Politique de vidéosurveillance De la SIDR

TABLE DES MATIERES

1. Objet et champ d'application de la politique de vidéosurveillance 2

2. Respect de la vie privée, protection des données et conformité réglementaire. 2

2.1. État de conformité 2

2.2. Audit 2

2.3. Notification de l'état de conformité au CEPD 2

2.4. Décision d'installer la vidéosurveillance au sein de la BEI. 3

2.5. Transparence. 3

2.6. Examens périodiques. 3

2.7. Solutions techniques favorisant le respect de la vie privée. 3

3. Espaces placés sous vidéosurveillance 4

4. Type d'informations à caractère personnel collecté et finalité 5

4.1. Brève description et caractéristiques techniques du système. 5

4.2. Objet de la surveillance 5

4.3. Limitation des finalités 6

4.4. Activités de surveillance ponctuelle. 6

4.5. Absence de collecte de catégories particulières de données. 6

5. Qui a accès aux données collectées et à qui sont-elles communiquées ? 7

5.1. Le personnel chargé de la sécurité interne et les agents de sécurité 7

5.2. Droits d'accès 8

5.3. Formation et information du personnel à la protection des données 8

5.4. Engagement de confidentialité du personnel de sécurité. 8

5.5. Transfert et communication de données 8

6. Comment est assurée la protection des données collectées ? 9

7. Durée de conservation des données 9

8. Information du public. 9

8.1. Approche multicouche 9

8.2. Notifications individuelles 10

9. Accès du public aux données 10

10. Droit de recours 11

1. Objet et champ d'application de la politique de vidéosurveillance

Ce document présente la politique de gestion des systèmes de vidéosurveillance, en fonction des besoins et contraintes de la SIDR en matière de sécurité, dans le respect des textes de références à savoir :

- Loi du 6 janvier 1978 modifiée en 2004 dite « loi informatique et libertés » ;
- Article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité dite « loi Pasqua » et décret n°96-926 du 17 octobre 1996
- Le code de la sécurité intérieur : Art L251-1 et suivant (information des IRP)
- Le code du travail : art L2323-32, art L1221-9 et L1222-4 (information individuelle des salariés),

À ces différents textes de loi sur la vidéosurveillance s'ajoute le décret du 3 août 2007 définissant les nouvelles normes techniques applicables à la vidéosurveillance et les articles du code civil et pénal en cas de non-respect des obligations ci-dessus.

2. Respect de la vie privée, protection des données et conformité avec la réglementation.

2.1. État de conformité

Le service Audit Qualité Procédures Sécurité :

- Définit les grands principes du système de vidéosurveillance déployé sur le patrimoine immobilier de la SIDR et dans ses locaux professionnels accueillant du public,
- Veille à l'adéquation des installations avec les besoins de sécurité et de sureté de chacun des sites rencontrés.
- Assure la conformité des équipements et du système en général par rapport aux recommandations du CEPD (le Comité Européen de la Protection des Données) et au suivie de la CNIL (Commission nationale de l'informatique et des libertés)
- Gère la coordination administrative préalable au déploiement et l'exploitation ultérieure des enregistrements

2.2. Audit

Lors de toute nouvelle installation ou modification notoire d'un système existant, la SIDR effectue un audit et une analyse d'impact de ces modifications. Lors de l'audit, les réclamations locataires relatives à la sécurité et à l'insécurité sur le groupe sont pris en compte.

Lorsqu'il s'agit d'immeuble d'habitation ou lorsqu'il s'agit de locaux de travail, les représentants du personnel et le correspondant protection des données-SIDR (correspondant informatique et liberté), sont informés du projet.

2.3. Notification de l'état de conformité à la CNIL

Compte tenu du déploiement du système, la SIDR a jugé nécessaire d'informer la CNIL de l'existante d'une politique vidéo-surveillance SIDR et de lui communiquer pour chacun des sites équipés un dossier complet avant sa réalisation.

Lors de l'adoption de la présente politique de vidéosurveillance, nous avons par ailleurs notifié notre état de conformité à la CNIL en lui adressant un exemplaire de notre politique de vidéosurveillance et une trame type d'un futur rapport d'audit.

La mise à disposition de chacun des dossiers réalisés par la SIDR à la CNIL sera possible sur simple demande écrite de celle-ci.

2.4. Décision d'installer la vidéosurveillance au sein de la SIDR

La vidéosurveillance a été mise en place dans le cadre de la mise en sureté globale du patrimoine immobilier et des locaux professionnels de la SIDR.

2.5. Transparence

La politique de vidéosurveillance SIDR existe en deux versions,

- L'une, à diffusion restreinte comportant l'ensemble des spécificités techniques types, les procédures SIDR les noms des intervenants SIDR et en annexe un dossier complet de chaque installation.
- L'autre, publique (la présente version), est consultable sur notre intranet Bichiques ainsi que sur notre site Web à l'adresse suivante : www.sidr.fr

La présente version publique de la politique de vidéosurveillance est une synthèse de la politique générale de la SIDR en la matière.

Pour des raisons de sécurité, certaines informations confidentielles ne sont pas reprises dans la version publique (implantation des camera système d'enregistrements, passage des câbles d'alimentation, etc ...) mais peuvent être consultées par la CNIL sur demande.

Par ailleurs, des affichages spécifiques sont mis en place au niveau des locaux SIDR et dans les bâtiments afin de signaler aux usagers ainsi qu'aux visiteurs que les sites sont sous vidéosurveillance.

2.6. Examens périodiques

Des examens périodiques sont réalisés. Ils servent à vérifier notamment si la politique de vidéosurveillance est toujours conforme au règlement et aux lignes directrices de la SIDR.
A minima une fois par an à date anniversaire de la mise en service de l'installation la SIDR fait réaliser, par une entreprise spécialisée externes (sous contrôle du service Maitrise des Risques et Système au Pilotage), un examen des systèmes de vidéosurveillance
Lors de ces examens périodiques, sont réévalués :

- L'utilité du système de vidéosurveillance ;
- Son adéquation avec les finalités pour lesquelles il a été conçu ;
- La nécessite de faire évoluer l'installation
- L'existence éventuelle d'alternatives appropriées.

Ces audits peuvent être complétés autant que de besoins par le service Maitrise des risques et système au pilotage de la SIDR.

2.7. Solutions techniques favorisant le respect de la vie privée

Les principales solutions techniques mises en œuvre favorisent le respect de la vie privée et s'orientent autour de 2 axes principaux, pour chaque typologie d'installation à savoir :

<u>Pour la typologie « immeubles d'habitation »</u>

- la position et les angles de prises de vues des caméras sont établis de manière à ne filmer que les parties privées de la SIDR à savoir les **espaces communs**
Sont donc exempt des enregistrements les zones des bâtiments pour lesquels les attentes en matière de respect de la vie privée sont élevées : (portes palières privatives des appartements, les balcons ou terrasses privatives des locataires les espaces extérieurs du domaine public, etc.…).

- L'accès aux données enregistrées n'est autorisé que par mot de passe et pour la seule personne responsable du traitement des données, à savoir le Directeur General de la SIDR.

Il peut déléguer ces droits à une personne désignée dans la liste définie à cet effet dans la démarche globale.

Pour la typologie « locaux administratifs »

- la position et les angles de prises de vues des caméras sont établis de manière à ne filmer que les parties privées de la SIDR réservées à l'accueil du public mais également à la protection des bien en cas d'intrusion dans les locaux …
Sont donc exempt des enregistrements les zones pour lesquels les attentes en matière de respect de la vie privée sont élevées : (ex. : les bureaux, les espaces de détente, les toilettes, les vestiaires, les accès et locaux des IRP pendant les heures d'activité …)

- L'accès aux données enregistrées n'est autorisé que par mot de passe et pour la seule personne responsable du traitement des données, à savoir le Directeur General de la SIDR. Il peut déléguer ces droits à une personne désignée dans la liste définie à cet effet dans la démarche globale. La programmation spécifique (heure de mise en service ou d'arrêt des enregistrements pour les locaux des IRP sont fait en présence d'un représentant des IRP).

Particularité SIDR :

Pour l'ensemble des locaux d'accueils public (hall d'agence, hall locaux administratifs, bureau d'encaissement, et bureaux d'accueil personnalisé individuel) la SIDR couplera l'enregistrement sonore à la prise de vue pour permettre la levée de doute en cas d'agression verbale avec ou sans manifestation physique de l'agresseur vis-à-vis d'un des salariés SIDR. (Les conditions d'accès et d'affichage seront identiques à celles de la vidéo-surveillance simple)

3. Espaces placés sous vidéosurveillance

Vidéo-surveillance simple

Pour la typologie « immeubles d'habitation »

Pour assurer la sécurité du personnel, des visiteurs et pour la protection des biens, les espaces suivants seront susceptibles d'être sous vidéosurveillance :

- Parking,
- Local vélos ou poussettes,
- Hall d'entrée,
- Les entrées et les sorties du bâtiment
- Locaux VO,
- Portes d'ascenseur,
- Escaliers,
- Zone de dépose des encombrants,
- Gaines techniques,
- Local vidéosurveillance,
- Certaines zones comportant des équipements techniques spécifiques
- Espaces extérieurs si résidentialisés avec un contrôle d'accès

Pour la typologie « locaux administratifs »

Pour assurer la sécurité du personnel, des visiteurs et pour la protection des biens, les espaces suivants seront susceptibles d'être sous vidéosurveillance :

- Les halls d'accueil public
- Les bureaux d'accueils individualisés et personnalisés } Avec enregistrements sonores
- Les parkings aériens et souterrains privés et clôturés
- Les zones de stockages
- Les locaux à risques particuliers regroupant des informations sensibles et qui nécessitent une protection renforcée pour une raison bien spécifique;
- Les entrées et les sorties des bâtiments (y compris les issues de secours),

4. Type d'informations à caractère personnel collecté et finalité

4.1. Brève description et caractéristiques techniques du système

Pour chaque bâtiment de la SIDR équipés d'un système de vidéosurveillance système est conçu selon le même principe. Seules les quantités de matériel (caméras, enregistreurs) changent selon la taille du site et les besoins en matière de sécurité.
Etant donné que chaque bâtiment est équipé de son propre système, les images provenant des Caméras qui y sont installées sont gérées et traitées localement.
Le système se compose de plusieurs enregistreurs numériques équipés chacun d'un disque dur où sont stockées les images et d'un dispositif de détection de mouvement. Il enregistre tous les mouvements détectés par les caméras dans les zones placées sous surveillance, ainsi que la mention de la date, de l'heure et du lieu d'enregistrement.

Toutes les caméras :

- Fonctionnent 24h/24, sept jours sur sept dans les locaux d'habitation. Pour les bureaux il en est de même à l'exception de celles a proximité ou dans les locaux IRP qui ne sont activée qu'entre 20h et 6h, les weekends et jours fériés.
- Comportent des projecteurs infrarouges intégrés pour la surveillance nocturne.
- Bénéficient d'un positionnement visible, aucune camera n'est dissimulée
- Fonctionnent sans système « intelligent » de TRACKING toutes fois tous les autres systèmes permettant d'améliorer la netteté des images peuvent équiper les cameras SIDR. (BLC, WDR, HLC, DEFOGGING, 3DDNR ...)

Certaines caméras positionnées dans les zones accessibles au public dans nos locaux administratifs peuvent être a vision 360 sous réserve de ne pas être motorisées, elles peuvent aussi bénéficier d'enregistrements sonores.

La liste des caméras et des enregistreurs sites par site peut être consultée par les organismes de contrôle sur simple demande et font partie du dossier de politique vidéosurveillance a diffusion restreinte.

4.2. Objet de la surveillance

La SIDR utilise son système de vidéosurveillance à des fins de sécurité et de sureté exclusivement.
Le système de vidéosurveillance contribue à assurer la protection des infrastructures, la sécurité du personnel, des locataires et des visiteurs, ainsi que la protection des biens et des informations situées ou stockées dans les locaux tels que les bureaux SIDR.

Pour les locaux administratifs uniquement l'utilisation de l'image peut également être utilisée pour une fonction de contrôle d'accès à certaines zones.

Le système de vidéo intervient obligatoirement en complément d'autres systèmes de sécurité physique tels que les systèmes de contrôle des accès et détection intrusions physiques. Il fait partie des mesures adoptées pour renforcer les mesures plus générales appliquées dans le domaine de la sécurité et contribue à prévenir, à dissuader.
De plus, la vidéosurveillance contribue :

- À la levée de doute et à l'identification en cas d'atteintes à la sécurité des visiteurs ou du personnel travaillant dans les locaux (agressions physiques, ou verbales par exemple).
- Faciliter les enquêtes des forces de l'ordre en cas de vol d'équipement, de matériel, de dégradations ou de détériorations d'équipements dont la SIDR est régulièrement concernée.

4.3. Limitation des finalités

Le système n'est utilisé à nulles autres fins que celles exposées ci-dessus. Il n'est pas utilisé pour surveiller le travail des employés ou pour contrôler leur présence sur leur lieu de travail. Il n'est pas non plus utilisé à des fins d'enquête (autres que celles faisant suite à des incidents ou incivilités telles que définis ci-dessus).
Les éventuels transferts d'images vers des organes d'enquête ne peuvent avoir lieu que dans des circonstances spécifiques, et sur demande des forces de l'ordre (cadre délits ou d'enquêtes judiciaires), conformément aux dispositions de la politique générale de vidéosurveillance.
Aucune autre utilisation ne pourra en être faite.

4.4. Activités de surveillance ponctuelle

La SIDR ne fait pas pour ses bâtiments d'habitation de surveillance ponctuelle. Cependant à la demande des forces de l'ordre ou du service de sureté d'une commune la SIDR pourra permettre cette activité de surveillance ponctuelle via son système vidéo, si et seulement si la demande est faite par écrit. Dans ce cas le service Maitrise des Risques et Système au Pilotage de la SIDR tient à jour un registre des interventions il en est de même pour toute consultation de données.

4.5. Absence de collecte de catégories particulières de données

Les systèmes de vidéosurveillance en place dans les bâtiments ou les locaux de la SIDR n'ont pas pour objet de capter (en zoomant ou en orientant délibérément la caméra à cette fin, par exemple) ou, d'une manière générale, de traiter des images (en les indexant ou en établissant des profils) susceptibles de révéler des « catégories spéciales de données », à savoir : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé ou à la vie sexuelle1.
Aucune surveillance de zones propices à la révélation, par les images captées, de données relevant de ces catégories particulières n'est effectuée par les systèmes vidéosurveillance de la SIDR.

5. Qui a accès aux données collectées et à qui sont-elles communiquées ?

5.1. Le personnel chargé de la sécurité interne et les agents de sécurité externes.

Pour les bâtiments d'habitation :
Les enregistrements de vidéosurveillance sont uniquement accessibles au Responsable du Traitement des Données et sur site, à savoir :

- Pour la SIDR le Directeur général de la SIDR ou par délégation spécifique :

(Par ordre de priorité)

- Le Directeur General Adjoint
- L'Ingénieur Sécurité & Sûreté
- Le Responsable du service Audit, Qualité, Procédures et Sécurité

- Pour les agents de sécurité externes :

A l'heure actuelle la SIDR n'a pas fait pas appel à un service de vidéo-surveillance externe, les images ne sont donc pas externalisées ni consultables à distance mais si le besoin de requérir à cette prestation était identifiée une consultation serait lancée pour retenir un opérateur ayant les agréments requis. Les agents de sécurité de cette structure pourraient avoir un accès aux images filmées en direct mais uniquement en mode visualisation sans possibilité d'effectuer des recherches ou des relectures.

Pour les locaux administratifs et accueillants du public :

Les enregistrements de vidéosurveillance sont uniquement accessibles au responsable du traitement des données et sur site, à savoir :

- Pour la SIDR le Directeur général de la SIDR ou par délégation spécifique :

(Par ordre de priorité)

- Le Directeur General Adjoint
- L'Ingénieur Sécurité & Sûreté
- Le Responsable du service Audit, Qualité, Procédures et Sécurité

- Pour chaque site accessible au public de la SIDR un effectif de 3 personnes est désigné afin de permettre une surveillance globale du site concerné.

(Par ordre de priorité)

- Le Responsable de site ou Responsable d'agence en fonction du local
- L'assistante du responsable de site ou personne désignée
- Le Gestionnaire de clientèle du site concerné

Ces personnes ont en charge la surveillance du site d'ont-ils dépendent pendant les heures d'ouverture au public. Pendant ces heures ils ont un accès aux images filmées en direct mais uniquement en mode visualisation sans possibilité d'effectuer des recherches ou des relectures.

Un bouton poussoir d'alerte permet en cas d'incident dans les zones d'accueils d'informer immédiatement la personne en charge de la surveillance.

A l'aide de la visualisation des images en direct la personne peut immédiatement faire appel aux forces de l'ordre et motiver la demande d'intervention.

- Pour les agents de sécurité externes :

A l'heure actuelle la SIDR n'a pas fait pas appel à un service de vidéo-surveillance externe, les images ne sont donc pas externalisées ni consultables à distance mais si le besoin de requérir à cette prestation était identifiée une consultation serait lancée pour retenir un opérateur ayant les agréments requis. Les agents de sécurité de cette structure pourraient avoir un accès aux images filmées en direct mais uniquement en mode visualisation sans possibilité d'effectuer des recherches ou des relectures.

5.2. Droits d'accès

La démarche globale de vidéosurveillance de la SIDR mentionne de façon claire et précise et nominative qui a accès aux images filmées ou à l'architecture technique du système de vidéosurveillance, dans quel but ces droits d'accès sont créés et en quoi ils consistent.

Ce document précise notamment qui est autorisé à :

- Visionner les images en temps réel ;
- Visionner les images enregistrées ;
- Copier le fichier image ;

- Télécharger ;
- Effacer ;
- Exporter les données,
- Effectuer la maintenance technique,

5.3. Formation et information du personnel à la protection des données

Toutes les personnes dotées de droits d'accès, (y compris les agents de sécurité externes si une externalisation devait être mise en place), ont reçu :

- Une information par le correspondant protection des données- SIDR à la protection des données,
- Une formation pour l'extraction des images et l'utilisation du logiciel de vidéosurveillance sera assurée par l'entreprise ayant réalisé l'installation.

En cas de modification des personnes ayant un accès la personne remplaçante aura obligatoirement reçu cette information avant la prise en charge de cette activité dans ses missions.

5.4. Engagement de confidentialité du personnel

À la fin de leur formation, toutes les personnes en charge de la vidéosurveillance SIDR ont signé un engagement de confidentialité (cet engagement fera partie intégrante du contrat de l'entreprise sous-traitante si une externalisation est mise en place).

Ces engagements sont :

- Inclus dans le registre générale vidéo- surveillance SIDR
- Annexe au contrat de travail des salariés concernés

5.5. Transfert, communication ou visualisation de données

La visualisation des données peut se faire :

- Par toute personne qui en a fait la demande (au Directeur Général de la SIDR) sous réserve que le demandeur soit effectivement la personne concernée par l'enregistrement ou le représentant légal de la personne filmée.

L'éventuel transfert ou communication de données ne peut se faire :

- Qu'aux forces de l'ordre ou à un représentant de l'état sur demande spécifique dans le cadre d'une enquête,
- Que par le Directeur Général de la SIDR, ou par délégation

Tout acte de visualisation de données par des tiers, de transfert ou de communication de données à des tiers doivent être motivées et faire l'objet d'une évaluation rigoureuse quant à leur nécessité et à la compatibilité de leurs finalités avec celles initialement poursuivies.

Ces actes de visualisation, transfert ou communications sont répertoriés consignés dans un registre tenu à jour par l'Ingénieur Sécurité & Sûreté de la SIDR.

L'identification de la personne qui a eu accès aux données est clairement renseignée et fait l'objet d'un émargement de cette dernière.

Le personnel de la Direction des Ressources Humaines ne dispose d'aucun droit d'accès aux données.

6. Comment est assurée la protection des données collectées ?

Afin d'assurer la sécurité du système de vidéosurveillance, et notamment celle des données à caractère personnel, un certain nombre de dispositions ont été prises sur les plans technique et organisationnel. Ces dispositions sont détaillées dans la politique générale de vidéosurveillance de la SIDR.

Quelques-unes des mesures mises en place sont :

- Les serveurs sur lesquels les images sont stockées se trouvent dans des locaux sécurisés, protégés par des dispositifs de sécurité physique ; des dispositifs pare-feu protègent le périmètre de l'infrastructure informatique. Enfin, les principaux systèmes informatiques qui renferment les données bénéficient de mesures de protection renforcées ;
- Les droits d'accès accordés aux utilisateurs leur permettent d'accéder uniquement aux ressources absolument indispensables à l'accomplissement de leurs tâches ;
- Seul l'administrateur du système, spécialement désigné à cet effet par le Directeur Générale de la SIDR, est en mesure d'accorder, de modifier ou d'annuler les droits d'accès d'une personne. Tout octroi, modification ou annulation de droits d'accès est régi par les critères établis au sein de la politique générale de sécurité en matière de vidéosurveillance vu ci-dessus.
- La politique générale de sécurité en matière de vidéosurveillance comporte une liste mise à jour de l'ensemble des personnes qui ont accès au système à tout moment et décrit en détail leurs droits d'accès.

7. Durée de conservation des données

Les images sont conservées pour une durée de 30 jours au maximum quel que soit la nature du local surveillé. Au-delà, les enregistrements sont systématiquement et automatiquement détruits.
Si nécessaire, seules les images pouvant être utilisées à des fins d'enquête ou de preuve suite à un incident de sécurité peuvent être conservées plus longtemps. Leur conservation est rigoureusement consignée et la nécessité de leur conservation est régulièrement réexaminée.

8. Information du public

8.1. Approche multicouche

Est mise en place à l'intention du public une information appropriée et exhaustive sur nos activités de vidéosurveillance. Cette information se fait selon une approche multicouche qui associe les mesures suivantes :

- L'installation sur place de panneaux d'information destinés à signaler au public la présence d'un dispositif de surveillance voir pour certains locaux spécifiques d'enregistrement sonore et à lui fournir des informations essentielles sur le traitement des données ;
- La publication de la présente politique de vidéosurveillance sur l'intranet SIDR ainsi que sur le site Web-SIDR à l'intention des personnes qui souhaiteraient en savoir plus sur les activités de vidéosurveillance de la SIDR ;
- La possibilité de consulter dans nos locaux d'accueil public une version papier de la politique générale de vidéosurveillance sur demande ;
- Une adresse mail : dpo@sidr.fr est mise à la disposition des personnes souhaitant obtenir des informations complémentaires ;
- Sont également installés des panneaux d'information à proximité des espaces surveillés, notamment près de l'entrée principale de chaque site, des accès secondaires, des accès aux parkings, des salles d'attentes et des bureaux d'encaissement ou d'accueil personnalisés.

8.2. Notifications individuelles

Outre les mesures précédentes, les personnes identifiées grâce aux caméras sont également informées individuellement dès lors qu'une ou plusieurs des conditions suivantes s'appliquent :

- Les images sont conservées au-delà de la durée normale de conservation ;
- Leur identité est mentionnée dans un fichier,
- Une action à leur encontre est engagée par la SIDR auprès des forces de l'ordre,

La communication de ces notifications peut être :

- Faite par les forces de l'ordre,
- Temporairement retardée, par exemple lorsqu'un délai est nécessaire à la prévention, à la recherche, à la détection ou à la poursuite d'infractions pénales

Une consultation systématique et immédiate du correspondant protection des données-SIDR est effectuée pour tous les cas de ce type afin de garantir le respect des droits de la personne concernée.

9. Accès du public aux données

Le public est en droit d'accéder aux données à caractère personnel le concernant qui se trouvent en possession de la SIDR afin de les faire rectifier ou effacer.
Les demandes d'accès à ces données pour toute rectification, blocage ou d'effacement sont à adresser par écrit au :

Directeur Général de la SIDR
SIDR 12 Rue Felix GUYON
A Saint Denis

La demande devra préciser :

- Le motif de la demande ;
- L'action souhaitée ;
- Le site ou l'enregistrement a été effectué ;
- L'heure ou l'enregistrement a été effectué.

Chaque demande fera l'objet d'une analyse et d'une recherche de correspondance entre la prise de vue et l'identité du demandeur.
Seule les demandes qui ne sont pas en lien avec un méfaits pourrons être rectifiées ou effacées.

10. Droit de recours

Si elle estime que les droits qui lui sont reconnus par le règlement (CE) n° 45/2001 ont été violés consécutivement au traitement par la SIDR de données à caractère personnel la concernant, toute personne a le droit de saisir la CNIL
(**C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés https://www.cnil.fr)

Avant d'engager une telle procédure, nous conseillons aux personnes souhaitant déposer un recours de contacter :

Le Correspondant de la Protection des Données de la SIDR
SIDR 12 Rue Felix GUYON
A Saint Denis

Toute personne concernée peut obtenir, selon l'article 14 du règlement, un droit de rectifications de données dans le cas où celles-ci la concernant seraient erronées en s'adressant au Correspondant Informatique et Liberté de la SIDR (le Correspondant Protection des Données de la SIDR) :
Après vérification des données, le Correspondant Protection des Données de la SIDR apportera les modifications adéquates et ce dans un délai de quinze jours après demande de rectifications.

Dans le cas d'une demande d'effacement, une consultation du Correspondant Protection des Données de la SIDR sera effectuée par le **Directeur Général de la SIDR.** Dès réception de l'avis du Correspondant Protection des Données de la SIDR, confirmant la nécessité d'effacement des données, ces dernières seront effacées dans les 72 h qui suivent.

Jacques DURAND

Directeur Général