

RAPPORT DE DIAGNOSTIC
Conformité RGPD

Application – HéliSMUR

INEA

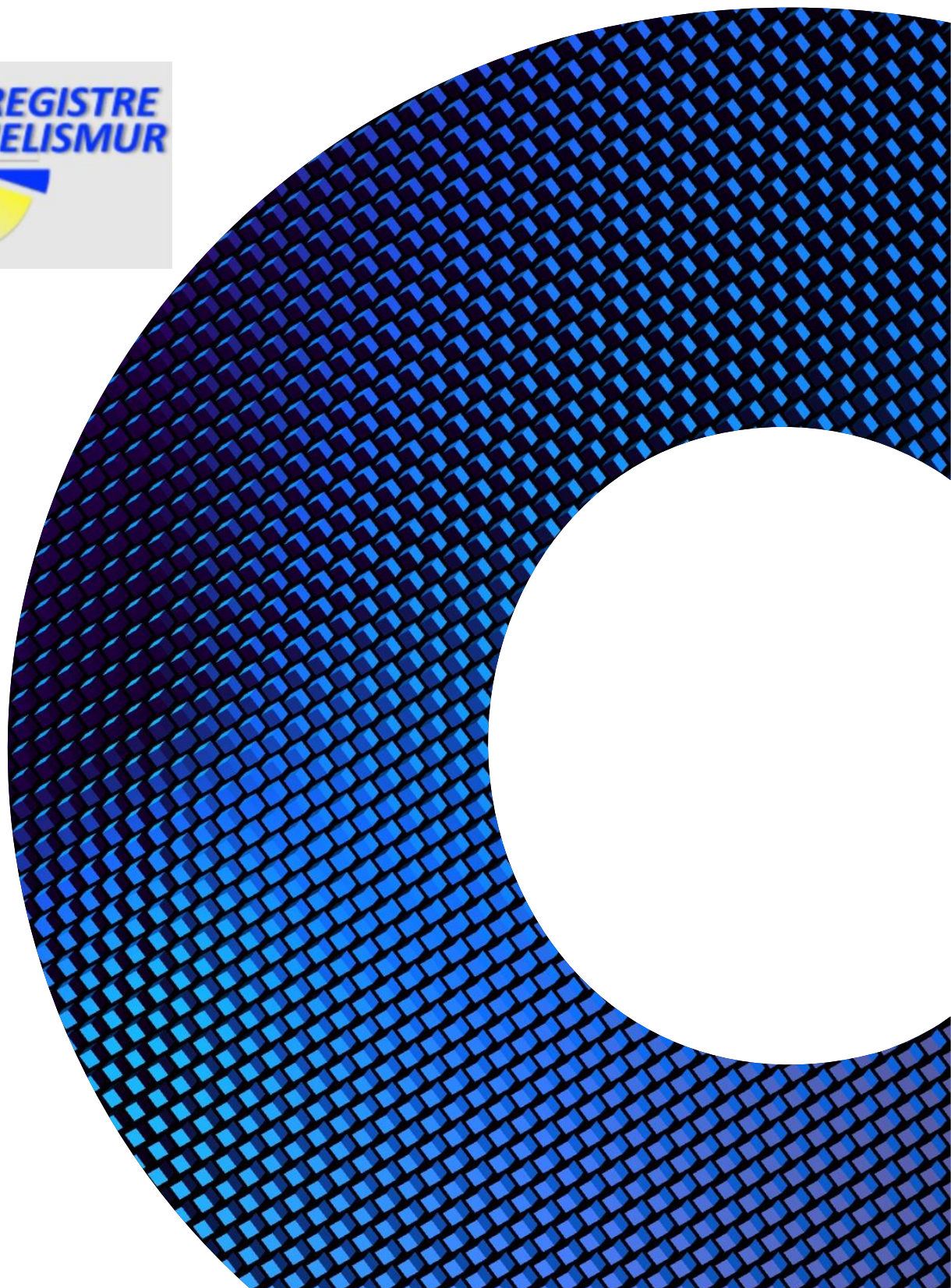


Table des matières

TABLE DES MATIERES.....	2
I- INTRODUCTION.....	4
A- Présentation de l'application	4
B- Contexte de la mission	4
C- Organisation des ateliers du diagnostic	5
Atelier n°1.....	5
Atelier n°2.....	6
Atelier n°3.....	6
Atelier n°4.....	7
II- METHODOLOGIE DU DIAGNOSTIC.....	7
A- Traitements de données	7
Les traitements listés ci-dessous ont été identifiés sur la base des informations fournies lors des différents ateliers menés avec nos interlocuteurs. Ils ne sont donc pas exhaustifs et ne peuvent remplacer le registre de traitements qui doit être mis en place par l'organisme responsable des traitements.	
Traitement n°1 :	8
Traitement n°2 :	8
Traitement n°3 :	8
Traitement n°4 :	9
Traitement n°5 :	9
Traitement n°6 :	9
B- Points de conformités identifiés	10
1- Vérification de la licéité des traitements et limitation de leur finalité	11
2- Information des personnes concernées	12
3- Minimisation des données	13
4- Mise en place des mesures de sécurité des données	14
5- Définition des durées de conservation et d'archivage	15
6- Documentation de la conformité (Accountability)	17
7- Respect des principes de Privacy by design / Privacy by default	18
8- Implication du DPO et moyens mis à sa disposition	20

9- Respect des droits des personnes	22
10- Réalisation des analyses d'impact relatives à la protection des données (AIPD)	24
11- Transmission auprès des différents destinataires	26
12- Encadrement des transferts de données en dehors de l'UE	28
C- Evaluation des vidéos visualisées (les vidéoprotections des sites)	29

Version du document :	Version 1.0 du 11/12/2024
Réunion de restitution :	19/12/2024
Auteurs :	Houssini M. BOUKARI - Associate Onepoint h.boukari@groupeonepoint.com

I- INTRODUCTION

A- Présentation de l'application

Créé en 2015, le registre HéliSMUR est un outil cartographique qui permet à la régulation des SAMU de gérer les missions d'urgence hélicoptérées, grâce à un répertoire des zones de posées et la géolocalisation de tous les hélicoptères (y compris les opérateurs privés et de sécurité civile). Il comprend aussi des outils d'aide à la décision pour optimiser l'organisation des transports hélicoptérés.

Grâce à sa base de données, le registre HéliSMUR permet par ailleurs une exploitation statistique et une analyse de l'activité (part de vols primaires, gravité des patients pris en charge, mapping dynamique...)

La période COVID a été l'occasion de tester l'application pour le suivi des évacuations sanitaires en France et en transfrontalier, en affichant notamment les hélicoptères allemands. C'est un outil accessible à tous les SAMU, l'activité hélicoptérée ne s'arrêtant pas aux frontières d'une région.

B- Contexte de la mission

Le projet est celui d'un registre des missions HéliSMUR, avec des données Médicales, organisationnelles, aéronautiques, géographiques. L'analyse de ces données devrait permettre de comprendre l'activité HéliSMUR en termes d'organisation, de processus décisionnels et de pathologies. L'utilisation d'une interface permettant d'incrémenter le registre est nécessaire. La meilleure façon de recueillir les données étant la saisie « dans l'instant » (pendant le temps de gestion de la mission), l'outil idéal pour gérer les missions hélico et incrémenter une base de données à visée statistique, est bien sûr un logiciel de régulation.

En l'absence d'harmonisation des logiciels de régulation médicale, une proposition d'utiliser une plateforme web collaborative, utilisable par toutes les régulations d'un territoire donné (région, zone de défense), pour gérer les missions HéliSMUR et incrémenter une base de données commune, a été faite. Le projet est donc un module d'aide à la régulation permettant d'incrémenter un registre.

Soucieux de la conformité de l'application, INEA souhaite au préalable s'assurer de la protection des données qui sont traitées en dressant dans un premier temps un état des lieux sur les **traitements existants**, puis dans un second temps élaborer un plan d'action à mettre en œuvre pour une meilleure prise en compte du RGPD dans le projet.

C'est donc dans cette optique que onepoint est missionné pour établir un diagnostic de **la conformité des traitements** effectués via HéliSMUR et élaborer un plan d'action associé. Nous avons reçu pour mission, d'analyser les écarts de conformité des traitements et de définir les actions correctives relatives au règlement général sur la protection des données.

L'exhaustivité du diagnostic réalisé, dépend donc directement de l'exhaustivité des documents transmis, ainsi que du contenu des échanges eu au cours des ateliers.

C- Organisation des ateliers du diagnostic

Des ateliers ont été menés avec les personnes clés du projet pour le périmètre de l'étude. Ils ont permis d'évaluer le niveau de maturité de la protection des données à caractère personnel.

Ci-dessous la liste des ateliers effectués et des sujets abordés.

Atelier n°1

Date de l'entretien :	05/11/2024	Durée :	1h30	
	Prénom NOM	Fonction	Adresse électronique	
Présents :	Houssini M. BOUKARI	Consultant RGPD	h.boukari@groupeonepoint.com	
	Djamel ZITOUNI	Spécialiste de modélisation – informaticien théoricien	djamel.zitouni@univ-lille.fr	
Les sujets abordés				
• Les données collectées • Les traitements de données • Les logiciels installés (les applications de régulation) • Les intervenants sur la partie conception des modules • La consultation des images via les webcams (les webservice)				

Atelier n°2

Date de l'entretien :	15/11/2024	Durée :	45 minutes
	Prénom NOM	Fonction	Adresse électronique
Présents :	Houssini M. BOUKARI	Consultant RGPD	h.boukari@groupeonepoint.com
	Djamel ZITOUNI	Spécialiste de modélisation – informaticien théoricien	djamel.zitouni@univ-lille.fr
Les sujets abordés			
• Les données collectées (approfondissement) • Les traitements de données (validation des traitements identifiés précédemment) • Mode d'accès des applications de régulation • Les sources de collecte de données • Les mentions d'informations • La base juridique du traitement de données à des fins de recherche			

Atelier n°3

Date de l'entretien :	28/11/2024	Durée :	45 minutes
	Prénom NOM	Fonction	Adresse électronique
Présents :	Houssini M. BOUKARI	Consultant RGPD	h.boukari@groupeonepoint.com
	Djamel ZITOUNI	Spécialiste de modélisation – informaticien théoricien	djamel.zitouni@univ-lille.fr

Thématiques abordées
• Identification du responsable des traitements • Les destinataires des données et du registre • Les services chargés de l'enregistrement des données

Atelier n°4

Date de l'entretien :	06/12/2024	Durée :	1h
	Prénom NOM	Fonction	Adresse électronique
Présents :	Houssini M. BOUKARI	Consultant RGPD	h.boukari@groupeonepoint.com
	Coralie ACHARD-TORTUL	Juriste droit du numérique - DPO	dpo@esante-hdf.fr
	Ismaël SALAH	Chef de Projets	ismael.salah@esante-hdf.fr
Thématiques abordées			
• Identification du responsable des traitements • Identification des cas de sous-traitances			

II- Méthodologie du diagnostic

Dans le cadre de la réalisation du diagnostic de conformité, onepoint s'est dotée d'une démarche adaptée au contexte du projet (registre HéliSMUR).

Cette démarche consiste à identifier les données manipulées et les traitements associés, retracer leur cycle de vie (collecte, conservation, destination) et ainsi, évaluer le niveau de conformité global de l'application tout en prenant en compte les points de non-conformité. Ceci, afin d'identifier et de prioriser les recommandations de mise en conformité.

A- Traitements de données

Les traitements listés ci-dessous ont été identifiés sur la base des informations fournies lors des différents ateliers menés avec nos interlocuteurs. Ils ne sont donc pas exhaustifs

et ne peuvent remplacer le registre de traitements qui doit être mis en place par l'organisme responsable des traitements.

Traitement n°1 :

Gestion de la régulation des informations	
Finalité	Réguler les informations collectées via les applications de régulation et les faire transiter pour ensuite pouvoir apporter la solution ou extraire les données nécessaires à la planification de l'intervention.
Application/Logiciel	HéliSMUR
Base légale	Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne

Traitement n°2 :

Planification des interventions	
Finalité	Planifier les interventions
Application/Logiciel	HéliSMUR
Base légale	Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne

Traitement n°3 :

Edition des ordres de missions	
Finalité	Editer les ordres de mission pour chaque intervention
Application/Logiciel	HéliSMUR
Base légale	Intérêts légitimes du responsable du traitement ou d'un tiers
Sous-traitants	

Traitement n°4 :

Utilisation des données à des fins scientifiques et expérimentales	
Finalité	Utiliser les données pour des recherches scientifiques et expérimentales
Application/Logiciel	HéliSMUR
Base légale	Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne

Traitement n°5 :

Enregistrement des interventions	
Finalité principale	Enregistrer les interventions dans le registre HéliSMUR
Application/Logiciel	HéliSMUR
Base légale	Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne

Traitement n°6 :

Consultation des Webcams installés sur les sites	
Finalité	Consulter la météo via les images des webcams installés sur les sites d'atterrissage
Application/Logiciel	HéliSMUR

Base légale	Sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne
--------------------	---

B- Points de conformités identifiés

• Points de non-conformité

- 1. Absence d'un traitement de données :** lors des ateliers, aucune mention des données de connexion n'a été faite. Pourtant, il s'agit d'une application nécessitant un accès avec au minimum un login et un mot de passe. Une fiche de traitement doit donc être créée et insérée dans le registre des traitements.
- 2. Les mentions d'informations ne sont pas prévues.** Il faut prévoir un moyen d'informer les personnes concernées.
- 3. Manque de procédures applicables :** Il manque de nombreuses procédures applicables et appliquées pour répondre aux événements du RGPD
- 4. Conservation des données :** Il n'y a pas eu de travail sur la conservation et l'archivage des données pour la grande majorité des supports numériques
- 5. Aucune préanalyse et analyse d'impact n'a encore été réalisée,** pourtant il s'agit des données de santé qui transitent via l'application, donc des données sensibles.
- 6. Les accès aux données des organismes externes** n'ont pas été suffisamment délimités
- 7. Les contrats de sous-traitance** ne sont pas pour l'heure prévus. Pourtant, la partie conception des modules qui est réservée aux CHU relève d'une sous-traitance conformément au RGPD.

• Thématiques de conformité

Il ressort de ce diagnostic, 12 thématiques de conformité qui seront abordées dans la suite de ce document.

1. Vérification de la licéité des traitements et limitation de leur finalité
2. Information des personnes concernées

3. Minimisation de données
4. Mise en place des mesures de sécurité des données
5. Définition des durées de conservation et d'archivage
6. Documentation de la conformité (*accountability*)
7. Respect des principes de Privacy by design / Privacy by default
8. Implication du DPO et moyens mis à sa disposition
9. Respect des droits des personnes
10. Réalisation des analyses d'impact relatives à la protection des données (AIPD)
11. Transmission auprès des différents destinataires
12. Encadrement des transferts de données en dehors de l'UE
13. La vidéoprotection des sites

1- Vérification de la licéité des traitements et limitation de leur finalité

Lorsque des traitements de données sont mis en place, il faut à la fois réfléchir au **fondement permettant de les réaliser et définir quels en seront les objectifs**. Ces étapes sont primordiales pour s'assurer, a priori, de la conformité des traitements allant être réalisés.

L'article 5 (1) du RGPD définit les six principes de conformité, parmi ceux-ci, on retrouve :

- Au point (a) : le principe de licéité du traitement notamment, complété par l'article 6 du RGPD présentant les six bases légales possibles à un traitement (le consentement, le contrat / les mesures précontractuelles, l'obligation légale, la sauvegarde des intérêts vitaux, l'intérêt public / l'autorité publique et les intérêts légitimes) ;



Recommandations

Un **inventaire exhaustif des traitements** réalisés pour l'application doit être effectué, afin de **tracer les différentes bases légales et l'ensemble des finalités des traitements** réalisés au sein d'HéliSMUR.

Afin de mener à bien cet inventaire, il sera nécessaire de **faire participer l'ensemble des services**, en demandant à chacun de faire **un retour quant aux traitements mis en place** (par exemple, en mettant à leur disposition un modèle vierge de registre des traitements et des exemples de traitements de données déjà validés).

Afin de les aider dans cette tâche, un(e) responsable de la conformité pourrait animer des ateliers sur ce sujet.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Action G01-01

2- Information des personnes concernées

Pour chacun des traitements mis en œuvre, **une information doit être délivrée aux personnes concernées** par ces collectes de données personnelles. Cette information devant être transmise, que les données aient été collectées directement auprès des personnes concernées ou non.

Les articles 12 à 14 du RGPD indiquent les modalités à respecter afin d'informer correctement les personnes concernées.

L'article 12 prévoit que l'information doit être communiquée « *d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ».

L'article 13 liste les éléments devant apparaître dans l'information transmise, au moment de la collecte de données directement auprès de la personne concernée, dont des informations sur les acteurs du traitement, les éléments clés du traitement et les droits découlant du traitement réalisé.

Enfin, l'article 14 énonce ce que doit contenir l'information transmise aux personnes concernées par des collectes de données indirectes et pose un délai d'un mois maximum



Recommandations

Une version plus complète d'une **Charte de protection des données personnelles** doit être présente sur le site d'INEA, faisant office d'information principale pour les personnes concernées par les traitements.

Les services doivent s'assurer d'avoir une information disponible et pertinente lors de la mise en place d'un nouvel outil ou service, impliquant la réalisation de traitements de données.

En interne, **des mentions d'information types pourraient être rédigées** afin de pouvoir prévoir une information pour chacun des grands types de traitements de données réalisés.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G02-01

3- Minimisation des données

Des éléments propres aux données doivent être pris en compte pour réaliser un traitement conforme : **il faut limiter les données utilisées et s'assurer que ces données correspondent bien à la réalité** de la situation de la personne concernée.

L'article 5 (1) du RGPD définit, parmi les six principes de conformité :

- Au point (c) : le principe de minimisation des données du traitement, requérant une réflexion sur les données traitées afin que seules celles adéquates et pertinentes soient collectées ;
- Au point (d) : le principe d'exactitude, nécessitant de maintenir à jour les données traitées et d'effacer ou rectifier celles qui ne se révéleraient plus appropriées.



Recommandations

Afin de respecter le **principe de minimisation** des données, il vous sera conseillé :

- De vous baser sur une **cartographie exhaustive des traitements réalisés dans l'application**, cet élément vous permettant alors de définir les **données pertinentes** pour chacun des traitements ;

- De **définir des lignes directrices** à l'attention des différents services, afin de les accompagner dans la définition des données adéquates.

En complément, il faudra **sensibiliser régulièrement les équipes quant au principe de minimisation** et à la nécessité de ne pas porter atteinte à l'honneur ou à la réputation des personnes concernées par les traitements.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G03-01 et suivantes

4- Mise en place des mesures de sécurité des données

Afin de sécuriser les données, contre les différents risques pouvant impacter ces dernières, il sera nécessaire de **réfléchir à la mise en place de mesures techniques de sécurité**.

L'article 5 (1) (f) du RGPD énonce le principe d'intégrité et de confidentialité. Parmi les mesures pouvant être mises en place pour assurer la sécurité des données, on trouvera notamment les mesures techniques et les mesures organisationnelles.

L'article 32 propose, quant à lui, des mesures pouvant notamment être mises en place afin de garantir un niveau de sécurité adapté au risque, telles que : la pseudonymisation, le chiffrement, des moyens permettant de garantir l'intégrité, la disponibilité, la résilience et la disponibilité des systèmes et données ou une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la



Recommandations

Des mesures de sécurité doivent être mises en œuvre afin de garantir une meilleure conformité de HéliSMUR et du responsable de traitement INEA. Il s'agit essentiellement des politiques et procédures internes pour la sécurité des outils informatiques et le respect des droits des personnes.

Ces **politiques et procédures essentielles** pour assurer la sécurité des outils informatiques doivent être réfléchies, rédigées et mises en place. Cela sera le cas de la PSSI, mais aussi notamment du Plan de Reprise d'Activité (PRA) et du Plan de Continuité d'Activité (PCA).

La **charte informatique doit être mutualisée et régulièrement mise à jour**, afin d'actualiser les recommandations dispensées au regard de l'évolution des pratiques, appareils, outils et standards de sécurité.

Des **procédures internes** doivent être mises en place pour réagir et appliquer les bonnes pratiques en cas **d'évènement visé par le RGPD**. Il sera alors nécessaire de formaliser, communiquer et régulièrement sensibiliser quant à :

- **La procédure en cas de demandes de droit des personnes concernées ;**
- **La procédure en cas de violation de données personnelles ;**
- **La procédure en cas de contrôle de la CNIL.**

Un travail important de **limitation des accès aux données, dossiers et outils informatiques** doit être mis en place, afin que chacun des services n'accède qu'aux informations lui étant utiles et pour lesquels il est habilité à avoir accès.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G04-01 et suivants

5- Définition des durées de conservation et d'archivage

Le sujet de la limitation dans le temps du stockage des données personnelles emporte une série de réflexion : durée de conservation en base active, tri des données à la fin de ces durées, archivage des données, mesures à mettre en place lors de l'archivage des données...

L'article 5 (1) (e) du RGPD prévoit que les données personnelles ne peuvent être conservées que « pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Il faut distinguer 3 étapes concernant les durées :

- **La conservation en base active**, qui va correspondre aux données disponibles dans les outils, logiciels et bases de données d'utilisation courante, ainsi que dans les documents papiers utilisés actuellement (s'il y en a) ;
- **L'archivage intermédiaire**, où une partie des données seront entreposées (autant pour les supports numériques et pour les supports papiers) pour une période, tout en prévoyant des mesures de sécurité supplémentaires et un accès limité aux seules personnes habilitées au sein des services ;
- **L'archivage définitif**, pour des cas exceptionnels liés à l'intérêt public, à la recherche scientifique ou historique, ainsi qu'à des fins statistiques.

L'article 89 du RGPD prévoit différentes garanties et dérogations applicables aux traitements des données placées en archivage définitif.



Recommandations

Un travail transversal doit être entamé pour limiter les durées de conservation et d'archivage. **Plus aucune donnée personnelle ne peut être conservée pour des durées illimitées**, il sera nécessaire soit de **prévoir la durée fixe de conservation ou d'archivage**, soit de **préciser quel sera l'évènement déclencheur** pour que l'une de ces durées débute.

Afin de **définir les différentes durées de conservation et d'archivage applicables au sein d'une Politique de conservation et d'archivage des données**, nous vous suggérons de vous référer tout d'abord aux durées s'appliquant impérativement à votre organisme ou en cas de contentieux :

- Aux **durées obligatoires applicables aux principaux objectifs du registre HéliSMUR** ;
- Aux **durées de prescription applicables pour intenter une action en justice** (par exemple, le délai de droit commun en matière civile personnelle ou mobilière est de 5 ans, selon l'article 2224 du Code civil).

Une fois ces éléments pris en compte, il sera conseillé de se référer aux **publications proposées par la CNIL** :

- Le [guide pratique sur les durées de conservation](#), élaboré en partenariat avec le Service interministériel des archives de France (SIAF) ;

- [Le référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un **dispositif d'alertes professionnelles**.](#)

En plus de ces publications, il sera également possible de s'intéresser aux **articles directement publiés sur le site de la CNIL** ou à ses anciens référentiels datant d'avant l'entrée en vigueur du RGPD, maintenus accessibles par la CNIL en guise d'inspiration dans le cas où elle n'aurait pas encore publié quant à certaines thématiques.

Une fois les durées définies et les durées applicables documentées dans une **Politique de conservation et d'archivage des données**, il faudra compléter ce travail par une réflexion sur les **modalités de stockage, de tri, d'archivage et de suppression des données**.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G05-01 et suivantes

6- Documentation de la conformité (*Accountability*)

Depuis l'entrée en vigueur du RGPD, la plupart des démarches de déclaration auprès de la CNIL quant à la mise en place de traitements de données ont disparues. A présent, **il sera nécessaire pour le responsable de traitement de documenter sa conformité**.

C'est l'article 5 (2) du RGPD qui vise le principe de responsabilité : « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté ».

Parmi les documents de conformité, le RGPD présente à l'article 30 le principal document pour prouver son accountability : le registre des traitements. Cet article rappelle le contenu devant obligatoirement y apparaître (finalités, catégories de données, de personnes concernées et de destinataires...), pour le responsable du traitement et également pour le sous-traitant.



Recommandations

Des procédures concernant l'ensemble des thématiques du RGPD doivent être mises en place, communiquées et régulièrement renouvelées. Nous vous recommandons de rapidement faire appliquer les procédures afin de répondre à un évènement lié au RGPD.

Il sera nécessaire de créer rapidement un **registre des traitements exhaustif**, visant **l'ensemble des traitements mis en place via l'application**. Ce registre pourra contenir des informations supplémentaires afin de faciliter les différentes démarches propres au respect des normes de protection des données.

Afin de vous aider dans la **modélisation de votre registre des traitements**, vous pouvez utiliser le modèle de fiche proposé lors de notre étude. Vous pouvez également vous référer aux **éléments proposés par la CNIL**. Un autre document proposé par l'autorité peut aussi vous servir comme inspiration, quant à certains de ses éléments : [son propre registre des traitements](#).

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G06-01 & 02

7- Respect des principes de Privacy by design / Privacy by default

Ces principes consistent en la mise en place des mesures appropriées et des garanties nécessaires pour assurer, **dès la conception et par défaut**, la mise en œuvre effective des principes de protection des données et, par conséquent, des droits et libertés des personnes concernées.

L'article 25 du RGPD précise que « Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. »

L'article 25 définit à la fois les éléments dès la conception et les éléments par défaut à prendre en compte. Ces deux types d'éléments doivent être pris en compte lors de la

mise en place des traitements de données, aussi bien au lancement d'un nouveau service, que lors de la mise en place d'un nouvel outil.



Recommandations

Il va être nécessaire de réfléchir à une **politique dédiée aux principes de protection des données dès la conception et par défaut** au sein d'INEA et la mettre en place au sein de l'ensemble des équipes.

Cette politique devra permettre, **pour tout nouveau projet de traitement, d'outil et de service**, de **réfléchir à chacune des étapes de son développement à son implication en matière de protection des données**.

Pour mener à bien les objectifs de cette politique, il sera nécessaire de **mettre en œuvre un travail transversal entre différents services et acteur clés du projet**, afin que **soient pris en compte tous les aspects impactant le traitement de données envisagé**.

Pour vous aiguiller sur le sujet, nous vous recommandons de vous référer aux [lignes directrices proposées par le Comité européen de la protection des données concernant la protection des données dès la conception et protection des données par défaut](#).

Pour chacun des différents principes issus du RGPD, le Comité propose différents **éléments clés à prendre en compte** :

- **Transparence** : Clarté, sémantique, accessibilité, contextualité, pertinence, conception universelle, compréhensibilité, canaux multiples, structuration par couches ;
- **Licéité** : Pertinence, différenciation, finalité déterminée, nécessité, autonomie, obtention du consentement, retrait du consentement, mise en balance des intérêts, prédétermination, cessation, ajustement, répartition des responsabilités ;
- **Loyauté** : Autonomie, interaction, attentes, non-discrimination, non-exploitation, choix du consommateur, équilibre de pouvoir, absence de transfert des risques, absence de tromperie, respect des droits, éthique, véracité, intervention humaine, algorithmes loyaux ;
- **Limitation des finalités** : Prédétermination, spécificité, orientation en fonction des finalités, nécessité, compatibilité, limitation du traitement ultérieur, limitations de la réutilisation, réexamen ;

- **Minimisation des données** : Evitement du recours aux données, limitation, limitation de l'accès, pertinence, nécessité, agrégation, pseudonymisation, anonymisation et suppression, flux de données, état des connaissances ;
- **Exactitude** : Source des données, degré d'exactitude, précision mesurable, vérification, effacement / rectification, éviter la propagation d'erreurs, accès, maintien de l'exactitude, données tenues à jour, conception des données ;
- **Limitation de la conservation** : Suppression et anonymisation, effectivité de l'anonymisation et de la suppression, automatisation, critères de conservation, justification, contrôle de l'application des politiques en matière de conservation, sauvegardes / journaux, flux de données ;
- **Intégrité et confidentialité** : Système de gestion de la sécurité de l'information (SGSI), analyse de risque, sécurité dès la conception, maintenance, gestion du contrôle d'accès, transferts sécurisés, conservation sécurisée, pseudonymisation, sauvegardes / journaux, reprise après sinistre / continuité d'activité, protection en fonction du risque, gestion de l'intervention en cas d'incident lié à la sécurité, gestion des incidents ;
- **Responsabilité** : Démonstration de la conformité, démonstration du respect des principes, démonstration des effets des mesures prises, démonstration des raisons pour lesquelles les mesures sont considérées comme appropriées et efficaces, rappel des obligations applicables au responsable de traitement.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G07-01 à 02

8- Implication du DPO et moyens mis à sa disposition

Le Délégué à la Protection des Données (*Data Protection Officer* ou DPO en anglais) est la personne, désignée en interne ou en externe, qui va identifier et orchestrer les mesures de mise en conformité.

L'article 37 du RGPD requiert que le DPO soit désigné si l'organisme réalisant les traitements est une autorité publique ou un organisme public, ainsi que dans les cas où les traitements réalisés par la structure exigent un suivi régulier et systématique à grande échelle des personnes concernées ou s'ils permettent la collecte à grande échelle de catégories particulières de données personnelles ou de données personnelles relatives à des condamnations pénales et à des infractions.

En dehors de ces cas, il sera conseillé de désigner un DPO, par exemple, à partir du moment où l'activité de la structure se révélera à risque ou impliquera le traitement des données de

Afin que le DPO puisse pleinement exercer ses fonctions, il faudra s'assurer de désigner une personne disposant des **compétences requises**, mais aussi **mettre en place l'ensemble des moyens nécessaires** afin qu'il puisse mener à bien ses missions.

L'article 38 du RGPD énonce les différents prérequis afin que le DPO puisse exercer ses fonctions :

- Son association, de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données ;
- L'octroi des ressources nécessaires pour exercer ses fonctions et pour entretenir ses connaissances spécialisées ;
- L'absence d'instruction de la part de la hiérarchie ;
- La possibilité pour toute personne concernée par les traitements de données de prendre contact auprès du Délégué ;
- L'encadrement de ses missions grâce au secret professionnel ou à une obligation de confidentialité ;
- La possibilité d'exercer d'autres missions et tâches, sans qu'elles n'entraînent un conflit d'intérêts avec ses missions de Délégué.

Dans le cadre de ce projet (registre HéliSMUR), le DPO doit réaliser un certain nombre de tâches qui sont délimitées par l'article 39 du RGPD.

L'article 39 du RGPD liste les missions minimales du DPO :

- L'information et le conseil du responsable du traitement ou du sous-traitant et de leurs employés respectifs quant à leurs obligations en matière de protection des données ;
- Contrôler le respect des normes en matière de protection des données, notamment quant à la répartition des responsabilités, la sensibilisation et la formation du personnel, ainsi que les audits liés à ceux-ci ;
- Dispenser des conseils en matière d'analyses d'impact relative à la protection des données ;
- Coopérer avec l'autorité de contrôle (la CNIL en France) et être un point de contact pour cette dernière.

Au-delà des missions apparaissant listées dans l'article 39, il est possible de viser des **missions supplémentaires**, tant que ces dernières permettent également le **suivi des mesures mises en place afin d'assurer que les traitements sont conformes** aux normes en matière de protection des données personnelles. L'objectif étant de l'impliquer suffisamment dans les actions afin d'assurer constamment la conformité de l'outil.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G08-01 et suivants

9- Respect des droits des personnes

Le RGPD, en plus de faire peser différentes obligations sur les épaules des responsables et sous-traitants, va également **octroyer différents droits aux personnes concernées** par les traitements de données réalisés par ces deux catégories d'acteurs.

Le RGPD ouvre les droits suivants aux personnes concernées : le droit à l'information (articles 12 à 14), le droit d'accès (article 15), le droit de rectification (article 16), le droit à l'effacement ou « droit à l'oubli » (article 17), le droit à la limitation du traitement (article 18), le droit à la portabilité des données (article 20), le droit d'opposition (article 21) et le droit de refus des prises de décisions individuelles automatisées, comme le profilage (article 22).

Il est essentiel de **pouvoir répondre rapidement à ces demandes de droits**, car l'organisme aura, par principe, **un délai d'un mois pour traiter et répondre à la demande de la personne concernée** par l'un des traitements mis en œuvre.

L'article 12 (3) du RGPD prévoit que le responsable du traitement doit répondre à une demande de droit dans un délai d'un mois, à moins qu'il ne prévienne la personne d'une prolongation de ce délai de deux mois supplémentaires, soit à cause de la complexité de la demande, soit parce qu'il doit traiter un nombre important de demandes.



Recommandations

La **procédure de gestion des demandes de droits des personnes concernées doit être refondue** afin qu'elle permette d'accompagner l'ensemble des équipes lorsqu'une demande de droits est transmise à leur service.

Il sera nécessaire que cette procédure précise au moins :

- Les **différents types de demandes de droits** ouvertes par le RGPD ;
- Les **bons réflexes à adopter en cas de réception d'une demande** (informations à demander à la personne, personnel à contacter au sein de INEA, préparation éventuelle de documents pour la personne en interne allant répondre...) ;
- Les **réflexions** devant être engagées par la personne évaluant **s'il faut vérifier ou non l'identité de la personne** et **s'il faut répondre ou non à la demande** ;
- La **méthodologie pour répondre à une demande valable**.

Les informations listées ci-dessus pourront également être séparées en **plusieurs procédures**, comme une **procédure synthétique pour l'ensemble des services** et une **procédure détaillée pour le ou les services en charge de la réponse à la demande**.

En plus de la procédure allant être mise en place, il sera nécessaire que les équipes **soient prêtes à répondre aux demandes de droit**. Par exemple, dans le cadre d'une demande de droit d'accès, il sera alors nécessaire que **les équipes sachent où se trouvent les informations des différentes personnes concernées par leurs traitements**, afin d'être capables de rassembler l'ensemble des informations à transmettre lors de la réponse à la demande.

Pour retransmettre des informations quant aux demandes de droits reçues, il sera éventuellement possible de s'appuyer sur un **réseau de référent internes** (voir ci-dessus nos recommandations quant à **l'implication du DPO et moyens mis à sa disposition**).

Enfin, il sera vivement conseillé au DPO de **centraliser les demandes d'exercice de droits issus du RGPD au travers d'un registre unique**, afin :

- D'avoir une vision exhaustive des demandes de droits exercées auprès d'INEA ;
- De pouvoir contrôler que les services internes permettent bien de faire droit à ces demandes, notamment en termes de délai (1 mois).

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G09-01

10-Réalisation des analyses d'impact relatives à la protection des données (AIPD)

Le RGPD impose au responsable du traitement, lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, de **réaliser une analyse d'impact relative à la protection des données (AIPD)**.

L'article 35 du RGPD prévoit que le responsable du traitement effectue une analyse d'impact relative à la protection des données (AIPD) lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

De plus, l'article prévoit que cette analyse devra être réalisée pour 3 cas particuliers : l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques par le biais d'un traitement automatisé et afin de prendre des décisions importantes, le traitement à grande échelle de données sensibles et la surveillance systématique à grande échelle d'une zone accessible au public.

Afin d'encadrer davantage de traitements par la réalisation d'une telle analyse, [les lignes directrices du G29 relatives aux analyses d'impact](#) identifient neuf critères qui imposeraient la réalisation d'une AIPD (évaluation/scoring, décision automatique,

surveillance systématique, données sensibles ou données à caractère hautement personnel, collecte à large échelle, croisement de données, personnes vulnérables, usage innovant, exclusion du bénéfice d'un droit/contrat).

A partir de deux de ces critères, une analyse d'impact devra être réalisée. Si un seul de ces critères s'applique au traitement, il faudra s'interroger sur la pertinence de réaliser une AIPD.

Par ailleurs, **la CNIL a publié deux documents dédiés :**

- [Une liste de traitements qui nécessitent la réalisation d'une AIPD ;](#)
- [Une liste des traitements pour lesquels une AIPD ne sera pas nécessaire.](#)

Dès lors qu'elle devra être réalisée, l'analyse d'impact relative à la protection des données se décomposera alors en trois parties :

- **Une description détaillée** du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels ;
- **L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux** (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
- **L'étude, de nature plus technique, des risques sur la sécurité des données** (confidentialité, intégrité et disponibilité), **ainsi que leurs impacts potentiels** sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.



Recommandations

Une procédure de gestion des analyses d'impact relatives à la protection des données (AIPD) doit être mise en place au sein de l'organisme.

Il apparaît nécessaire de **revoir l'ensemble des fiches de traitement** afin, d'une part, **d'identifier les traitements qui nécessitent la réalisation d'une AIPD** et, d'autre part, **de formaliser un plan de réalisation en fonction de l'exposition aux risques**.

Il faudra réaliser les analyses d'impact pour les traitements mentionnés ci-dessus. Ces analyses ne pourront s'effectuer qu'avec la collaboration de chacun des services pouvant mettre en œuvre le traitement, encadrer celui-ci ou en sécuriser les données.

Il sera nécessaire à l'avenir de **vérifier systématiquement**, avant la mise en place d'un traitement, **si ce traitement est susceptible d'engendrer un risque élevé** pour les droits

et libertés des personnes physiques et, **le cas échéant, réaliser alors une analyse d'impact.**

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G10-01

11-Transmission auprès des différents destinataires

Le RGPD va s'intéresser également aux différentes personnes et entités allant recevoir des informations de la part de l'organisme : aussi bien destinataires internes à l'organisme que destinataires externes (responsables de traitements, sous-traitants et tiers autorisés).

L'article 26 du RGPD va prévoir pour les responsables conjoints d'un traitement, définissant ensemble les finalités et moyens de ce traitement, qu'ils devront contractualiser afin de faire apparaître leurs obligations respectives en matière de protection des données et le point de contact pour les personnes concernées.

L'article 28 du RGPD oblige le responsable et le sous-traitant à contractualiser et couvrir ainsi un certain nombre de thématiques (nature du traitement allant être réalisé – suivi des instructions documentées du responsable – obligation de confidentialité – sécurité des données traitées – encadrement du recrutement d'un autre sous-traitant – assistance du responsable pour les demandes de droits, les violations de données et les analyses d'impact – devenir des données à la fin de la prestation – mise à disposition des documents de

- **Destinataires internes et externes de l'organisme**

Les personnes et entités auxquels INEA transmet ou accorde des accès aux données doivent au préalable être identifiés, pour ensuite mieux encadrer les différents accès et transmissions possibles.



Recommandations

Un travail important de réflexion quant à la légitimité des accès, de documentation des accès possibles et de limitation des accès au sein de la société doit être rapidement entamé afin de sécuriser les informations collectées, notamment en cas d'accès non autorisé. Cette réflexion devant déboucher à la rédaction d'une **procédure interne de gestion des accès**.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G11-01 et suivantes

- **Sous-traitants**

Au sens de l'article 28 du Règlement Général sur la Protection des Données, le sous-traitant est la personne physique ou morale qui traite des données pour le compte d'un organisme dans le cadre d'un service ou d'une prestation. Ainsi, les sous-traitants, tout comme l'organisme responsable de traitements doivent respecter le RGPD.



Recommandations

Une revue des cas de sous-traitance doit être effectuée par INEA.

Des conventions ou contrats de sous-traitance, voire des avenants aux contrats doivent être mis en place et signés **avec chacun des sous-traitants** avec lesquels un contrat conforme à l'article 28 se révélerait absent.

Pour chacun de ces sous-traitants, il sera alors nécessaire **d'étudier les contrats transmis par ceux-ci**, pour vérifier s'ils sont conformes à l'article 28, et **de les interroger quant à leur conformité**, tout en leur demandant de transmettre tout document permettant d'attester de leur conformité.

NB: Nous vous rappelons que, dès lors qu'un prestataire est amené à collecter ou à accéder à des données personnelles pour votre compte, il sera nécessaire de revoir le contrat signé ou d'en prévoir un si ce n'est pas encore fait, peu importe que le contrat ait été signé avant ou après l'entrée en application du RGPD le 25 mai 2018.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G11-01 et suivants

12-Encadrement des transferts de données en dehors de l'UE

Le RGPD encadre strictement la possibilité de transférer des données personnelles en dehors de l'UE, en ne permettant de procéder ainsi qu'en ayant, au préalable, vérifié que la législation du pays du destinataire aura été déclarée adéquate ou, si ce n'est pas le cas, en ayant mis en place différents mécanismes.

L'article 45 du RGPD est celui permettant le transfert de données vers un pays dont la législation aura été déclarée comme adéquate par la Commission Européenne.

Au moment de la rédaction de ce rapport, les pays concernés sont les suivants d'après la Commission : Andorre, Argentine, Canada, Corée du Sud, Guernesey, Ile de Man, Iles Féroé, Israël, Japon, Jersey, Nouvelle-Zélande, Royaume-Uni, Suisse, Uruguay.

Différents articles du RGPD vont proposer les mécanismes permettant de réaliser un traitement en l'absence de décision d'adéquation, dont notamment :

- Des règles contraignantes permettant le transfert au sein d'un groupe de sociétés (article 47) ;
- Des clauses contractuelles types adoptés par la Commission Européenne (article 93) ;
- Un code de conduite approuvé par une autorité de contrôle (article 40) ;
- Un mécanisme de certification approuvé par un organisme de certification ou l'autorité de contrôle (article 42).

Enfin, des dérogations sont proposées à l'article 49 du RGPD pour des situations particulières, comme le sera le fait de demander le consentement explicite de la personne



Recommandations

Un inventaire des cas de transferts hors UE devra être effectué, ainsi que celui des mécanismes effectivement mis en place afin de réaliser le transfert.

Ces premières étapes permettront alors **de définir les cas où la mise en place d'un mécanisme permettant le transfert reste nécessaire. Il faudra alors régulariser au plus vite la situation avec chacun des prestataires ou partenaires allant recevoir des informations.**

Nous vous rappelons qu'il vous est possible, **dans des cas exceptionnels, de s'appuyer sur les dérogations** ouvertes par l'article 49 du RGPD.

Plan d'action

Pour cette thématique, nous vous proposons de vous référer aux actions suivantes du plan d'action (PLAN D'ACTION HéliSMUR.xlsx) :

- Actions G12-01 et suivantes

C- Evaluation des vidéos visualisées (les vidéoprotections des sites)

Dans le cadre de cette mission, il nous a été demandé de dresser des recommandations et préconiser des actions pour assurer la conformité de la vidéoprotection ou Vidéosurveillance.

Il était donc prévu de fournir :

- Un exemple d'affichage recommandé par la CNIL
- Registres des sites mentionnant :
 - Evaluation si vidéo surveillance ou vidéo protection
 - Le type d'affichage
 - La date de revue
 - Les recommandations pour la mise en conformité sous forme de procédure

D'après les différents travaux menés et sur la base des informations reçues lors des ateliers, il apparaît clair que ni INEA, ni le CHU n'est responsable des installations des webcams. HéliSMUR utilise donc des webcams publiques afin de bien repérer les sites et d'avoir également des informations précises sur la météo qu'il fait en temps réel. Les images consultées ne sont pas enregistrées sur l'application, encore moins hébergées sur les serveurs d'INEA. Aucune des obligations légales relatives aux mentions d'informations (panneaux), les démarches préalables auprès de la préfecture n'incombent donc pas l'organisme.

Par conséquent, il ne s'agit pas d'une vidéosurveillance ou d'une vidéoprotection mise en œuvre par HéliSMUR ou son responsable de traitement puisqu'il s'agit de simples consultations des images via les services proposés par d'autres prestataires responsables de leurs enregistrements vidéo. Ces enregistrements sur les sites n'ont pas été mis en place par INEA ou gérés via l'application. Ils sont consultés à distance par l'équipe dans le cadre de la planification de l'intervention.

Finalement, aucun registre ou type d'affichage n'est prévu sur ce volet. N'étant pas concerné par ces obligations, nous ne ferons pas de recommandation pour la mise en conformité d'un tel traitement. En revanche, il doit être inclus dans le registre de traitements par précaution en raison des possibilités d'images des personnes physiques présentes sur les sites, que l'on pourrait éventuellement voir au moment de la consultation. Raison pour laquelle nous l'avons identifié dans la fiche de traitement qui vous est mis à disposition.