

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'ENVIRONNEMENT, DE L'ÉNERGIE ET DE LA MER, EN CHARGE DES RELATIONS INTERNATIONALES SUR LE CLIMAT

Arrêté du 6 juin 2016 relatif à la mise en œuvre de systèmes de vidéosurveillance et à la création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès à certains locaux des ministères de l'environnement, de l'énergie et de la mer, du logement et de l'habitat durable

NOR : DEVK1615340A

La ministre de l'environnement, de l'énergie et de la mer, chargée des relations internationales sur le climat, et la ministre du logement et de l'habitat durable,

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment les I, 1° et IV de l'article 26 ;

Vu la délibération n° 2016-168 du 26 mai 2016 de la Commission nationale de l'informatique et des libertés,

Arrêtent :

Art. 1^{er}. – Le ministère de l'environnement, de l'énergie et de la mer, en charge des relations internationales sur le climat, et le ministère du logement et de l'habitat durable sont autorisés à mettre en œuvre les traitements de données à caractère personnel définis ci-après et mis en place au sein des locaux des services et établissements publics des ministères non ouverts au public présentant des risques particuliers en matière de sécurité. Ils visent, notamment, les zones et locaux abritant le système d'information ISIS (messagerie et portail étatique de niveau confidentiel défense) ou abritant des biens équivalents. Il est prévu que ces traitements puissent être mis en œuvre au sein de centres serveurs, d'un point d'importance vitale ou encore d'une zone de haute sécurité.

Ces traitements ont pour finalités d'assurer la protection des locaux mentionnés au premier alinéa en contrôlant leur accès au moyen de dispositifs d'authentification des personnes, de détecteurs d'intrusion et de l'emploi de caméras de vidéosurveillance.

Le contrôle d'accès et la vidéosurveillance peuvent être mis en œuvre de manière dissociée ou intégrée. Néanmoins, ne peuvent être filmés les lieux d'intimité (toilettes, vestiaires, salles de repos, etc.), ceux destinés aux activités syndicales ainsi que leurs accès et les endroits dans lesquels peuvent se tenir des échanges couverts par le secret professionnel.

Art. 2. – I. – Les données à caractère personnel et informations enregistrées dans les traitements mentionnés à l'article 1^{er} sont les suivantes :

- 1° Nom et prénoms, date et lieu de naissance ;
- 2° Nom de l'agent chargé de la délivrance des droits d'accès ;
- 3° Données relatives aux entrées et sorties ;
- 4° Date d'établissement, période de validité, niveau et numéro d'enregistrement de l'autorisation d'accès ;
- 5° Zones d'accès et points d'entrée et de sortie autorisés ;
- 6° Données relatives aux incidents, liés notamment au non-respect d'une interdiction d'accès ou à une tentative d'intrusion ;
- 7° Photographie d'identité ;
- 8° Images capturées par le dispositif de vidéosurveillance.

II. – Outre les données mentionnées au 1°, sont également enregistrées dans les traitements mentionnés à l'article 1^{er} les données suivantes :

1° Concernant les agents des ministères et des établissements publics mentionnés à l'article 1^{er} : sexe, nationalité, numéro d'identification, adresse professionnelle, matricule, grade ou qualité, fonction et service d'affectation ;

2° Concernant les prestataires habilités : sexe, nationalité, type de prestation, nom et adresse de la société d'emploi, direction donneuse d'ordre ;

3° Concernant les visiteurs : motif de la visite ; nom de la personne visitée et service d'affectation.

III. – Les contrôles d'accès par reconnaissance faciale sont interdits.

La captation du son et son enregistrement, dans le cadre des dispositifs mis en œuvre, ne sont pas autorisés en heures ouvrées.

Art. 3. – I. – Dans la limite de leurs attributions respectives et de leurs besoins d'en connaître, ont seuls accès aux données mentionnées à l'article 2 :

1° Les agents, spécialement désignés et individuellement habilités par le responsable des locaux ou le chef d'établissement, chargés de la sécurité et de la surveillance du lieu concerné ;

2° Le responsable des locaux ou le chef d'établissement au sein duquel les traitements sont mis en œuvre.

II. – Seuls les agents spécialement désignés et individuellement habilités par le responsable des locaux ou le chef d'établissement peuvent, *a posteriori*, rechercher et extraire des images ou des informations des systèmes de vidéosurveillance et de contrôle d'accès.

III. – Dans la limite de leurs attributions respectives et de leur besoin d'en connaître, peuvent être destinataires de tout ou partie des données enregistrées dans les traitements :

1° Le chef de service ou son représentant ;

2° Les personnes habilitées du service en charge de la discipline ;

3° Les agents des corps et services d'inspection et de contrôle relevant des ministères.

Art. 4. – Les opérations de recherche et d'extraction des données, effectuées par les agents mentionnés au II de l'article 3 du présent arrêté, font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et l'heure de la consultation et de l'extraction. Cet enregistrement est conservé pendant une durée d'un an.

Art. 5. – Les éléments d'identification, notamment liés aux déplacements des agents, des prestataires et des visiteurs, sont conservés, à compter de la fin de validité de l'autorisation d'accès :

– pour les agents et les prestataires, un an au plus ;

– pour les visiteurs, trois mois au plus.

Les éléments relatifs au déplacement des personnes sont conservés trois mois au plus.

Les images enregistrées par les caméras sont conservées pendant un délai ne pouvant excéder trente jours. Au terme de ce délai, les enregistrements qui n'ont fait l'objet d'aucune transmission à l'autorité judiciaire ou poursuite disciplinaire sont effacés.

Art. 6. – Le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 susvisée ne s'applique pas aux traitements autorisés par le présent arrêté.

Art. 7. – Les droits d'accès et de rectification prévus aux articles 39, 40 et au dernier alinéa de l'article 41 de la même loi s'exercent directement auprès du service gestionnaire du traitement.

Art. 8. – La mise en œuvre des traitements mentionnés à l'article 1^{er} est précédée de l'envoi à la Commission nationale de l'informatique et des libertés d'un engagement de conformité au présent arrêté.

Une copie de cet engagement de conformité est communiquée au fonctionnaire de la sécurité des systèmes d'information.

Un dossier technique décrivant le dispositif mis en place est établi et conservé avec la déclaration d'engagement. Les éléments constitutifs de ce dossier technique sont présentés dans l'annexe attachée au présent arrêté.

Ces documents sont tenus à la disposition de la Commission nationale de l'informatique et des libertés.

Art. 9. – Ces traitements sont mis en œuvre après avis des comités compétents en matière d'hygiène, de sécurité et des conditions de travail.

Les personnes susceptibles d'être filmées sont informées de l'existence d'un système de vidéosurveillance et des modalités d'accès aux images les concernant par affiches apposées à l'entrée des locaux présentant des risques particuliers pour la sécurité. La captation du son et son enregistrement, dans le cadre des dispositifs mis en œuvre, ne sont pas autorisés en heures ouvrées.

Art. 10. – Le vice-président du Conseil général de l'environnement et du développement durable, le secrétaire général des ministères, la commissaire générale au développement durable, les directeurs généraux et directeurs d'administration centrale, les directeurs des services déconcentrés, les directeurs des services techniques et à compétence nationale et les directeurs des établissements publics relevant des deux ministères visés à l'article 1^{er} sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel* de la République française.

Fait le 6 juin 2016.

*La ministre de l'environnement,
de l'énergie et de la mer,
chargée des relations internationales
sur le climat,*

Pour la ministre et par délégation :

*Le secrétaire général,
haut fonctionnaire de défense
et de sécurité,*

F. ROL-TANGUY

*La ministre du logement,
et de l'habitat durable,*

Pour la ministre et par délégation :

*Le secrétaire général,
haut fonctionnaire de défense
et de sécurité,*

F. ROL-TANGUY

ANNEXE

Annexe à l'arrêté relatif à la mise en œuvre de systèmes de vidéosurveillance et à la création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès à certains locaux des ministères de l'environnement, de l'énergie et de la mer, du logement et de l'habitat durable et à ses établissements publics.

(Articles 26 et 27 de la loi n° 78-17 du 6 janvier 1978 modifiée en 2004)

* Champs obligatoires

1 Déclarant

(à remplir)

Nom et prénom ou raison sociale* :	Sigle (facultatif)
Service :	N° SIRET* :
Adresse* :	N° SIREN Code établissement
Code postal* Ville*	Code APE* : _____
Adresse électronique* :	Téléphone* :
	Fax :

Personne à contacter au sein de l'organisme déclarant si un complément d'information doit être demandé et destinataire de l'avis :

Nom et prénom* :
Adresse électronique* :

2 Service chargé de la mise en oeuvre du traitement (lieu d'implantation)

(à remplir)

(Veuillez préciser quel est le service ou l'organisme qui effectue, en pratique, le traitement)

☐ Il s'agit du déclarant lui-même

☐ Le traitement est assuré par un tiers (prestataires, sous-traitant) ou un service différent du déclarant, veuillez compléter le tableau ci-dessous :

Nom et prénom ou raison sociale* :	Sigle (facultatif)
Service :	N° SIRET* :
Adresse* :	N° SIREN Code établissement
Code postal* Ville*	Code APE* : _____
Adresse électronique* :	Téléphone* :
	Fax :

3 Finalité du traitement (objectif(s) du traitement)*(point 5 et 7 à compléter)***1) La finalité du traitement :***

- ☐ Mise à disposition des usagers d'un ou plusieurs téléservices de l'administration électronique
- ☒ Sûreté de l'Etat, défense, sécurité publique
- ☐ Prévention, recherche, constatation ou poursuite des infractions pénales ou exécution des condamnations pénales ou des mesures de sûreté
- ☐ Authentification ou contrôle de l'identité des personnes par un dispositif biométrique
- ☐ Vérification des identités par consultation du RNIPP
- ☐ Recensement de la population en métropole et dans les collectivités d'outre-mer
- ☐ Autre, précisez (exemple : déterminer les conditions d'ouverture d'un droit par interconnexion avec utilisation du NIR):

2) Quel est l'objectif précis de votre traitement (exemple : mise en oeuvre d'une plate-forme internet destinée à permettre aux usagers d'accomplir des démarches administratives en ligne) ?*

L'objectif du traitement est de satisfaire les finalités exprimés à l'article 1 de l'arrêté en référence.

3) Veuillez préciser le fondement juridique du traitement ?

Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment les I, 1° et IV de l'article 26;

L'arrêté relatif à la mise en oeuvre de systèmes de vidéosurveillance et à la création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès à certains locaux des ministères de l'environnement, de l'énergie et de la mer, du logement et de l'habitat durable.

4) Les personnes peuvent-elles s'opposer à figurer dans ce traitement ?* ☐ Oui ☒ Non

NB : Si vous cochez « Non », cela signifie que le traitement est obligatoire et cela doit avoir été prévu par un texte législatif ou réglementaire

5) Nom et descriptif sommaire du logiciel ou de l'application utilisé(e)?**6) Quelles sont les personnes concernées par le traitement ?***

- ☒ Salariés ☐ Usagers Adhérents ☐ Clients (actuels ou potentiels) ☒ Visiteurs
- ☐ Patients ☐ Etudiants/élèves
- ☒ Autres (veuillez préciser) : stagiaires, vacataires et prestataires

(3- Finalité du traitement– suite)**7) Si vous utilisez une technologie particulière, merci de préciser laquelle :**

- ☐ Dispositif sans contact (ex. : RFID, NFC) ☐ Mécanisme d'anonymisation
☐ Carte à puce ☐ Géolocalisation (ex.: GPS couplé avec GSM/GPRS)
☐ Vidéosurveillance (hormis dispositif de reconnaissance faciale)
☐ Nanotechnologie

Autres (précisez) : capteurs, sondes, dispositifs anti-intrusion pour remontée d'alerte

4 Transfert de données hors de l'UE**(pré-rempli)*

Transmettez-vous tout ou partie des données traitées vers un pays situé hors de l'Union européenne et n'assurant pas un niveau de protection suffisant ? : ☒ Non ☐ Oui

! Si oui, merci de compléter l'annexe "Transfert de données hors de l'Union européenne" !

5 Données traitées*(tableau pré-rempli au regard des dispositions de l'arrêté de référence)*

Catégories de données	Détail (veuillez préciser ici le détail des données traitées)	Origine (comment avez vous collecté ces données ?)	Durée de conservation (combien de temps conserverez-vous les données sur support informatique ?)	Destinataires (veuillez indiquer les organismes auxquels vous transmettez les données)
<input checked="" type="checkbox"/> Etat civil, Identité, Données d'identification	<input checked="" type="checkbox"/> Nom, prénom <input checked="" type="checkbox"/> Adresse <input checked="" type="checkbox"/> Photographie <input checked="" type="checkbox"/> Date, lieu de naissance <input type="checkbox"/> Autres, précisez :	<input checked="" type="checkbox"/> Directement auprès de la personne concernée <input checked="" type="checkbox"/> De manière indirecte, précisez : Service des ressources humaines ou du responsable de sécurité	__ __ jours __ __ mois __ __ années <input checked="" type="checkbox"/> Autre, précisez : Agents et prestataires : 1 an au plus; Autres : 3 mois.	Destinataires :
<input type="checkbox"/> Vie personnelle	<input type="checkbox"/> Habitude de vie <input type="checkbox"/> Situation familiale <input type="checkbox"/> Autres, précisez :	<input type="checkbox"/> Directement auprès de la personne concernée <input type="checkbox"/> De manière indirecte, précisez :	__ __ jours __ __ mois __ __ années <input type="checkbox"/> Autre, précisez :	Destinataires :

(5 - Données traitées – suite)

Catégories de données	Détail (veuillez préciser ici le détail des données traitées)	Origine (comment avez vous collecté ces données ?)	Durée de conservation (combien de temps conserverez-vous les données sur support informatique ?)	Destinataires (veuillez indiquer les organismes auxquels vous transmettez les données)
<input checked="" type="checkbox"/> Vie professionnelle	<input type="checkbox"/> CV <input checked="" type="checkbox"/> Situation professionnelle <input type="checkbox"/> Scolarité, formation <input type="checkbox"/> Distinction <input type="checkbox"/> Autres, précisez :	<input checked="" type="checkbox"/> Directement auprès de la personne concernée <input checked="" type="checkbox"/> De manière indirecte, précisez : Service des ressources humaines et profil d'emploi pour le classifié	-- jours -- mois -- années <input checked="" type="checkbox"/> Autre, précisez : Agents et prestataires : 1 an au plus; Autres : 3 mois.	Destinataires :
<input type="checkbox"/> Informations d'ordre économique et financier	<input type="checkbox"/> Revenus <input type="checkbox"/> Situation financière (ex : taux d'endettement) <input type="checkbox"/> Autres, précisez :	<input type="checkbox"/> Directement auprès de la personne concernée <input type="checkbox"/> De manière indirecte, précisez :	-- jours -- mois -- années <input type="checkbox"/> Autre, précisez :	Destinataires :
<input checked="" type="checkbox"/> Données de connexion (adresse IP, logs, etc.)	<input checked="" type="checkbox"/> Identifiants des terminaux <input checked="" type="checkbox"/> Identifiants de connexions <input checked="" type="checkbox"/> Information d'horodatage Autres, précisez :	<input type="checkbox"/> Directement auprès de la personne concernée <input checked="" type="checkbox"/> De manière indirecte, précisez : Architecture technique, badges ou autres moyens	30 jours -- mois -- années Autre, précisez :	Destinataires :

5 - Données traitées – suite)

Catégories de données	Détail (veuillez préciser ici le détail des données traitées)	Origine (comment avez vous collecté ces données ?)	Durée de conservation (combien de temps conserverez-vous les données sur support informatique ?)	Destinataires (veuillez indiquer les organismes auxquels vous transmettez les données)
<input type="checkbox"/> Données de localisation (déplacements, données GPS, GSM, etc.)	<input type="checkbox"/> Par satellite <input type="checkbox"/> Par le téléphone mobile <input type="checkbox"/> Autres, précisez :	<input type="checkbox"/> Directement auprès de la personne concernée De manière indirecte, précisez :	-- jours -- mois -- années Autre, précisez :	Destinataires :

6 Données sensibles

(sans objet dans le cadre de l'arrêté de référence)

Ce chapitre est détaillé par la CNIL et est rappelé à titre informatif. Ces informations particulièrement sensibles font l'objet d'une déclaration spécifique hors du champ de l'arrêté.

Catégories de données	
<input type="checkbox"/> N° de sécurité sociale (NIR) <input type="checkbox"/> Données biométriques <input type="checkbox"/> Données génétiques (ADN)	<input type="checkbox"/> Infractions, condamnations, mesures de sûreté <input type="checkbox"/> Appréciation sur les difficultés sociales des personnes <input type="checkbox"/> Données de santé

7 Interconnexions*

(à remplir)

Procédez-vous à des interconnexions de fichiers (échange de données entre fichiers) ayant des finalités différentes ou poursuivant un intérêt public différent ? ☐ Non ☐ Oui

Si oui, veuillez compléter le tableau ci-dessous en apportant des précisions sur les fichiers que vous interconnectez :

	Organisme responsable Veuillez préciser ses coordonnées	Finalité Veuillez indiquer la finalité du fichier concerné	N° de déclaration à la CNIL (le cas échéant)
Fichier n°1			
Fichier n°2			

Etc. (à compléter le cas échéant)			

Veillez détailler les raisons pour lesquelles vous effectuez cette interconnexion et indiquez, le cas échéant, si cette interconnexion est prévue par un texte législatif ou réglementaire (si oui, précisez lequel) :

8 Le droit d'accès des personnes fichées

(à remplir)

Le droit d'accès est le droit reconnu à toute personne d'interroger le responsable d'un traitement pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication. Cf. article 32 de la loi et modèles de mentions d'information dans la notice

Comment informez-vous les personnes concernées par votre traitement de leur droit d'accès ?*

- ☐ Mentions légales sur formulaire ☐ Affichage
- ☐ Mentions sur site internet ☐ Envoi d'un courrier personnalisé
- ☐ Autres mesures (précisez) :

Veillez indiquer les coordonnées du service chargé de répondre aux demandes de droit d'accès :

- ☐ Il s'agit du déclarant lui-même
- ☐ Le traitement est assuré par un tiers (prestataires, sous-traitant) ou un service différent du déclarant, veuillez compléter le tableau ci-dessous :

Nom et prénom ou raison sociale* :	Sigle (facultatif)
Service :	N° SIRET*:
Adresse* :	N° SIREN _____ Code établissement _____
Code postal* Ville*	Code APE*: _____
Adresse électronique (facultatif) :	Téléphone* :
	Fax :

9 Sécurité et architecture informatique

(à remplir)

1) Nom(s) du (des) système(s) d'exploitation impliqués dans le traitement***2) Le système informatique est constitué :***

- ☐ De micro-ordinateurs (fixes ou nomades), terminaux, téléphones ou PDA. Veuillez préciser :
 - Leur nombre :
 - Leur type :
- ☐ D'un ou plusieurs serveur(s). Précisez s'ils sont :
 - ☐ Au sein de l'organisme
 - ☐ Externalisé(s)
- ☐ Autre architecture informatique :

3) Le logiciel d'application met en oeuvre :

- ☐ Une base de données. Nom :
- ☐ Un infocentre. Nom :
- ☐ Un logiciel d'analyse de données permettant d'effectuer des statistiques
- ☐ Autre :

(9 - Sécurité et architecture informatique – suite)**4) Nature du (ou des) réseau(x) informatique(s) de l'organisme utilisé(s) pour le traitement***

- ☐ Aucun réseau (par ex. élément autonome ou micro-ordinateur isolé)
- ☐ Un ou plusieurs réseaux sur un même site
- ☐ Plusieurs réseaux distants interconnectés
 - Mécanisme d'interconnexion (ex : VPN, Ligne spécialisée) :
- ☐ Un ou plusieurs réseaux externalisés chez un prestataire
 - ☐ Communications avec l'extérieur (ex : Internet)
 - ☐ Utilisation de technologies sans fil (ex : WiFi)
- ☐ Autre type de réseau :

5) Si le traitement implique des échanges avec des utilisateurs, un hébergeur ou des tiers externes (organismes, partenaires, clients, ...) y compris à l'étranger

Veuillez préciser les entités concernées par ces échanges :

- ☐ Echanges sur Internet (Web y compris par portail, Transfert de fichier, Email, etc.). Précisez les protocoles et les mécanismes cryptographiques mis en oeuvre :
- ☐ Echanges sur un réseau privé. Type d'interconnexion (ex: VPN, LS) :
- ☐ Transfert de supports numériques ou analogiques (disque, bande, cd-rom, clé USB,...)
 - Type de support et mécanismes cryptographiques :
- ☐ Autre(s) procédé(s) :

6) Sécurité physique des locaux et des équipements*

Veuillez décrire la sécurité des locaux et équipements hébergeant le traitement (ex. clés, badge d'accès, gardiennage) :

7) Sauvegarde*

- ☐ Des mesures assurent la sauvegarde du système informatique. Veuillez décrire :
 - Le type de support :
 - La fréquence des sauvegardes :
 - La sécurité physique du lieu de stockage des supports :
 - Les mécanismes cryptographiques (du stockage et/ou du transport) utilisés :
- ☐ La sauvegarde est externalisée. Nom de l'hébergeur :

8) Protection contre les intrusions :*

- ☐ Un antivirus est installé sur tous les postes prenant part au traitement
- ☐ Un système de détection d'intrusion (IDS) est utilisé. Nom :
- ☐ Une compartimentation du réseau avec des règles de filtrage est effectuée (ex. DMZ, firewall)
- ☐ Le traitement est confiné dans un ou plusieurs réseaux isolés des autres traitements (ex. VLAN)
- ☐ Autre procédé :

9) Mesures pour assurer la confidentialité des données lors du développement de l'application informatique*

- ☐ Les environnements de développement et de production sont distincts
- ☐ Les personnels affectés aux tâches de développement et de gestion/exploitation sont distincts
- ☐ La mise au point des logiciels s'effectue sur des données anonymisées fictives
 - ☐ anonymisées
 - ☐ fictives
- ☐ Autres mesures :

10) Mesures pour assurer la confidentialité des données lors des opérations de maintenance des logiciels ou des équipements*

- ☐ Les interventions de maintenance sont enregistrées dans une main-courante
- ☐ Les logiciels ou équipements informatiques font l'objet d'une télémaintenance
 - Mesures de sécurité appliquées lors de ces opérations :
 - Procédure particulière si la télémaintenance nécessite un accès aux fichiers de données à caractère personnel :
- ☐ La maintenance des matériels par un sous-traitant est faite en présence d'un informaticien de l'entreprise
- ☐ Les supports de stockage envoyés à l'extérieur pour réparation font l'objet d'une procédure de protection. Précisez :
- ☐ Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière. Précisez :

11) Authentification/identification des personnes habilitées à accéder à l'application :*

- ☐ Des profils d'habilitation définissent les fonctions ou les types d'informations accessibles à un utilisateur
- ☐ Le contrôle d'accès logique se fait
- ☐ par un mot de passe. Quelles sont ses caractéristiques (structure obligatoire, durée de validité, etc.) ?
 - ☐ par un dispositif matériel non-biométrique (ex. carte à puce). Précisez son nom et s'il est complété par la saisie d'un code secret ou PIN :
 - ☒ par un dispositif biométrique. Précisez lequel :
 - ☐ au moyen de certificats logiciels « client »
 - ☐ par un autre mécanisme. Précisez lequel :
- ☐ Décrivez brièvement la procédure de distribution des moyens de contrôle d'accès aux personnes habilitées :

12) Certaines données font l'objet d'une journalisation :

Accès à l'application	Accès aux fichiers de données à caractère personnel
<input type="checkbox"/> date/heure de connexion	<input type="checkbox"/> date/heure de connexion
<input type="checkbox"/> identifiant du poste de travail	<input type="checkbox"/> identifiant du poste de travail
<input type="checkbox"/> identifiant de l'utilisateur	<input type="checkbox"/> identifiant de l'utilisateur
<input type="checkbox"/> date/heure de déconnexion	<input type="checkbox"/> la référence des données accédées
<input type="checkbox"/> opération effectuée	<input type="checkbox"/> autres informations journalisées :
<input type="checkbox"/> autres informations journalisées :	Type d'accès journalisés, pour : <input type="checkbox"/> Consultation <input type="checkbox"/> Création <input type="checkbox"/> Mise à jour <input type="checkbox"/> Suppression <input type="checkbox"/> Autre :

13) Confidentialité/intégrité. L'application met en oeuvre des procédés :

- ☐ D'anonymisation des données. Nom du procédé :
- ☐ De chiffrement des données à caractère personnel stockées
- Algorithme (par ex. 3DES) :
 - Longueur de la clé :
- ☐ De contrôle d'intégrité des données à caractère personnel stockées
- Algorithme (par ex. 3DES) :
 - Longueur de la clé :
- ☐ De sécurisation du transport des données à caractère personnel
- Protocole de sécurisation (par ex. SSLv3) :
- ☐ D'authentification destinataire ou « serveur » (signature électronique, certificat,...)

- Procédé et nom commercial :
- ☐ D'authentification émetteur ou « client » (signature électronique, certificat,...)
 - Procédé et nom commercial :

10 Personne à contacter

(à remplir)

Veillez indiquer ici les coordonnées de la personne qui a complété ce questionnaire au sein de votre organisme et qui répondra aux éventuelles demandes de compléments que la CNIL pourrait être amenée à formuler

Nom et prénom ou raison sociale* :	Sigle (facultatif)
Service :	N° SIRET* :
Adresse* :	N° SIREN ----- Code établissement
Code postal* Ville*	Code APE* : -----
Adresse électronique* :	Téléphone* :
	Fax :

11 Signature du responsable

(à remplir)

Je m'engage à ce que le traitement décrit par ce dossier technique respecte les exigences de la loi du 6 janvier 1978 modifiée et les dispositions de l'arrêté relatif à la mise en œuvre de systèmes de vidéosurveillance et à la création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès à certains locaux des ministères de l'environnement, de l'énergie et de la mer, du logement et de l'habitat durable.

Personne responsable de l'organisme déclarant :

Nom et prénom*	Date* :
Fonction :	Signature
Adresse électronique pour l'envoi de l'avis* :	

Ce dossier technique a vocation à être conservé et à accompagner la déclaration d'engagement de conformité faite par l'entité auprès de la Commission nationale de l'informatique et des libertés (CNIL). Ces deux documents devront être mis à disposition de la CNIL dès lors que celle-ci en fera la demande.