MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Direction générale
de la Sécurité civile
et de la gestion des crises

Convention de partenariat

DIRECTION GÉNÉRALE
DE LA SÉCURITÉ CIVILE
ET DE LA GESTION DES CRISES

Sapeurs-Pompiers
de la Seine-Maritime

Entre

Le ministère de l'Intérieur,
Sis place Beauvau, 75 800 Paris cedex 08, représenté par le directeur général de la Sécurité civile et de la gestion des crises, M. Alain THIRION
Ci-après désigné par la « DGSCGC », d'une part

et

Le service départemental d'incendie et de secours de la Seine-Maritime,
6 rue du Verger – 76192 Yvetot, représenté par son président du conseil d'administration, Monsieur André GAUTIER, dûment habilité par délibération du bureau du conseil d'administration du service départemental d'incendie et de secours, aux fins des présentes,
Ci-après dénommé le « SDIS »,

Ci-après conjointement appelés « les parties ».

Il est préalablement exposé ce qui suit :

Préambule

La direction générale de la Sécurité civile et de la gestion des crises (DGSCGC) dont les missions sont fixées par le décret n° 2013-728 du 12 août 2013 modifié portant organisation de l'administration centrale du ministère de l'Intérieur et du ministère des outre-mer, a notamment en charge :

- de garantir la cohérence de la Sécurité civile au plan national, d'en définir la doctrine et d'en coordonner les moyens ;
- d'évaluer, de préparer, de coordonner et de mettre en œuvre des mesures de protection, d'information et d'alerte des populations, de prévention des risques civils de toute nature, de planification des mesures de Sécurité civile ;
- de mener les actions de secours visant à la sécurité des personnes et des biens, en temps de paix comme en temps de crise.

L'article L 1424-2 du CGCT fixe les missions des services d'incendie et de secours (SIS), notamment ils :

- sont chargés de la prévention, de la protection et de la lutte contre les incendies.
- concourent, avec les autres services et professionnels concernés, à la protection et à la lutte contre les autres accidents, sinistres et catastrophes, à l'évaluation et à la prévention des risques technologiques ou naturels ainsi qu'aux secours d'urgence.
- exercent, dans le cadre de leurs compétences, les missions de protection des personnes, des biens et de l'environnement ; de secours d'urgence aux personnes victimes d'accidents, de sinistres ou de catastrophes ainsi que leur évacuation.

Le SDIS détient pour sa part des données, métadonnées, fichiers, bases de données et autres systèmes informatiques contenant de l'information dont il est auteur ou producteur et sur lesquels il dispose des droits suffisants pour consentir la présente convention.

Afin de contribuer à l'accomplissement de la mission de service public de la DGSCGC, le SDIS a décidé de mettre gratuitement à la disposition de cette dernière lesdites données, métadonnées, fichiers, bases de données et autres informations sous format numérique.

Ceci étant exposé, il est convenu ce qui suit :

Article 1

Objet de la convention

La présente convention est conclue entre la DGSCGC et le SDIS. Elle a pour objet de définir les conditions dans lesquelles le SDIS met des données à disposition de la DGSCGC aux fins d'alimentation de l'entrepôt national de données de la Sécurité civile.

Cet entrepôt, géré par la DGSCGC, rassemble les données de Sécurité civile et notamment les données relatives aux opérations de secours des services d'incendie et de secours. Il sert de base aux travaux et études menées par la DGSCGC et de socle à l'outil de visualisation, et diffusion, de ces données.

Article 2

Échange des données

1 - Nature des données collectées

Le dictionnaire des données collectées est décrit en annexe 1.

2 - Utilisation des données

La DGSCGC utilise les données collectées aux fins de pilotage de l'activité des SIS au niveau national. Certaines données statistiques peuvent être diffusées publiquement sur le site data.gouv.fr, dans le respect du règlement général sur la protection des données à caractère personnel. Aucune donnée brute n'est publiée sur le site data.gouv.fr

L'inspection générale de la Sécurité civile et de la gestion des crises dispose d'un accès lui permettant d'utiliser des données des SIS dans le cadre de ses missions d'évaluation ou de suivi.

Le projet intègre la production d'indicateurs et d'analyses qui permettent la mise en perspective des données des SIS. Un outil de type observatoire est construit et un accès est fourni aux SIS.

3 - Pré-requis au niveau du SDIS

Les pré-requis nécessaires à l'échange des données sont précisés en annexe 2.

4 - Gestion des accès et sécurité

La gestion des accès à l'infrastructure du SDIS est réalisée conjointement par la DGSCGC et le SDIS. Les accès sont limités au strict nécessaire pour le transfert des données, la supervision et la maintenance.

La DGSCGC s'engage à garder confidentiel l'accès au réseau administratif du SDIS sur lequel les données sont copiées. Seule la DGSCGC peut disposer d'un accès à la partie spécifique du réseau administratif du SDIS concernée par les échanges des données.

L'ensemble des données évoluant sur des supports informatiques, les parties s'engagent à mettre en œuvre des moyens matériels suffisants afin de prévenir les cyber-attaques ou les avaries informatiques qui pourraient générer une fuite des données.

Les modalités des actions à distance et les éléments de sécurité sont précisées en annexe 3.

Article 3

Restriction et propriété intellectuelle

5 - Propriété intellectuelle

La convention n'est aucunement une cession de droits de propriété intellectuelle du SDIS à la DGSCGC, mais une simple mise à disposition des données dans les conditions définies dans la convention.

La DGSCGC s'engage à respecter les droits du SDIS et, par conséquent, les conditions, limites et restrictions d'exploitation des données, le cas échéant, telles qu'elles sont précisées dans l'article 2.

Le SDIS accorde à la DGSCGC le droit personnel, non cessible, non transmissible et non-exclusif d'utiliser les données pour les besoins de sa mission de service public.

La DGSCGC doit faire figurer sur tout document présentant tout ou partie des données, ou des études et analyses réalisées à partir de tout ou partie des données, la mention de leur source et la date de leur dernière mise à jour. Cette mention doit apparaître sous toute forme de support de diffusion, numérique ou non, de manière lisible.

Chacune des parties conserve la propriété intellectuelle des travaux réalisés à partir des données échangées.

6 - Autres restrictions

Aucune donnée à caractère personnel ou nominative n'est remontée au niveau de la DGSCGC (anonymisation faite localement avant transmission à la DGSCGC).

Les droits concédés à la DGSCGC par le SDIS aux termes de la convention, le sont à titre gracieux. En contrepartie, la DGSCGC s'engage à communiquer au SDIS les analyses qu'elle réalise permettant la mise en perspective des données des SIS.

Aucune revente de données transmises à la DGSCGC dans le cadre de cette convention ne peut être effectuée par cette dernière.

7 - Mises en garde

Le SDIS met tout en œuvre pour assurer la fiabilité des données collectées.
L'exactitude, la mise à jour, l'intégrité et l'exhaustivité de ces données ne peuvent cependant être totalement garanties par le SDIS.

Il appartient à la DGSCGC d'apprécier sous sa responsabilité entière et exclusive :

- l'opportunité d'utiliser les données ;
- la compatibilité des fichiers avec ses systèmes informatiques ;
- l'adéquation des données à ses besoins ;
- qu'elle dispose de la compétence suffisante pour utiliser les données ;
- l'opportunité d'utiliser la documentation ou les outils d'analyse fournis ou préconisés en relation avec l'utilisation des données, le cas échéant.

Article 4

Pilotage et suivi de la convention

Un comité de suivi, composé des signataires de la présente convention ou de leurs représentants, est institué avec pour missions :

- d'assurer le suivi de la réalisation des actions conformément aux modalités de coopération prévues dans la présente convention de partenariat ;
- d'émettre des préconisations sur la poursuite du partenariat.

Ce comité de suivi se réunit, en présentiel ou en distanciel, chaque fois que les signataires l'estiment nécessaire et dans un délai de deux mois quand il est saisi par au moins un des membres.

Il traitera également des questions techniques touchant à la sécurité : collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité.

Article 5

Communication

Les parties s'engagent à s'informer mutuellement au préalable de la mise en œuvre de toute action de communication liée à la présente convention.

Elles s'engagent à définir conjointement, pour les actions le nécessitant, les modalités de diffusion des travaux réalisés en commun et à faire apparaître sur tout support de diffusion les logos de chacune d'elles, dans des formats similaires.

Article 6

Durée de la convention

La présente convention est conclue pour une durée de 3 ans à compter de la date de sa signature par chacune des parties et reconductible 3 fois par tacite reconduction.

Article 7

Modifications de la convention

Toute modification de la présente convention, définie d'un commun accord entre les parties, fera l'objet d'un avenant formalisé par écrit. Les dispositions de l'avenant prennent effet à compter de sa signature par les deux parties. Les avenants ultérieurs font partie de la présente convention et sont soumis à l'ensemble des dispositions qui la régissent.

Article 8

Résiliation de la convention

Chacune des parties peut résilier la présente convention à tout moment, en cours d'exécution et pour tout motif, par l'envoi d'une lettre recommandée avec accusé de réception. La résiliation prend effet à l'expiration d'un délai de trois mois à compter de la

réception de la lettre recommandée avec accusé de réception et après clôture des actions engagées à la date du préavis. Les données transmises antérieurement à la date d'effet de la résiliation, restent dans l'entrepôt de données conformément aux règles relatives à leur durée de conservation.

Article 9
Litiges

Tout litige né de l'interprétation et/ou de l'exécution de la présente convention fera l'objet d'une tentative de règlement amiable entre les parties.

A défaut d'accord à l'issue d'un délai de 30 jours calendaires à compter de la réception d'une lettre recommandée avec avis de réception notifiée par l'une des deux parties et précisant la difficulté en cause, chacune des parties peut saisir le tribunal administratif compétent.

Annexes (3) :

- Annexe 1 : dictionnaire des données
- Annexe 2 : pré-requis techniques
- Annexe 3 : accès et sécurité

Fait à

En deux exemplaires originaux, le

Le président du conseil d'administration du SDIS 76	Pour le ministre et par délégation, le préfet, directeur général de la Sécurité civile et de la gestion des crises
André GAUTIER	Alain THIRION

Annexe 1 – Nature des données collectées

Les données collectées depuis les SIS ne contiennent aucune Donnée à Caractère Personnel, elles ne sont donc pas nominatives, et ne contiennent aucun champ de texte libre type commentaire ou observation.

Périmètre fonctionnel général

Le périmètre fonctionnel initial du projet est celui de « l'activité opérationnelle », et concerne les faits suivants :

- Appels

Donnée	Exemple
ID appel	Identifiant anonymisé avant envoi vers l'entrepôt
Date de début d'activité du centre commun 15-18-112	Paramétrage manuel
Date de fin d'activité du centre commun 15-18-112	Paramétrage manuel
Faisceau	18, 112, SAMU, ...
Groupe faisceau	Ligne urgence, autre
Sens	E / S
Temporalité	Année, mois, jour, heure
ID inter	
Rattaché inter ?	ID inter rattachement
Nature de l'intervention	Accident de vélo, feu d'entrepôt, ...
Primo appel ?	O/N
Date arrivée	
Date de présentation	
Date de 1er décroché du CTA	
Date de 1re alerte	
Date de raccroché du CTA	
Source	SIS, SYSTEL, NexSIS

- Interventions

Donnée	Exemple
N° intervention	
INSEE actuel	
INSEE original	
Lieu de l'intervention	
Localisation	Voie publique, local à sommeil, ...
Paramétrages	
Code du centre de premier appel	
Nature de l'intervention SDIS	Accident de vélo, feu d'entrepôt, ...
Raison de sortie SDIS	
Nature de l'intervention DG	
Nomenclature DG	
Surface brûlée	
Surface menacée	
Temporalité	Année, mois, jour, heure
Date arrivée 1er appel	
Date 1ere alerte	
Date 1er engin SDIS sur les lieux	

Date fin intervention	
Flags ? Local à sommeil, cheminée, carence, ...	

- Victimes

Donnée	Exemple
ID victime	Identifiant anonymisé avant envoi
ID inter	
Sexe	
Âge, tranche d'âge	
Victime SP intervenant	Oui/non
Etat victime fin d'intervention	Décédé, UA, UR, Impliqué
Etablissement	
Transport vers établissement. de soin	

- Engins engagés

Donnée	Exemple
ID engin engagé	
ID inter	
Centre	
Nomenclature type engin	
Mission engin	GFO dans Artémis
Fonction d'engagement engin	VSR pour FPTSR engagé sur du SR
Date alerte	
Date départ	
Date arrivée sur les lieux	
Date départ des lieux	
Date arrivée CH	
Date départ CH	
Date retour dispo	
Date fin	
Effectif au départ	

- Agents engagés

Donnée	Exemple
ID agent engagé	Identifiant anonymisé avant envoi
ID engin engagé	
Centre	
Nomenclature type engin	
Nomenclature grade	
Statut	
Fonction d'engagement agent	CA FDF, EQ SR, ...
Date alerte	
Date départ	
Date fin	

- Plannings des agents

Donnée	Exemple
ID planning agent	
ID agent	Identifiant anonymisé avant envoi
Centre	
Nomenclature grade	
Statut	
Nomenclature type de disponibilité	
Date début	
Date fin	

- Nomenclatures

Donnée	Exemple
Commune	
Centre	
Type engin	
Motif de départ	
Raison de sortie	
DGSCGC	

Reprise et conservation des données

Reprise depuis le 01/01/2018
Durée de conservation : 10 ans

Planification

Les traitements d'alimentation sont planifiés quotidiennement : objectif de mise à jour à J+2, J+7 maximum

Seules les données ayant été modifiées ou créées depuis la dernière alimentation de l'entrepôt y sont transférées. Au-delà de 3 mois, les données sont réputées définitives et ne sont plus modifiées dans l'entrepôt national. A titre exceptionnel et si l'impact sur l'ensemble des données le justifie, une mise à jour de données antérieures à 3 mois pourra être effectuée.

Annexe 2 – Pré-requis au niveau du SIS

Pendant la phase de raccordement du SIS, estimée à un mois, le SIS s'engage à mettre à disposition du prestataire les personnels du SIS ayant les compétences techniques et/ou les connaissances des outils métiers pour une durée estimée à 3 jours discontinus.

Pré-requis techniques :

Accès aux données sources	La base sur le réseau opérationnel n'est pas accessible. Une sauvegarde quotidienne avec déplacement sur le réseau administratif est nécessaire. L'accès à cette copie sur le réseau administratif est indispensable et doit être mis en, place par le SDIS ou l'éditeur du SGA/SGO.
Machine virtuelle Windows	Sur le réseau administratif du SIS et accessible pour installation des bases de données et de l'ETL. Minimum : quadri-pro, 16 Go RAM et 250Go de disque dur
Licences de base de données	Licence Oracle ou licence SQL server Licence de base de données permettant le stockage des données (technologies Oracle, Microsoft SQL Server ou PostGreSQL)
ETL Data Intelligence	Outil permettant le traitement des données (collecte, transformation, contrôles, planification, …)
Agent CIP	Programme permettant le déplacement des données de l'infrastructure SIS vers l'infrastructure DGSCGC
Ouverture de port	Port https 443 sortant permettant le déplacement des données de l'infrastructure SIS vers l'infrastructure DGSCGC
Accès à distance	Le SDIS doit permettre l'accès à distance de la machine virtuelle Windows. Cet accès permet : • l'installation des outils ; • la mise en place des traitements ; • la réalisation de la maintenance proactive si un traitement échoue, l'accès à distance de la machine virtuelle Windows doit respecter le consentement du sdis. Elle ne doit être possible que suite à l'acceptation explicite du sdis ou à l'initiative de ce dernier. Toute connexion arbitraire au sdis est interdite.

Pour les SIS déjà équipés de la solution AnalySDIS via l'éditeur Oxio/Ciril Group, le socle existant sera utilisé, si le SDIS le souhaite.

Annexe 3 – Accès et sécurité

8 - Accès à distance

Le télédiagnotic et la télémaintenance doivent respecter le même niveau de sécurité que celui des données traitées. La liaison établie pour les interventions ou le traitement ne l'est pas de façon permanente et fait l'objet d'une traçabilité au travers de logs édités et gérés par la DGSCGC.

Un journal d'événement est mis en place afin de collecter les actions réalisées lors de l'intervention et des traitements. Ce journal doit comporter à minima l'horodatage, le compte d'exécution, les commandes et messages des applications et du système.

Les mots de passe utilisés ne doivent pas être par défaut ou faibles.

L'exploitation de vulnérabilités sur un dispositif de télémaintenance est susceptible de faciliter les intrusions dans le système d'information et d'affecter ainsi la sécurité de l'ensemble du SI. Une attention particulière est portée aux outils et système de prise en main à distance en matière de faille de sécurité.

Les interventions doivent se faire aux jours et heures ouvrées (lundi au vendredi de 8h30 à 17h30).

Un rapport d'intervention est envoyé au SDIS (contacts listés au paragraphe 4) à chaque intervention. Il comprend la date et heure de début et fin d'intervention ainsi que les actions menées sur les environnements.

9 - Traitement automatisé

Tous les traitements automatisés font l'objet de traçabilité dans un journal d'événement. Ces traitements ne doivent pas nécessiter de droits élevés sur les systèmes.

Lors d'une erreur, le traitement ne doit pas être rejoué sans l'analyse et la correction du support. Les traitements automatisés doivent toujours préserver l'intégrité et la disponibilité des systèmes.

10 - Obligations des parties

Les deux parties s'informent préalablement de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système.

Les mécanismes de sécurité mis en œuvre doivent évoluer conformément à l'état de l'art : la découverte de failles dans un algorithme, un protocole, une implémentation logicielle ou matérielle, ou encore l'évolution des techniques de cryptanalyse et des capacités d'attaque par force brute doivent être pris en compte.

11 - Contacts :

Il appartient à chacune des parties d'indiquer tout changement dans la liste des contacts.

SDIS76
Chef de groupement « Pilotage Evaluation Prospective et SI »
Erwan MAHE 02 35 56 38 23
erwan.mahe@sdis76.fr

DPO
Luc ANDRIEU 02 32 70 70 92
luc.andrieu@sdis76.fr

DGSCGC
Responsable de traitement
Patrick ROUSSEL 01.72.71.66.76
patrick.roussel@interieur.gouv.fr

RCSSI et correspondant à la protection des données
Olivier Euverte 01.45.64.48.58
olivier.euverte@interieur.gouv.fr