@ΣΗΔΕ ΙΡΙΔΑ
6684f301972ec454ab5e8800
ΑΠ:Υ.Σ.4496
Υπογραφή: 03/07/24 10:15
Διανομή: 03/07/24 10:17

Politique de Confidentialité de Centaurus – Système de Vidéosurveillance et Caméras de Sécurité dans les Installations d'Hébergement du MMA

1. **Objectif et champ d'application de la politique de vidéosurveillance**

Afin d'assurer la sécurité des personnes hébergées dans les installations d'hébergement du MMA, du personnel et des visiteurs, des bâtiments ainsi que des biens, Le ministère des Migrations et de l'Asile (M.M.A) exploite un système de vidéosurveillance. Cette politique de Confidentialité ci-dessous décrit le système de vidéosurveillance du ministère et les garanties que reçoit le ministère, en tant qu'organisme de protection des données personnelles, de la vie privée et des autres droits fondamentaux et intérêts légitimes des **personnes** enregistrées sur les caméras.

La détection, l'investigation et la poursuite des crimes ainsi que la protection des biens et des personnes par la collecte de données à caractère personnel à l'aide de systèmes de vidéosurveillance dans les bâtiments d'hébergement du MMA. Le MMA veille constamment à ce que les outils de "sauvegarde" appropriés, tels que les codes de conduite, les certifications et les labels, les DPIA standards et les contrats standards, soient en place.

2. Comment s'assurer que le système de vidéosurveillance tient compte de la protection de la vie privée et des données, et qu'il est conforme à la loi sur la protection des données ?

2.1. **Régime de conformité**. Le MMA traite les images en tenant compte de la directive 1/2011 de l'AHPD (Autorité Hellénique de Protection des Données) et des lignes directrices 3/2019 du Comité Européen de la Protection des Données [CEPD] [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_el.pdf hyperlien vers les lignes directrices sur le site du European Data Protection Supervisor]. Le processus de mise en conformité avec la loi 4624/2019 (Journal officiel 137 A') est en cours, en adaptation et en harmonisation avec le Règlement général sur la protection des données (UE 2016/679) du 25.5.2018 et la directive (UE 2016/680) du Parlement européen, qui renforce le cadre de protection des personnes concernées par le traitement des données à caractère personnel dans l'Union européenne.

2.2. **Inspection par le Ministère lui-même**. Le système est soumis à un contrôle régulier - une inspection des besoins de conformité réglementaire par les services internes (Direction Générale des Technologies, de l'Information et des Applications et du DPD) du MMA lui-même.

2.3. **Partage du régime de conformité.** Conformément au Règlement, il n'y a pas d'obligation de notifier ni d'obtenir l'approbation de l'autorité de protection des données pour l'installation et l'exploitation d'un système de vidéosurveillance. Le rapport d'analyse d'impact sur les parties dissidentes (DPIA), tel qu'il a été mis à jour et complété, fait partie intégrante de la présente Politique de Confidentialité.

2.4. **Contacts avec l'autorité compétente en matière de protection des données dans l'État membre**. L'autorité compétente en matière de protection des données dispose de toute information demandée pour l'utilisation du système sous la responsabilité du délégué à la protection des données, qui conserve une copie du dossier de traitement, une copie de la politique de sécurité et un rapport sur les risques liés au traitement.

2.5. **Décision de l'administration sur la légalité de la vidéosurveillance des installations d'hébergement**. La décision d'utiliser le système de vidéosurveillance actuel et d'adopter les mesures de protection décrites dans cette politique de surveillance a été prise par le Secrétaire Général du Ministère concerné.

La base juridique principale ou générale du traitement de la vidéosurveillance est l'exécution d'une mission d'intérêt public dans l'exercice de l'autorité publique [art. 6, par. 1, point e) du RGPD] alors que le traitement de catégories particulières de données (biométriques) est effectué pour des motifs d'intérêt public important (article 9, paragraphe 2, point g) du RGPD), sur la base du Règlement de Dublin III ou du code de l'immigration, tandis que les CCAC (Centres Fermés d'Accès Contrôlé) constituent des "infrastructures critiques de l'État". Conformément à l'article 6 par. 1 (e) du RGPD, d'une part, une base juridique pour le traitement des données à caractère personnel est mise en place sans qu'il soit nécessaire de la répéter dans la loi et, d'autre part, le traitement, en tant que restriction d'un droit individuel, doit avoir une base dans le droit de l'État membre en ce sens qu'une disposition spécifique de la loi n'est pas nécessaire pour chaque traitement individuel (voir art. 45 du RGPD), mais la loi (voir art. 41 RGPD) ne doit pas confier au responsable du traitement l'exercice de l'autorité publique ou l'exécution d'une mission d'intérêt public dans le cadre de laquelle le traitement est effectué comme nécessaire aux fins de l'article 6, par 1, point e) cf. Avis de l'AHPD 6/2016. La base de la législation nationale est la législation existante sur la politique d'immigration, qui est appliquée en conjonction avec les nouvelles dispositions du RGPD et de la loi n°. 4624/2019, la directive 1/2011 du AHPD sur la protection des personnes et des biens et les lignes directrices 3/2019 du Comité Européen de la Protection des Données sur le traitement des données à caractère personnel au moyen de dispositifs de capture vidéo. La directive 1/2011 stipule (article 2, par 1) que les finalités pour lesquelles le traitement des données à caractère personnel est autorisé sont la protection des personnes et/ou des biens et la fourniture de services de santé. Dans l'ordre juridique grec, pour le traitement des données à caractère personnel par une autorité publique, l'article 14 de la loi v.3917/2011 s'applique également.

En outre, le système « Centaurus » est interconnecté avec la police grecque et, par conséquent, la possibilité de traiter des catégories particulières de données à des fins répressives ne peut en principe être exclue. La législation nationale exige que le responsable du traitement coopère avec les autorités répressives (par exemple, au cours d'une enquête) ; la base juridique de la transmission des données est l'obligation légale prévue à l'article 6, paragraphe 1, point c).

2.6. **Transparence.** La politique de vidéosurveillance se présente sous deux formes, l'une à usage restreint et l'autre à usage public, qui sont publiées respectivement sur l'intranet du MMA et sur le site web du MMA**.** Cette version publique de la politique de vidéosurveillance contient des informations sommaires sur des sujets spécifiques ou des pièces jointes. Les informations ne sont omises de la version publique que lorsque leur confidentialité est absolument nécessaire pour des raisons impérieuses (par exemple, pour des raisons de sécurité ou pour préserver la confidentialité).

2.7. **Pondération des intérêts :** la pondération des intérêts est obligatoire. Les libertés et droits fondamentaux, d'une part, et les intérêts légitimes du responsable du traitement, d'autre part, doivent être soigneusement évalués et mis en balance. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement, à savoir la sauvegarde des biens et la protection des personnes hébergées, des employés et d'autres personnes (obligations de diligence) dans les locaux des installations d'hébergement du MMA, qui ne sont pas supplantés par l'intérêt ou les droits et libertés fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel. Le MMA peut procéder à une surveillance vidéo des personnes séjournant dans les lieux d'hébergement du MMA lorsqu'il existe un intérêt légitime supérieur qui prévaut sur les intérêts, les droits et les libertés des personnes concernées ou pour la constatation, l'exercice ou la défense d'un droit en justice. Le MMA applique le principe de proportionnalité aux systèmes de vidéosurveillance : ceux-ci doivent être proportionnés et nécessaires par rapport à l'objectif poursuivi, qui ne peut être atteint par des moyens moins intrusifs.

Ils possèdent également le droit d'accéder aux données les concernant, ainsi que le droit de demander la rectification des données inexactes ou l'effacement des données qui ont été traitées illégalement (dans le cas des personnes qui ont acquis la nationalité d'un État membre de l'UE au cours de la période qui suit l'introduction d'une demande de protection internationale), et le droit d'être informés des procédures d'exercice de ces droits (voir l'article 29 du Règlement (UE) n° 603/2013).

Les droits sont exercés auprès du responsable du traitement, qui est le MMA.

Le MMA assure que la surveillance des résidents dans les installations d'hébergement des CAI (Services d'Accueil et d'Identification) du ministère n'est pas autorisée, sauf dans des cas exceptionnels :

– est justifiée par la nature et les conditions de vie dans les lieux d'hébergement ; et

– est nécessaire pour protéger leur santé et leur sécurité ou pour protéger des zones critiques à l'intérieur des installations d'hébergement

Les données collectées par le système de vidéosurveillance ne seront pas utilisées comme critères de profilage ou d'évaluation du comportement général (religieux, racial, sexuel, etc.).

Le MMA assure que la surveillance des employés (fonctionnaires du Service d'Accueil et d'Identification et du service d'asile du MMA, officiers de police et employés du ministère des, du ministère des affaires étrangères de la République de Chypre et du Ministère de la Protection Civile, les officiers de police et les agents de protection des citoyens, les employés de diverses professions des organisations non gouvernementales (avocats, interprètes, travailleurs sociaux, psychologues, médecins, agents de santé), le personnel du Bureau européen de soutien pour l'asile (European Asylum Support Office – EASO) et les personnes recrutées par les services locaux (OTA) dans le cadre des programmes de travaux d'intérêt général de l'OAED) sur les lieux de travail ne sont pas autorisés, sauf dans des cas exceptionnels :

– est justifiée par la nature et les conditions du travail ; et

– est nécessaire pour protéger la santé et la sécurité des travailleurs ou pour protéger les lieux critiques de travail

Les données collectées par le système de vidéosurveillance ne seront pas utilisées comme critères exclusifs d'évaluation du comportement et des performances des employés.

2.8. **Contrôles réguliers**. Un contrôle régulier de la protection des données sera effectué chaque année par les fonctionnaires du ministère. Au cours de ces révisions périodiques, nous réévaluerons la protection des données :

- le système de vidéosurveillance reste nécessaire,
- le système continue à servir l'objectif fixé,
- les mesures de sécurité des informations enregistrées sont adéquates,
- les alternatives appropriées ne sont pas disponibles.

Les examens réguliers couvriront également toutes les autres questions abordées dans le premier rapport, en particulier la question de savoir si notre politique de vidéosurveillance reste conforme au règlement et aux lignes directrices (contrôle d'adéquation) et si elle est suivie dans la pratique (contrôle de conformité). Des copies des rapports périodiques seront également jointes à la présente politique de vidéosurveillance et en feront partie intégrante.

2.9. **Solutions technologiques respectueuses de la vie privée.** Les solutions technologiques et organisationnelles suivantes visant à protéger la vie privée sont également mises en œuvre, à titre d'exemple (voir les lignes directrices, section 3.4) :

- Marques spéciales CCTV de vidéosurveillance placée à des endroits bien visibles
- Modification du ciblage des caméras (minimisation des données)
- Les enregistreurs sont placés dans des lieux sécurisés où des mesures appropriées sont en place
- Caméras installées dans la salle informatique

2.10 **Vidéosurveillance ad hoc à l'aide d'un drone**

Afin d'assurer la sécurité des hôtes des installations d'hébergement du SAI, du personnel et des visiteurs, des bâtiments et des biens, le ministère des Migrations et de l'Asile (MMA), en tant que configuration du système CENTAURUS, a la possibilité d'effectuer une **surveillance vidéo ad-hoc à l'aide d'un équipement Drone**. La vidéosurveillance à l'aide d'un drone n'est mise en œuvre que dans des cas exceptionnels.

Les opérateurs de drones et les pilotes planifient les trajectoires de vol et les angles auxquels les données des capteurs de drones sont collectées de manière à réduire au minimum le risque d'enregistrer des personnes se trouvant dans ces bâtiments ou emplacements ou y entrant ou en sortant, sauf si cela est nécessaire aux fins de l'exploitation du drone.

Les opérateurs de drones et les pilotes planifient leur temps de vol, par exemple l'heure de la journée et le jour de la semaine, de manière à minimiser le risque d'enregistrer des personnes dans ces lieux. Par exemple, les opérations à proximité de lieux de culte

(dans les installations d'accueil) pendant les heures de prière, à moins que cela ne soit nécessaire aux fins de l'exploitation du drone.

Dans la mesure du possible, les opérateurs de drones et les pilotes souhaitant voler à proximité de sites sensibles doivent informer les représentants responsables de ces sites des détails de leur opération et rester visibles à tout moment.

Lorsque des catégories particulières de données à caractère personnel sont susceptibles d'être collectées au cours d'un vol de drone au-dessus ou à proximité de zones sensibles, les opérateurs et les pilotes doivent s'assurer qu'ils agissent sur une base juridique appropriée conformément aux articles 9 et 10 du RGPD.

Les contrôleurs de drones et les pilotes planifient et exécutent leurs vols de manière à limiter la collecte de données à caractère personnel aux données nécessaires aux fins de l'exploitation du drone.

Les exploitants et les pilotes de drones cherchent à enregistrer le minimum de données à caractère personnel et la qualité minimale des données à caractère personnel requises aux fins de l'exploitation du drone. Cette exigence s'étend au type de capteurs utilisés, à leur puissance, au type de données collectées et au type de trajectoire de vol choisie.

Pour minimiser les données personnelles collectées et le degré d'intrusion dans la vie privée, les pilotes et les opérateurs de drones :

• Ils pilotent le drone de manière à collecter et/ou enregistrer le moins de données possible sur les personnes non impliquées au sol,

• Ils utilisent des capteurs bas de gamme ou ajustent la qualité des données par le biais de contrôles logiciels,

• Ils contrôlent les capteurs du drone qui sont activés pendant le vol et le moment où ils le sont,

• Ils contrôlent le moment où les données sont enregistrées et le moment où elles sont transmises,

• Ils enregistrent des images plutôt que des vidéos,

• Ils utilisent un flux en direct sécurisé au lieu d'enregistrer des données,

• Utiliser des alternatives à l'imagerie photographique, par exemple l'imagerie thermique,

• Ils volent à des altitudes plus ou moins élevées, selon les circonstances, afin de minimiser l'impact sur les personnes au sol.

Lorsqu'un vol de drone a lieu à proximité de personnes non impliquées et surtout lorsqu'il a lieu au-dessus ou à proximité de zones privées ou sensibles, l'équipement du drone dispose de capacités logicielles de contrôle :

• les capteurs activés, par exemple optiques, thermiques, audio, de géolocalisation et lorsque les capteurs sont activés ou désactivés pendant le vol,

• la direction dans laquelle les capteurs du drone sont orientés ou l'angle sous lequel ils fonctionnent,

• la qualité des données enregistrées (par exemple, la résolution, la sensibilité du capteur), et/ou

• quand les données collectées sont enregistrées et quand elles ne le sont pas.

Les pilotes de drone sont entrainés et capables d'utiliser l'équipement de drone sélectionné de manière sûre et efficace et de le contrôler de manière à réduire les données à caractère personnel enregistrées au strict minimum, dans l'unique but de l'utilisation du drone.

3. Quelles sont les infrastructures du MMA sous surveillance ?

CENTRE AGIA EIRINI
CENTRE ALEXANDRIA
CENTRE D'ACCUEIL DIAVATA
CENTRE DRAMA
CENTRE ELEYSINA
CENTRE FILIPPIADA
RIC FYLAKIOU
CENTRE KATSIKA
CENTRE KAVALAS
ÉTABLISSIMENT KERANIS
CENTRE CORINTHE
CCAC KOS
CENTRE KOUTSOXEROU
CENTRE KYLLINI
CENTRE LAGADIKON
CCAC LEROS
CENTRE D'ACCUEIL Malakasa
RIC Malakasa
CENTRE OINOFYTA
CENTRE POLYKASTRO
CENTRE PYRGOS
CENTRE RITSONAS
CCAC SAMOS
CENTRE SCHISTOU
CENTRE SERRES
CENTRE SINTIKI
CENTRE THIBAS
CENTRE VAGIOHORIOU
CENTRE VEROIA
CENTRE VOLOS

- L'accès aux caméras et aux archives n'est autorisé qu'au personnel permanent du MMA, de la société de sécurité et de la police grecque.

Il n'y a pas de caméras dans les endroits où l'on s'attend à ce que la vie privée soit respectée, tels que les bureaux individuels, les zones de loisirs, les toilettes, les installations sanitaires et autres. L'emplacement des caméras a été soigneusement étudié afin de minimiser la surveillance des zones qui ne sont pas pertinentes pour les objectifs visés.

4. Quelles sont les informations personnelles que nous recueillons et dans quel but ?

4.1. **Description concise et spécifications techniques détaillées du système**. Le système de vidéosurveillance est un système mixte composé de caméras statiques et de caméras de type PTZ. Il enregistre des images numériques et est équipé d'un système de détection de mouvement. Il enregistre tout mouvement dans les zones couvertes, ainsi que l'heure, la date et le lieu. Toutes les caméras fonctionnent 24 heures sur 24, sept jours sur sept. La qualité de l'image permet dans la plupart des cas d'identifier des personnes dans les zones couvertes par la caméra (voir instructions, section 6.4). Les caméras fixes sont préconfigurées et ne peuvent pas être déplacées ou mises au point par les opérateurs. Les caméras PTZ peuvent être contrôlées par les opérateurs. Seul le responsable de l'installation est habilité à modifier les paramètres de ciblage et d'enregistrement.

Aucune technique de surveillance intelligente ou de haute technologie n'est utilisée (voir le point 6.9 des lignes directrices), le système n'est pas interconnecté avec d'autres systèmes puisqu'un réseau physiquement isolé est utilisé (point 6.10), il n'y a pas de connexion ou d'accès à l'internet et aucune surveillance secrète (point 6.11), enregistrement audio ou "télévision en circuit fermé parlante" (point 6.12) n'est utilisée.

4.2. **Objectif de la surveillance**. Le MMA utilise le système de vidéosurveillance dans le seul but d'assurer la sécurité des résidents des structures d'hébergement, du personnel qui y travaille, des moyens et infrastructures et du contrôle d'accès. Le système de vidéosurveillance permet de contrôler l'accès au bâtiment et d'assurer la sécurité des installations des centres d'hébergement, la sécurité des résidents, du personnel et des visiteurs, ainsi que des biens et des informations situés ou stockés dans les installations. Il complète d'autres systèmes de sécurité physique, tels que les systèmes de contrôle d'accès physique et les systèmes de contrôle d'intrusion. Elle s'inscrit dans le cadre de mesures visant à soutenir des politiques de sécurité plus larges et contribue à prévenir, dissuader et, si nécessaire, enquêter sur les accès physiques non autorisés, y compris l'accès non autorisé à des zones sécurisées telles que les bureaux protégés, l'infrastructure des systèmes d'information ou les informations opérationnelles. En outre, la vidéosurveillance contribue à la prévention, à la détection et à l'investigation des vols d'équipements ou de biens appartenant au gouvernement hellénique, aux visiteurs ou au personnel, ainsi que des menaces pour la sécurité des résidents, des visiteurs ou du personnel travaillant dans les bureaux (par exemple, incendie, agression).

4.3. **Limitation de la finalité.** Le système n'est pas utilisé à d'autres fins, par exemple pour contrôler le travail des employés ou leur présence au travail. Le système est utilisé comme outil d'investigation (autre que pour les enquêtes sur les incidents).

Les images ne peuvent être transférées aux organes d'enquête (Police grecque, Procureur général) que dans des cas exceptionnels, dans le cadre d'une enquête disciplinaire ou pénale formelle, comme décrit au point 6.5 ci-dessous (voir les points 5.7, 5.8 et 10.3 des lignes directrices).

4.4. **Aucune surveillance ad hoc n'est prévue**. Aucune fonction de surveillance ad hoc n'est prévue (voir les lignes directrices, section 3.5).

4.5. **Caméras Internet**. Les caméras Internet ne sont pas autorisées (voir section 5.10 des lignes directrices).

4.6. **Aucune catégorie spécifique de données n'a été collectée.** Aucune catégorie particulière de données n'est collectée (point 6.7 des lignes directrices).

5. **Quelle est la base juridique de la vidéosurveillance ?**

La base juridique principale ou générale du traitement de la vidéosurveillance est l'exécution d'une mission d'intérêt public dans l'exercice de l'autorité publique [art. 6, par. 1, point g), du RGPD].Le traitement de catégories particulières de données (biométriques) est effectué pour des raisons d'intérêt public important (article 9, paragraphe 2, point g), du RGPD), sur la base du règlement Dublin III ou du code de l'immigration, tandis que les CCAC constituent des "infrastructures critiques de l'État", conformément à la loi n° 4624/2019 et basé sur les consignes 1/2011 et aux lignes 3/2019 du CEPD. L'intérêt public réside dans la nécessité de protéger les infrastructures critiques appartenant à l'État grec, les ressources humaines et les informations qu'elles contiennent contre les actes illicites. En outre, avec un sens particulier de la responsabilité et du respect de l'être humain, le cadre de protection susmentionné inclut également la sécurité de la vie, l'intégrité physique, la santé et les biens des résidents, de notre personnel, de nos partenaires et, en général, des visiteurs entrant dans la zone surveillée. La collecte de données est limitée à la prise d'images uniquement et dans des lieux où nous avons évalué qu'il existe une possibilité accrue de commettre des actes illégaux et une protection accrue des personnes et des biens, par exemple aux points d'entrée, sans se concentrer sur les lieux où la vie privée des personnes dont les images sont prises peut être excessivement restreinte, y compris leur droit au respect des données à caractère personnel.

6. Qui a accès aux informations et à qui sont-elles divulguées ?

6.1. **Personnel de sécurité et partenaires externes - agents de sécurité.** La vidéo enregistrée n'est accessible qu'aux employés autorisés du MMA et non à l'ensemble du personnel de sécurité et de gardiennage. La vidéo en direct dans le centre de réception des signaux est accessible aux agents de sécurité en service. Ces agents appartiennent à une société spécialisée sous-traitante qui fournit des services de sécurité, de maintenance et d'assistance technique pour les systèmes, qui peuvent être sous-traités en vertu de l'article 14, par. 1 N3907/2011. La société contractante est liée par un contrat écrit

qui assure la confidentialité et la sécurité du traitement (sous-traitant).

6.2. Droits d'accès. La politique de sécurité de la MMA en matière de vidéosurveillance (voir section 7 ci-dessous) doit clairement spécifier et documenter par écrit qui a accès au matériel de vidéosurveillance et/ou à l'architecture technique du système de vidéosurveillance, dans quel but et quel est le contenu des droits d'accès. En particulier, le document doit préciser qui a le droit :

- Visualisation de la vidéo en temps réel,
- Visionnage du matériel enregistré ou
- Copie d'un fichier d'enregistrement optique,
- Téléchargement d'un fichier d'enregistrement optique,
- Suppression d'un fichier d'enregistrement optique ; ou
- Modifier les paramètres de n'importe quelle partie du matériel.

6.3. **Formation à la protection des données**. Tous les membres du personnel du MMA disposant de droits d'accès, y compris les agents de sécurité qui sont des contractants externes, ont suivi au moins une formation à la protection des données. Une formation est prévue pour chaque nouveau membre du personnel et des séminaires périodiques de sensibilisation à la protection des données et de conformité seront organisés au moins une fois tous les deux ans pour l'ensemble du personnel disposant de droits d'accès (voir le point 8.2 des lignes directrices).

6.4. **Obligations de confidentialité.** Après la formation, chaque membre du personnel de sécurité du contractant est lié par un accord de confidentialité. L'accord a également été signé par le sous-traitant (société de projet contractante) qui met à disposition les collaborateurs externes. (voir section 8.3 des lignes directrices).

6.5. **Transferts et divulgations**. Tous les transferts et divulgations de données en dehors du module de sécurité doivent être documentés et soumis à une évaluation rigoureuse de la nécessité du transfert et de la compatibilité des objectifs du transfert avec l'objectif initial de sécurité et de contrôle d'accès du traitement (voir le chapitre 10 des lignes directrices). La politique de transfert est régie par le GDPR 679/2016 (voir les sections 10.5 et 7.2 des lignes directrices). Le DPD du MMA est consulté dans tous les cas.

Les autorités de poursuite et de police peuvent y avoir accès dans le cadre d'enquêtes ou de poursuites pénales**.**

Dans des cas exceptionnels, l'accès peut également être accordé :

- Au Procureur sur son ordre
- À l'autorité de surveillance compétente
- Les personnes qui mènent une enquête interne formelle ou une procédure disciplinaire au sein de l'entreprise,

à condition que l'on puisse raisonnablement s'attendre à ce que les transferts contribuent à l'enquête ou à la poursuite d'une infraction disciplinaire ou pénale. Les demandes de collecte de données ne seront pas servies.

7. **Comment protégeons-nous et sauvegardons-nous les informations ?**

Afin de protéger la sécurité du système de vidéosurveillance, une certaine procédure a été établie. Cette procédure comprend des instructions destinées au service ou à la société de gardiennage extérieure qui supervise les moniteurs à l'entrée des structures.

Les mesures de sécurité raisonnables suivantes sont notamment prises :

- Des zones sécurisées, protégées par des mesures de sécurité physique, hébergent les serveurs qui stockent les images enregistrées. Des pares-feux de réseau protègent le périmètre logique de l'infrastructure informatique. Les principaux systèmes informatiques contenant les données font l'objet de mesures de sécurité et de contrôle d'accès renforcées
- Les mesures administratives comprennent l'obligation pour chaque membre du personnel de - toute partie extérieure ayant accès au système (y compris les personnes chargées de la maintenance des équipements et des systèmes) à prendre des mesures de sécurité distinctes.
- Les utilisateurs ne se voient accorder des droits d'accès qu'au niveau strictement nécessaire à l'exécution de leurs tâches.
- Seul l'administrateur du système spécifiquement désigné par le responsable du traitement à cette fin est en mesure d'accorder, de modifier ou de révoquer les droits d'accès des personnes.
- Toute attribution, modification ou suppression de droits d'accès doit être conforme aux critères définis dans la politique de sécurité en matière de vidéosurveillance.
- La politique de sécurité en matière de vidéosurveillance contient une liste actualisée de toutes les personnes ayant accès au système à un moment donné et précise leurs droits d'accès.

8. **Combien de temps conservons-nous les données ?**

Les enregistrements visuels des caméras de surveillance sont conservés pendant 15 jours, après quoi ils sont automatiquement supprimés. Si nous détectons un incident pendant cette période, nous isolons une partie de la vidéo et la conservons pendant un (1) mois au maximum, afin d'enquêter sur l'incident et d'entamer une procédure judiciaire pour défendre nos intérêts légaux, tandis que si l'incident implique un tiers, nous conservons la vidéo pendant trois (3) mois au maximum. Si les fichiers et les données audio et vidéo stockés ou l'enregistrement effectué en temps réel ne donnent pas lieu à la survenance d'un événement relevant de la finalité prévue, les données seront détruites au plus tard dans les quinze (15) jours civils, sous réserve de dispositions plus spécifiques de la législation applicable à des catégories particulières de responsables du traitement des données. En cas d'incident lié à la finalité du traitement, le MMA conserve les téléchargements dans lesquels l'événement en question a été enregistré

dans un dossier distinct pendant trois (3) mois. Après la période susmentionnée, le MMA peut conserver les données pendant une période plus longue uniquement dans des cas exceptionnels où l'incident nécessite une enquête plus approfondie. Dans ce cas, le MMA a l'obligation d'informer l'Autorité de la durée nécessaire pour conserver ces téléchargements. Si des séquences doivent être conservées pour approfondir l'enquête ou prouver un incident de sécurité, elles peuvent être conservées si nécessaire et uniquement avec l'autorisation du délégué à la protection des données. La demande de conservation est strictement documentée et la nécessité de la conservation est réexaminée périodiquement, avec l'avis du délégué à la protection des données.

Le système est également surveillé en direct par le personnel de sécurité à la réception de chaque abri et dans le bâtiment de sécurité, 24 heures par jour.

9. **Comment fournissons-nous des informations au public ?**

9.1. Approche à plusieurs niveaux : fournir au public des informations sur la manière de regarder la vidéo de manière efficace et complète (voir les lignes directrices, section 11). À cette fin, nous adoptons une approche à plusieurs niveaux, qui consiste en une combinaison des deux méthodes suivantes :

- des avis sur le site (panneaux d'information) pour informer le public qu'une surveillance est en cours et pour lui fournir des informations utiles sur le traitement ; et
- Des brochures sur la politique de surveillance sont également disponibles à la réception des abris. Un numéro de téléphone et une adresse électronique sont fournis pour toute demande de renseignements.
- Nous prévoyons également une notification sur place, à proximité des zones surveillées. Nous avons placé un avis à l'entrée principale, un à la réception, un à l'entrée du parking et un au bureau annexe dans la cour.

L'avis de protection des données sur site de l'agence figure à l'annexe 8.

9.2. **Notification individuelle spéciale.** En outre, les personnes doivent également recevoir une notification individuelle si elles sont filmées (par exemple, par le personnel de sécurité au cours d'une enquête de sécurité), pour autant qu'une ou plusieurs des conditions suivantes soient remplies :

- Leur identité est indiquée dans chaque fichier,
- L'enregistrement vidéo est utilisé contre l'individu,
- Il est conservé au-delà de la période de conservation normale,
- déplacé à l'extérieur de l'installation de sécurité, ou
- Si l'identité de la personne est divulguée à une personne extérieure à l'installation de sécurité.

Le signalement peut parfois être temporairement retardé, par exemple s'il est nécessaire à la prévention, à l'enquête, à la détection et à la poursuite d'activités criminelles.

Dans tous ces cas, le DPD est consulté pour s'assurer que les droits de la personne sont respectés.

10. **Comment les membres du public peuvent-ils vérifier, modifier ou supprimer leurs informations** ? Le public a le droit d'accéder aux données personnelles détenues et de les corriger et/ou de les compléter. Toute demande d'accès, de rectification, de blocage et/ou de suppression des données personnelles doit être adressée au délégué à la protection des données en charge du MMA (courriel : dpo@migration.gov.gr formulaire de contact : https://migration.gov.gr/epikoinonia, 196 - 198 Avenue Thivon, P.O. Box 182 33, Agios I. Rentis - Nikaia, Attique). Il/elle peut également vous contacter pour toute autre question concernant le traitement des données personnelles.

Dans la mesure du possible, le MMA répond à une demande d'enquête dans un délai de 30 jours ouvrables. Si cela n'est pas possible, le demandeur est informé des prochaines étapes et de la raison du retard dans les 30 jours. Même dans les cas les plus complexes, l'accès est accordé ou une réponse finale motivée rejetant la demande est donnée dans un délai d'un mois au plus tard. Le MMA doit faire de son mieux pour répondre plus tôt, en particulier si le demandeur démontre l'urgence de sa demande.

En cas de demande spécifique, le visionnage des images peut être organisé ou le demandeur peut recevoir une copie des images enregistrées sur un DVD ou un autre support de stockage portable (clé USB). Dans le cas d'une telle demande, les demandeurs doivent décliner leur identité au-delà de tout doute raisonnable (par exemple, ils doivent porter une carte d'identité lorsqu'ils sont surveillés) et, dans la mesure du possible, préciser également la date, l'heure, le lieu et les circonstances au moment de l'enregistrement dans le système de vidéosurveillance. Ils doivent également fournir une photographie récente et nette d'eux-mêmes, permettant au personnel de sécurité de les identifier à partir des images examinées.

Une demande d'accès peut être refusée si, par exemple, la restriction de l'accès est nécessaire pour sauvegarder l'enquête sur une infraction pénale. La restriction peut également être nécessaire pour protéger les droits et libertés d'autres citoyens/travailleurs, par exemple lorsque d'autres personnes sont également présentes dans la vidéo et qu'il n'est pas possible d'obtenir leur consentement à la divulgation de leurs données à caractère personnel ou d'utiliser le traitement d'images pour remédier à l'absence de consentement.

11. **Droit de recours**

Toute personne a le droit de saisir l'autorité chargée de la protection des données à caractère personnel si elle estime que ses droits ont été violés du fait du

le traitement de leurs données personnelles par l'organisation. Auparavant, nous recommandons aux personnes concernées d'essayer de prendre contact avec :

- Le MMA (voir coordonnées ci-dessus) et/ou
- Le délégué à la protection des données du MMA

Les employés du MMA peuvent également demander un réexamen par l'autorité administrative compétente en vertu du statut général du personnel du MMA.

Dernière mise à jour : juin 2024