procédure pénale, les vidéos peuvent être conservées pour une durée supplémentaire.
Les journaux sont horodatés et leur durée de rétention est de 90 jours.

Évaluation : Acceptable

Comment les personnes concernées sont-elles informées à propos du traitement ?

Les personnes concernées sont informées à propos du traitement au moyen de panneaux affichés en permanence de façon visible dans les lieux concernés. Ils sont compréhensibles par tous les publics et comportent chacun :

- Un pictogramme représentant une caméra, indiquant que le lieu est placé sous vidéoprotection ;
- La finalité du traitement ;
- L'existence de droits informatiques et de liberté ;
- Les coordonnées pour l'exercice des droits (numéro de téléphone).

Cependant, les panneaux n'indiquent ni la durée de conservation des données, ni les droits des individus à introduire une réclamation auprès de la CNIL.

Évaluation : Améliorable
Plan d'actions / mesures correctives :

En plus des informations affichées sur les panneaux d'affichage de la ville, il serait nécessaire de :

- Préciser la durée de conservation des images (30 jours) ;
- Indiquer le droit des personnes à introduire une réclamation auprès de la CNIL, en mentionnant ses coordonnées.

Afin que les panneaux restent lisibles, l'intégralité des informations qui doivent être portées à la connaissance du public peut l'être par d'autres moyens, notamment par le biais du site web de la ville. Ces autres informations sont, notamment, :

- La base légale du traitement ;
- Les destinataires des données personnelles.

Commentaire d'évaluation : Suivant les recommandations de la CNIL, les panneaux d'affichage doivent comporter a minima les informations suivantes :

- Un pictogramme indiquant une caméra ;
- Les finalités du traitement ;
- Les bases légales ;
- La durée de conservation des images ;
- Le nom ou la qualité, et le numéro de téléphone du responsable/du délégué à la protection des données (DPO) ;
- L'existence des droits informatiques et libertés ;
- Le droit d'introduire une réclamation auprès de la CNIL, en précisant ses coordonnées.

Comment les personnes concernées peuvent-elles exercer leurs :

- Droit d'accès et droit à la portabilité ?
- Droit de rectification et droit à l'effacement ?
- Droit de limitation et droit d'opposition ?

Les personnes concernées sont informées à propos du traitement par le biais des panneaux d'affichage indiquant le numéro de téléphone à contacter pour l'exercice de leurs droits, notamment le droit d'accès.

Évaluation : Acceptable

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Un contrat entre la Ville d'Orly et le prestataire INEO/EQUANS a été établi. Il est constitué des pièces suivantes :

- L'acte d'engagement (AE) et ses annexes ;
- Le cahier des clauses administratives particulières (CCAP).

Le contrat ne contient aucune clause RGPD ou relative à la protection des données personnelles.

Évaluation : Améliorable

Plan d'actions / mesures correctives :
Intégrer un avenant au marché comprenant des clauses RGPD.

Commentaire d'évaluation : Il est impératif d'intégrer au contrat des clauses RGPD visant à s'assurer de la confidentialité des données traitées et de la mise en place de mesures de sécurité suffisantes.

Contrôle des accès logiques

Une gestion des accès stricte est mise en place par la Ville d'Orly. Les accès aux images sont limités aux seuls agents de la Ville ayant été habilités et ayant reçu une formation adéquate.

Évaluation : Acceptable

Journalisation des évènements

Un système de journalisation est mis en place au niveau du logiciel GENETEC permettant la traçabilité des différentes actions réalisées sur les images vidéos (historiques des configurations et historiques des manipulations utilisateurs). Les journaux sont horodatés et leur durée de rétention est de 90 jours.

Évaluation : Acceptable

Sensibilisation des utilisateurs

Chaque service de la ville a désigné un référent opérationnel RGPD qui a été, a minima, sensibilisé au RGPD et aux bonnes pratiques. De plus, le DSI de la ville fait partie du COPIL de la mise en conformité au RGPD.

L'ensemble des agents ayant accès aux enregistrements ont été formés et sensibilisés aux différentes pratiques liées au RGPD.

Évaluation : Acceptable

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Les données n'ont pas vocation à être transférées hors Union Européenne.

Évaluation : Acceptable

Protection des locaux

Un système de Gestion Technique des Bâtiments (GTB) permettant de contrôler et surveiller les différents équipements électriques et mécaniques a été mis en place et les matériels informatiques sont également protégés.
Un contrôle d'accès est mis en place, permettant la distinction des zones à risque. Les bureaux sont systématiquement fermés lors de l'absence du personnel. De plus, pour accéder au pôle, il est nécessaire de disposer d'un badge. Ainsi, les visiteurs ne peuvent pas y accéder directement.

Évaluation : Améliorable

Plan d'actions / mesures correctives :

- Créer un registre des visiteurs ;
- Accompagner les visiteurs lors de leur présence dans les locaux.

Commentaire d'évaluation : D'autres mesures pourraient renforcer cette sécurité, sans que cela n'engendre de dépenses importantes pour la ville.

Sécurisation des serveurs

Les serveurs ne font pas l'objet de sauvegardes régulières et ne disposent pas de mécanismes de redondance.

Évaluation : Améliorable

Plan d'actions / mesures correctives : Mettre en œuvre des sauvegardes régulières des serveurs, ainsi qu'un système de redondance.

Commentaire d'évaluation : La mise en place de sauvegardes régulières et de mécanismes de redondance permettrait d'accroître la sécurisation du système.

Mot de passe

Chaque agent dispose d'un mot de passe personnel pour accéder au logiciel GENETEC, répondant aux règles de complexité suivantes :

- 8 caractères,
- 1 lettre majuscule,
- 1 lettre minuscule,
- 1 caractère numérique,
- 1 caractère spécial.

Évaluation : Améliorable

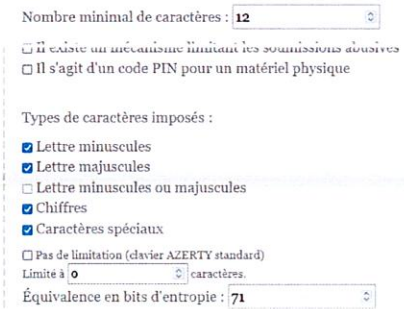
Plan d'actions / mesures correctives :

Il serait nécessaire de mettre en œuvre une politique de mot de passe en suivant les nouvelles recommandations de la CNIL. Si le logiciel n'impose pas un certain format, il est conseillé de :

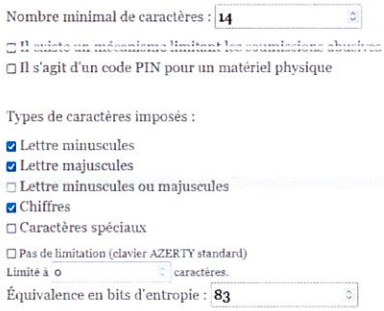
- définir des règles permettant aux utilisateurs d'avoir des mots de passe sécurisés, (exemple : un mot de passe de 12 caractères avec des caractères spéciaux, ou un mot de passe comprenant a minima 14 caractères) ;
- interdire certains mots de passe ;
- formaliser une politique de mot de passe.

Ci-après des exemples de **niveau d'entropie en fonction des règles définies** :

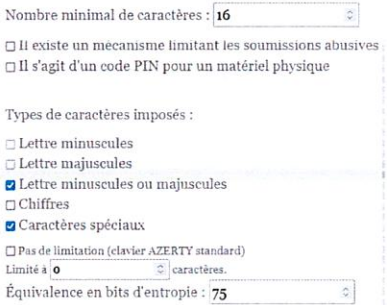
Exemple 1 : minimum de 12 caractères comprenant majuscules, minuscules, chiffres et caractères spéciaux.



Exemple 2 : minimum 14 caractères comprenant majuscules, minuscules et chiffres, **sans** caractère spécial obligatoire.



Exemple 3 : une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots.



Gérer les risques

Le traitement faisant l'objet de cette analyse est recensé dans le registre des traitements.

Un audit de conformité RGPD a été réalisé. Il a permis de déterminer les mesures existantes et a donné lieu à un plan d'actions.

Évaluation : Acceptable

Gestion des postes de travail

Les postes de travail sont sécurisés par des mots de passe. Toutefois, ces derniers ne répondent à aucune règle de robustesse. De plus, des antivirus régulièrement mis à jour sont utilisés et une politique de mise à jour régulière est mise en place.

Les applications téléchargées ne provenant pas de sources sûres ne sont pas exécutées et l'usage d'applications nécessitant des droits de niveau administrateur est limité.

Évaluation : Améliorable

Plan d'actions / mesures correctives : Il serait judicieux de prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné. Il conviendrait également de configurer les logiciels pour que les mises à jour se fassent automatiquement.

Commentaire d'évaluation : Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent l'un des principaux points d'entrée.

Organisation de la politique de la vie privée

La ville a désigné la société AESATIS comme DPO externalisé, chargée de la mise en conformité au RGPD. De plus, des référents RGPD par service ont été désignés et sont impliqués dans le projet. Ils sont remplacés au fur et à mesure des départs / arrivées dans la direction ou le service concernés.
La ville dispose d'un corpus documentaire qui est continuellement alimenté. Cette analyse en fera d'ailleurs partie.

Évaluation : Acceptable

Sécurisation du réseau interne

Les accès internet sont limités et les services non nécessaires sont bloqués.
De plus, les réseaux ouverts aux invités sont séparés du réseau interne et les flux entrants et sortants sur les équipements sont filtrés. Pour l'accès à distance, un VPN est imposé. En revanche, le système ne bénéficie pas de mécanismes de continuité d'activité.

Évaluation : Améliorable

Plan d'actions / mesures correctives :
- Réaliser des tests d'intrusions (recommandés tous les 3 ans) afin de détecter les vulnérabilités et failles de sécurité ;
- La télémaintenance doit s'effectuer via un VPN ;
- S'assurer qu'aucune interface réseau n'est accessible depuis internet ;
- Mettre en œuvre un système de continuité d'activité.

Commentaire d'évaluation :
De nombreuses mesures restent à mettre en œuvre afin de garantir une sécurisation optimale du réseau interne.

Risques

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé au logiciel GENETEC, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un ASVP, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un ASVP, tiers négligeant.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, sensibilisation des utilisateurs, protection des locaux, sécurisation des serveurs, mot de passe, gérer les risques, gestion du poste de travail, organisation de la politique de la vie privée, sécurisation du réseaux interne.

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Au regard du type de données et du périmètre des caméras de vidéoprotection, la gravité du risque d'un accès illégitime aux images est évaluée comme importante.

En effet, ces images permettent d'identifier des personnes physiques et un accès illégitime pourrait avoir des conséquences importantes sur la vie privée des personnes filmées.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante.

En effet, la politique de mots de passe pour accéder au logiciel n'est actuellement pas suffisante au regard des recommandations, et il n'y a pas de verrouillage automatique des postes de travail. Par ailleurs, aucun test d'intrusion n'est mis en place, et il n'y a aucune clause RGPD dans le contrat qui lie la commune au prestataire.

Évaluation : Améliorable

Plan d'actions / mesures correctives :

- Réaliser des tests d'intrusions (recommandés tous les 3 ans) afin de détecter les vulnérabilités et failles de sécurité ;
- La télémaintenance doit s'effectuer via un VPN ;
- S'assurer qu'aucune interface réseau n'est accessible depuis internet ;
- Mettre en œuvre un système de continuité d'activité ;
- Faire évoluer la politique de mots de passe conformément aux recommandations en vigueur ;
- Mettre en place un verrouillage automatique des postes de travail.

Risques

Modification non désirée de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé au logiciel GENETEC, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un ASVP, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un ASVP, tiers négligeant.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, sensibilisation des utilisateurs, protection des locaux, sécurisation des serveurs, mot de passe, gérer les risques, gestion du poste de travail, organisation de la politique de la vie privée, sécurisation du réseau interne.

Risques

Modification non désirée de données

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

La gravité du risque d'une modification des images est évaluée comme maximale. En effet, une modification de ces images pouvant identifier une personne physique pourrait avoir des conséquences redoutables sur sa vie privée.

De plus, ces images peuvent faire l'objet de preuves. Leur modification pourrait entrainer une perte de droits pour les personnes concernées.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante.

En effet, bien que le nombre d'intervenants dans le cadre de ce traitement et d'échanges soient limités, il n'existe aucune sauvegarde régulière ou mécanisme de redondance.

Évaluation : Améliorable

Plan d'actions / mesures correctives : Mettre en œuvre des sauvegardes régulières des serveurs, ainsi qu'un système de redondance.

Commentaire d'évaluation : La mise en place de sauvegardes régulières et de mécanismes de redondance permettrait d'accroître la sécurisation du système.

Risques

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Sentiment d'atteinte à la vie privée, chantage, harcèlement, refus d'accès à certaines prestations, risques corporels, risques psychologiques, dommages psychologiques, cyberharcèlement, dépression, perte de temps pour réitérer des démarches, diffamation donnant lieu à des représailles.

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Acte interne de malveillance, acte externe de malveillance, fuite de données, vol de données, piratage informatique, consultation humaine, interception du flux sur le réseau, accès non autorisé au logiciel GENETEC, erreur humaine, vol de matériel, accès non autorisé aux locaux.

Quelles sources de risques pourraient-elles en être à l'origine ?

Attaquant ciblant la structure, attaquant ciblant un ASVP, employé malintentionné, employé négligeant, personnel de maintenance, tiers malintentionné, entourage d'un ASVP, tiers négligeant, incendie, inondation.

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, sensibilisation des utilisateurs, protection des locaux, sécurisation des serveurs, mot de passe, gérer les risques, gestion du poste de travail, organisation de la politique de la vie privée, sécurisation du réseau interne.

Risques

Disparition de données

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Au vu du périmètre des caméras de vidéoprotection et de la quantité des images enregistrées, la disparition des images peut entrainer de lourdes conséquences. Ainsi, la gravité est évaluée comme maximale.

De plus, la disparition des images peut entrainer une perte de preuves dans le cadre d'un contentieux et, ainsi, une perte de droit pour la personnes concernée.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

La vraisemblance du risque est évaluée comme importante.

En effet, bien que le nombre d'intervenants dans le cadre de ce traitement et d'échanges soient limités, il n'existe aucune sauvegarde régulière ou mécanisme de redondance.

Évaluation : Améliorable

Plan d'actions / mesures correctives : Mettre en œuvre des sauvegardes régulières des serveurs, ainsi qu'un système de redondance.

Commentaire d'évaluation : La mise en place de sauvegardes régulières et de mécanismes de redondance permettrait d'accroître la sécurisation du système.

Risques

Vue d'ensemble des risques

Impacts potentiels

- Sentiment d'atteinte à la vie privée
- Chantage
- Harcèlement
- Refus d'accès à certaines prestations
- Risques corporels
- Risques psychologiques
- Dommages psychologiques
- Cyberharcèlement
- Dépression
- Perte de temps pour réitérer des démarches
- Diffamation donnant lieu à des représailles

Menaces

- Acte externe de malveillance
- Acte interne de malveillance
- Fuite de données
- Vol de données
- Piratage informatique
- Consultation humaine
- Interception de flux sur le réseau
- Accès non autorisé
- Erreur humaine
- Vol de matériel
- Accès non autorisé aux locaux

Sources

- Attaquant ciblant l'organisme
- Attaquant ciblant un ASVP
- Employé malintentionné
- Employé négligeant
- Personnel de maintenance
- Tiers malintentionné
- Entourage d'un ASVP
- Tiers négligeant
- Incendie
- Inondation

Mesures

- Contrôle des accès logique
- Sensibilisation
- Protection des locaux
- Sécurisation des serveurs
- Mot de passe
- Gérer les risques
- Gestion du poste de travail
- Organisation de la politique de la vie privée
- Sécurisation du réseau interne

Accès illégitime à des données	Gravité : **Maximale**	
	Vraisemblance : **Importante**	
Modification non désirée des données	Gravité : **Maximale**	
	Vraisemblance : **Importante**	
Disparition des données	Gravité : **Maximale**	
	Vraisemblance : **Importante**	

Validation

Avis du DPD et des personnes concernées

Nom du DPD

Société AESATIS, représentée par sa dirigeante Madame Bernadette LEROY

Statut du DPD

Le traitement pourrait être mis en œuvre.

Opinion du DPD

Les mesures proposées pour sécuriser le traitement sont suffisantes pour sa bonne mise en œuvre mais des mesures correctives doivent être mises en œuvre.

Recherche de l'avis des personnes concernées

Le service en charge du traitement et son responsable de traitement valident la mise en œuvre du traitement au vu de leur nécessité.

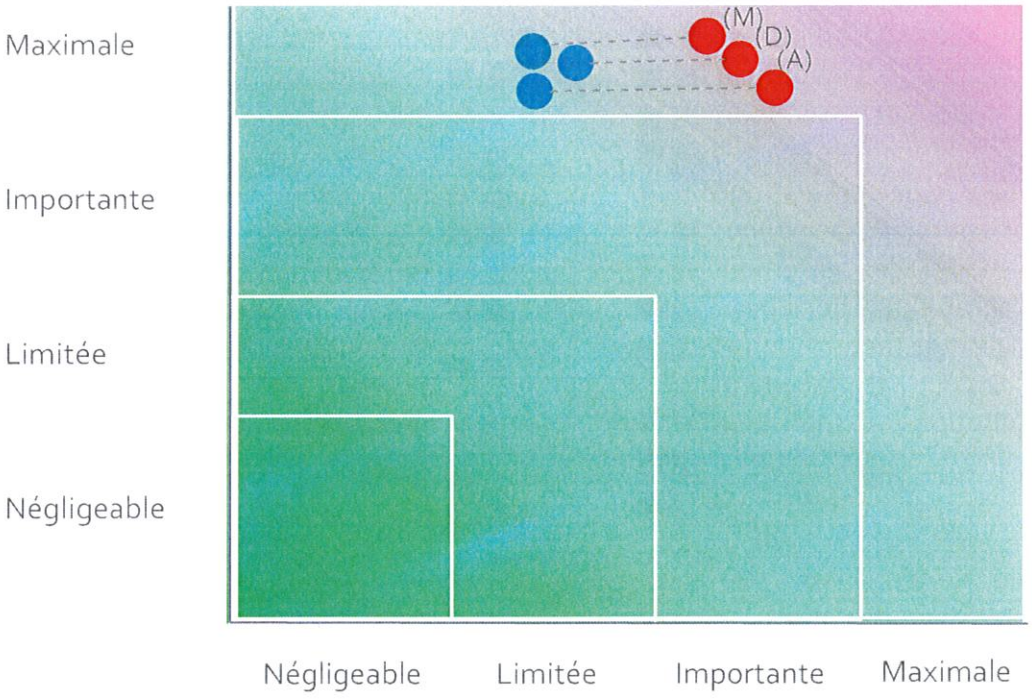
Raison pour laquelle l'avis des personnes concernées n'a pas été demandé

Les personnes concernées n'ont pas été consultées car le traitement est déjà en œuvre.

Validation

Cartographie des risques

Gravité du risque



Vraisemblance du risque

- Mesures prévues ou existantes
- Avec les mesures correctives mises en œuvre
- (A)ccès illégitime à des données
- (M)odification non désirée de données
- (D)isparition de données

Validation

Plan d'action

Vue d'ensemble

Principes fondamentaux

- Finalités
- Fondement
- Données adéquates
- Données exactes
- Durée de conservation
- Information des personnes
- Recueil du consentement
- Droit d'accès et à la portabilité
- Droit de rectification et d'effacement
- Droit de limitation et d'opposition
- Sous-traitance
- Transferts

Mesures existantes ou prévues

- Contrôle des accès logique
- Sensibilisation
- Protection des locaux
- Sécurisation des serveurs
- Mot de passe
- Gérer les risques
- Gestion du poste de travail
- Organisation de la politique de la vie privée
- Sécurisation du réseau interne

Risques

- Accès illégitime à des données
- Modification non désirée de données
- Disparition de données

Mesures Améliorables
Mesures Acceptables

Principes fondamentaux

Transparence

Évaluation : Améliorable
Plan d'actions / mesures correctives :

En plus des informations affichées sur les panneaux d'affichage de la ville, il serait nécessaire de :

- Préciser la durée de conservation des images (30 jours) ;
- Indiquer le droit des personnes à introduire une réclamation auprès de la CNIL, en mentionnant ses coordonnées.

Afin que les panneaux restent lisibles, l'intégralité des informations qui doivent être portées à la connaissance du public peuvent l'être par d'autres moyens, notamment par le biais du site web. Ces autres informations sont, notamment, :

- La base légale du traitement ;
- Les destinataires des données personnelles.

Commentaire d'évaluation : Suivant les recommandations de la CNIL, les panneaux d'affichage doivent comporter a minima les informations suivantes :

- Un pictogramme indiquant une caméra ;
- Les finalités du traitement installé ;
- La durée de conservation des images ;
- Le nom ou la qualité et le numéro de téléphone du responsable/du délégué à la protection des données (DPO) ;
- L'existence des droits informatiques et libertés ;
- Le droit d'introduire une réclamation auprès de la CNIL, en précisant ses coordonnées.

Sous-traitants

Évaluation : Améliorable

Plan d'actions / mesures correctives :
Intégrer un avenant au marché comprenant des clauses RGPD.

Commentaire d'évaluation : Il est impératif d'intégrer au contrat des clauses RGPD visant à s'assurer de la confidentialité des données traitées et de la mise en place de mesures de sécurité suffisantes.

Mesures existantes ou prévues

Protection des locaux

Évaluation : Améliorable

Plan d'actions / mesures correctives :

- Créer un registre des visiteurs ;
- Accompagner les visiteurs lors de leur présence dans les locaux.

Commentaire d'évaluation : D'autres mesures pourraient renforcer cette sécurité, sans que cela n'engendre de dépenses importantes pour la ville.

Sécurisation des serveurs

Évaluation : Améliorable

Plan d'actions / mesures correctives : Mettre en œuvre des sauvegardes régulières des serveurs, ainsi qu'un système de redondance.

Commentaire d'évaluation : La mise en place de sauvegardes régulières et de mécanismes de redondance permettrait d'accroître la sécurisation du système.

Mesures existantes ou prévues

Mot de passe

Évaluation : Améliorable

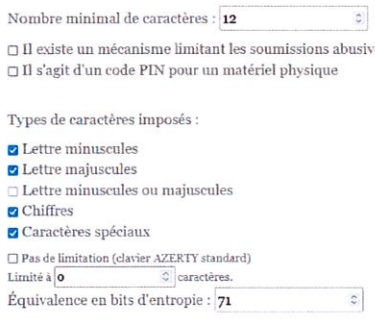
Plan d'actions / mesures correctives :

Il serait nécessaire de mettre en œuvre une politique de mots de passe en suivant les nouvelles recommandations de la CNIL. Si le logiciel n'impose pas un certain format, il est conseillé de :

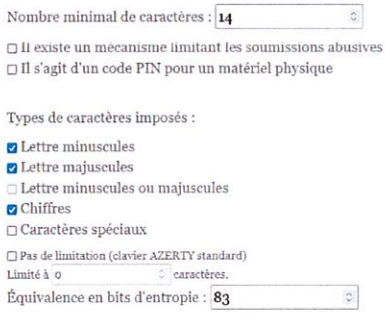
- Définir des règles permettant aux utilisateurs d'avoir des mots de passe sécurisés, exemple un mot de passe de 12 caractères avec des caractères spéciaux, ou un mot de passe comprenant, a minima, 14 caractères ;
- Interdire certains mots de passe ;
- Pratiquer un renouvellement régulier des mots de passe pour les comptes de type administrateur ;
- Formaliser une politique de mot de passe.

Ci-après des exemples de **niveau d'entropie en fonction des règles définies** :

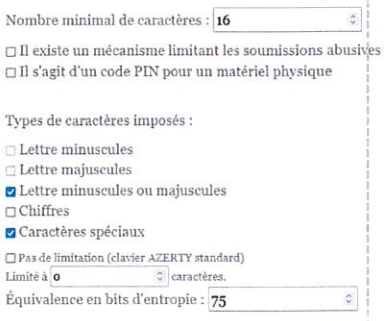
Exemple 1 : minimum de 12 caractères comprenant majuscules, minuscules, chiffres et caractères spéciaux.



Exemple 2 : minimum 14 caractères comprenant majuscules, minuscules et chiffres, **sans** caractère spécial obligatoire.



Exemple 3 : une phrase de passe doit être utilisée et elle doit être composée d'au minimum 7 mots.



Mesures existantes ou prévues

Gestion du poste de travail

Évaluation : Améliorable

Plan d'actions / mesures correctives : Il serait judicieux de prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné.
Il convient également de configurer les logiciels pour que les mises à jour se fassent automatiquement.

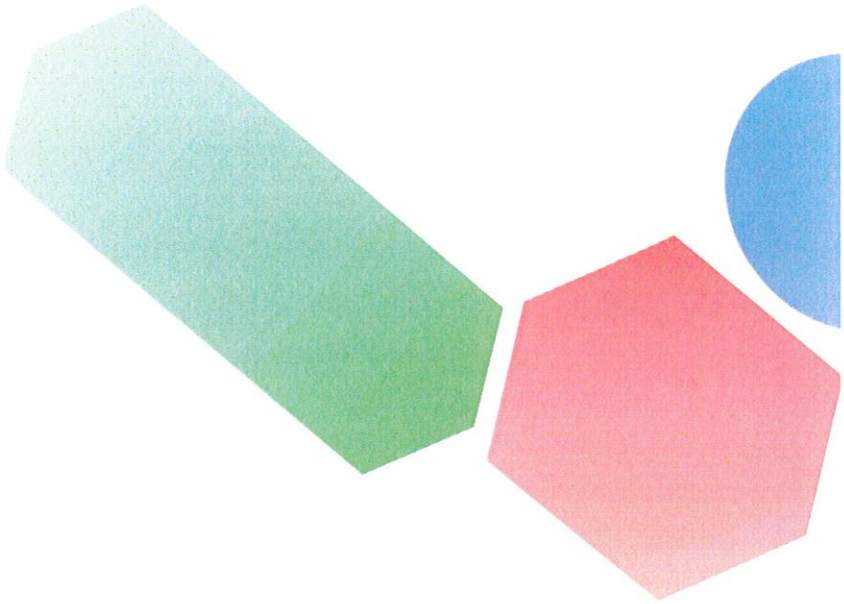
Commentaire d'évaluation : Les risques d'intrusion dans les systèmes informatiques sont importants et les postes de travail constituent l'un des principaux points d'entrée.

Sécurisation du réseau interne

Évaluation : Améliorable

Plan d'actions / mesures correctives :
Réaliser des tests d'intrusion (recommandés tous les 3 ans) afin de détecter les vulnérabilités et failles de sécurité.
La télémaintenance doit s'effectuer via un VPN.
S'assurer qu'aucune interface réseau n'est accessible depuis internet.
Mettre en œuvre un système de continuité d'activité.

Commentaire d'évaluation :
De nombreuses mesures restent à mettre en œuvre afin de garantir une sécurisation optimale du réseau interne.



AESATIS