SDIS TARN
Sapeurs-Pompiers

EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS DU BUREAU
DU CONSEIL D'ADMINISTRATION
DU SERVICE DÉPARTEMENTAL D'INCENDIE ET DE SECOURS DU TARN

SÉANCE DU 07 NOVEMBRE 2023

L'an deux mille vingt trois et le sept du mois de novembre, à neuf heures, le bureau du conseil d'administration, régulièrement convoqué, s'est réuni au nombre prescrit par la Loi, dans les locaux de l'État-Major du SDIS, 15, rue de Jautzou, sous la présidence de M. Michel BENOIT.

Présents: Membres à voix délibérative :
MM. Michel BENOIT, Bernard MIRAMOND, Jean-Michel BOUAT.
Mme Eva GERAUD.

Participent à la séance :
Colonel Jimmy GAUBERT, directeur départemental.
Colonel Eric VIAL, directeur départemental adjoint.
Lieutenant-colonel Philippe CNOCQUART, sous-directeur pilotage et stratégie.

Secrétaire :
Colonel Jimmy GAUBERT, directeur départemental.

Absent excusé :
Christophe TESTAS.

Nombre de membres à voix délibérative en exercice : 5 / présents : 4 / votants : 4.
Date de la convocation : 31 octobre 2023.
~~~~~~
RAPPORT N°062/BUR-11/2023

OBJET : convention de raccordement à l'observatoire des services d'incendie et de secours (ObSIS)

L'ObSIS est l'entrepôt national de données opérationnelles des SIS permettant à la DGSCGC et aux services d'incendie et de secours (SIS) de suivre au quotidien les indicateurs opérationnels de l'ensemble des SIS. Le directeur général de la sécurité civile et de la gestion des crises ambitionne de raccorder à l'ObSIS, à l'horizon de la fin d'année 2024, le plus grand nombre de SIS désireux de s'engager dans la démarche.

Sur le plan fonctionnel, ce raccordement conduit à ce que le SDIS mette des données à la disposition de la DGSCGC aux fins d'alimenter l'entrepôt national de données opérationnelles de la Sécurité Civile. A terme, cet entrepôt, géré par la DGSCGC, rassemblera les données de Sécurité civile et notamment celles relatives aux opérations de secours des services d'incendie et de secours. Il servira de base aux travaux et études menés par la DGSCGC et de socle à l'outil de visualisation et diffusion de ces données.

Sur le plan technique, la société Oxio est le prestataire désigné par la DGSCGC pour la construction de cet entrepôt. Le SDIS du Tarn étant déjà équipé de la solution Oxio d'aide à la décision, les pré-requis nécessaires à ce raccordement sont réunis.

Sur le plan administratif, une convention (dont le projet est présenté en annexe) doit être signée entre le président et le directeur général de la sécurité civile et de la gestion des crises. Cette convention prévoit notamment :

- qu'aucune donnée nominative n'est stockée dans l'entrepôt national (le SDIS doit pseudonymiser la donnée avant livraison) ;
~~~~~~

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

- que l'alimentation de l'entrepôt national est quotidienne ;
- qu'une reprise des données depuis le 01/01/2018 sera effectuée pour disposer de suffisamment de recul ;
- que la durée de conservation des données par la DGSCGC est fixée à 10 ans ;
- qu'un plan d'assurance sécurité et de protection des données personnelles soit établi ;
- que la durée de la convention est fixée à 3 ans et reconductible 3 fois tacitement.

Budgétairement, le raccordement à l'ObSIS représente un coût nul pour le SDIS.
Fonctionnellement, il permettra de réduire, voire d'éviter, les lourdes tâches de reporting menées annuellement par les agents du service pour alimenter les enquêtes de la DGSCGC.

LE BUREAU DU CONSEIL D'ADMINISTRATION,

après en avoir délibéré, DÉCIDE à l'unanimité,

- d'autoriser le président à procéder au raccordement du SDIS du Tarn à l'ObSIS ;
- de valider le projet de convention en annexe ;
- d'autoriser le président à en modifier les termes et à la signer.

Document signé électroniquement par
le président du conseil d'administration,

Michel BENOIT

Délais et voies de recours :
La présente décision peut faire l'objet d'un recours devant le tribunal administratif, dans un délai de deux mois, à compter de sa date de notification ou de publication.
Le tribunal administratif de Toulouse peut être saisi par courrier (68, rue Raymond IV - BP 7007 - 31068 TOULOUSE CEDEX 7) ou par l'application informatique Télérecours, accessible par le lien : http://www.telerecours.fr

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

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

Observatoire des services d'incendie et de secours (ObSIS)

Convention de partenariat

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

SDIS TARN
Sapeurs-Pompiers

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

Entre

Le ministère de l'Intérieur et des outre-mer,
Sis place Beauvau, 75 008 Paris, représenté par le directeur général de la Sécurité civile et de la gestion des crises, M. Julien MARION
Ci-après désigné par la « DGSCGC », d'une part

et

Le service départemental d'incendie et de secours du TARN,
Sis 15, rue de Jautzou, 81012 ALBI CEDEX 09, représenté par son président du conseil d'administration, Monsieur Michel BENOIT, 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 :

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

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 et aux soins d'urgence.
- exercent, dans le cadre de leurs compétences, les missions suivantes :
    - La prévention et l'évaluation des risques de sécurité civile ;
    - La préparation des mesures de sauvegarde et l'organisation des moyens de secours ;
    - La protection des personnes, des animaux, des biens et de l'environnement ;
    - Le secours et les soins d'urgence aux personnes ainsi que leur évacuation, lorsqu'elles sont victimes d'accidents, de sinistres ou de catastrophes, présentent des signes de détresse vitale ou présentent des signes de détresse fonctionnelle justifiant l'urgence à agir.

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 :

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

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

Remontée des données

1 - Nature des données collectées

Le dictionnaire des données collectées est décrit en annexe 1. Aucune donnée nominative n'est stockée dans l'entrepôt national.

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. 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. Il en est de même pour les états-majors interministériels de zone (EMIZ).

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 précisés en annexe 3.

Article 3

Restriction et propriété intellectuelle

1 - 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.

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 (ObSIS) et la date à laquelle le jeu de données exposé est complet. 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.

2 - Autres restrictions

Aucune donnée nominative n'est remontée au niveau de la DGSCGC La pseudonymisation des données est faite localement sur l'environnement du SDIS 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.

3 - 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 :

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

- 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.

Envoyé en préfecture le 10/11/2023
Reçu en préfecture le 10/11/2023
Publié le
ID : 081-288100019-20231107-2023_062_BUR-DE

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
- Annexe 4 : Plan d'assurance sécurité et de protection des données personnelles (PASPDP)

Fait à

En deux exemplaires originaux, le

Le président du conseil d'administration du SDIS 81	Pour le ministre et par délégation, le directeur général de la Sécurité civile et de la gestion des crises
Michel BENOIT	Julien MARION

Annexe 1 – Nature des données collectées

Les données collectées depuis les SIS ne sont pas nominatives, et ne contiennent aucun champ de texte libre type commentaire ou observation.

1 - 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 technique pseudonymisé 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**
ID intervention	Identifiant technique
INSEE actuel	
INSEE original	
Lieu de l'intervention	Ramené à la commune
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 1ère alerte	
Date 1er engin SDIS sur les lieux	
Date fin intervention	

Flags ? Local à sommeil, cheminée, carence, …	

- Victimes

Donnée	**Exemple**
ID victime	Identifiant technique pseudonymisé avant envoi
ID inter	
Sexe	
Âge	
Victime SP intervenant	Oui/non
État victime fin d'intervention	Décédé, UA, UR, Impliqué
Établissement	
Transport vers établissement. de soin	

- Engins engagés

Donnée	**Exemple**
ID engin engagé	Identifiant technique
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 technique pseudonymisé avant envoi
ID engin engagé	
Centre	
Nomenclature type engin	
Nomenclature grade	Sauf Contrôleur général et colonel
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 technique pseudonymisé 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	

2 - Reprise et conservation des données

Reprise depuis le 01/01/2018
Durée de conservation : 10 ans. Cette durée est nécessaire afin de disposer de suffisamment d'historique pour faire de la prospective et pour consolider les tendances évolutives des indicateurs suivis.

3 - 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 250 Go 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 ; • 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

1 - Accès à distance

Le télédiagnostic 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 a 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.

2 - 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.

3 - 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.

4 - Contacts :

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

SDIS 81
Service
Prénom NOM téléphone
@sdis81.fr

Service
Prénom NOM téléphone
@sdis81.fr

DGSCGC
Responsable des opérations sur les données
Patrick ROUSSEL 01.72.71.66.76
dgscgc-obsis@interieur.gouv.fr

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

Annexe 4 – Plan d'assurance sécurité et de protection des données personnelles (PASPDP)

Objet du document

Le plan d'assurance sécurité et de protection des données personnelles (PASPDP) décrit l'ensemble des dispositions spécifiques que les parties s'engagent à mettre en œuvre pour répondre aux exigences de sécurité et de protection des données personnelles du SIS. Il définit en particulier l'organisation qui sera mise en place, la méthodologie à suivre pour gérer la sécurité du projet, la protection des données et les mesures techniques, organisationnelles et procédurales qui seront mises en œuvre.

Description du projet

Projet

Le projet d'Observatoire des services d'incendie et de secours (ObSIS) vise à collecter les données opérationnelles des SIS en un entrepôt national, supervisé par la Direction Générale de la Sécurité Civile et de la Gestion des Crises (DGSCGC)

Statut des parties

Le SDIS est responsable de traitement jusqu'à la mise à disposition des données pseudonymisées. La DGSCGC est responsable de traitement à partir des données pseudonymisées, de leur remontée dans l'ObSIS et jusqu'à leur exploitation.
Oxio-ciril group est sous-traitant pour la DGSCGC.

Opérations de traitement de données à caractère personnel.

Le prestataire Oxio-Ciril Group est autorisé à traiter pour le compte de la DGSCGC les données à caractère personnel nécessaires pour fournir les services suivants:

- La nature des opérations réalisées sur les données est la collecte des données, leur stockage et le calcul d'indicateurs.
- La finalité du traitement est le pilotage de l'activité de sécurité civile au moyen d'indicateurs standardisés et leur partage à l'ensemble des SIS via un outil de visualisation.
- Les données à caractère personnel traitées sont limitées :
  - (1) à celles relatives aux identifiants et courriels des utilisateurs de la plateforme. Leur durée de conservation ne pourra en aucun cas excéder celle nécessaire à l'exécution de ses services.
  - et (2) à celles qui sont intégrées au périmètre fonctionnel général détaillé en annexe 1 de la convention conclue entre la DGSCGC et les SDIS dans le cadre du projet ObSIS. Leur durée de conservation est fixée à un maximum de 10 ans.
- Les catégories de personnes concernées sont les utilisateurs de la plateforme ainsi que les sapeurs-pompiers et personnels administratifs et techniques du SIS et victimes prises en charges lors des opérations de secours.

Engagements de sécurité et de protection des données personnelles pour le prestataire mandaté par la DGSCGC

Cadre juridique

Article 1 - Règlement spécifique

Si, dans le cadre de la prestation contractée, une réglementation particulière (non mentionnée ci-dessus) s'applique ou lui est imposée ultérieurement à la signature de ce PASPDP et mettant en défaut le respect des exigences de sécurité et de protection des données personnelles du SIS, alors chaque partie doit :

- En informer les autres parties avant sa mise en œuvre effective,

- Montrer, s'ils existent, quels sont les moyens mis en œuvre pour maintenir le respect des exigences en regard des exigences fonctionnelles et techniques afférentes à cette réglementation.

Article 2 - Veille juridique

Le prestataire mandaté par la DGSCGC et la DGSCGC doivent avoir mis en place sur le périmètre de la prestation, une veille juridique leur permettant d'être constamment informés des évolutions légales et réglementaires susceptibles d'évoluer.

Article 3 - Localisation géographique des services et des données

Le prestataire mandaté par la DGSCGC s'engage, pour l'ensemble du périmètre de la prestation, à spécifier précisément les lieux géographiques dans lesquels les données informatiques du SIS sont amenées à être hébergées. De même, le prestataire mandaté par la DGSCGC précisera si ses infrastructures (techniques ou organisationnelles) sont gérées par une entité juridique appartenant à un pays de l'union européenne. Le prestataire mandaté par la DGSCGC s'engage à informer la DGSCGC sur tout changement de localisation des données.

Article 4 - - Opérateurs des données

Le prestataire mandaté par la DGSCGC peut faire appel à un sous-traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit la DGSCGC. Tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants devra également faire l'objet d'une information préalable par écrit de la DGSCGC. Cette information indiquera clairement les activités sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. La DGSCGC dispose d'un délai minium d'un mois à compter de la date de réception de cette information pour présenter ses objections. La sous-traitance ne peut être effectuée que si la DGSCGC n'émet aucune objection particulière à la sous-traitance envisagée dans un délai d'un mois. Dès lors que le prestataire mandaté par la DGSCGC a recours au service d'un sous-traitant préalablement autorisé par la DGSCGC, il s'engage à faire respecter au sous-traitant retenu par la voie contractuelle, les obligations prévues par la présente convention.

Au même titre que le prestataire mandaté par la DGSCGC initial, le sous-traitant est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de la DGSCGC. Il appartient au prestataire de s'assurer que son sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées. Si le sous-traitant ne remplit pas ses obligations, le prestataire mandaté par la DGSCGC demeure pleinement responsable devant la DGSCGC de l'exécution par le sous-traitant de ses obligations. Le PASPDP est donc applicable à l'ensemble des intervenants. En cas de non-respect des procédures ou des mesures prescrites, il doit en être référé immédiatement à la DGSCGC.

Organisation de la sécurité

Par dérogation aux éventuelles stipulations contraires de cet article, il est précisé que la DGSCGC est seule décisionnaire s'agissant de la sécurité et de la conformité du projet en matière de protection des données. Si le sous-traitant s'engage à l'assister de bonne foi dans ce cadre, le sous-traitant ne saurait cependant pas assumer la charge des obligations incombant à la DGSCGC en tant que responsable de traitement et de maître d'ouvrage du projet envisagé.

Article 5 - Rôle du responsable sécurité du prestataire

Obligations générales

Le prestataire dispose d'un responsable de la sécurité SI (RSSI) et d'un délégué à la protection des données (DPD).
Le prestataire mandaté par la DGSCGC peut, dans le cadre du marché de maintenance, avoir un rôle de conseil, de mise en garde et de recommandations en termes de sécurité de mise à l'état de l'art. Le prestataire mandaté par la DGSCGC informera préalablement la DGSCGC de toute opération susceptible de provoquer l'indisponibilité (ou une dégradation des performances) du système. Le prestataire mandaté par la DGSCGC est responsable du maintien en condition de sécurité du système qu'il héberge et infogère pendant toute la durée de la convention.
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.

Obligations spécifiques au Règlement Général sur la Protection des Données (RGPD)

Le prestataire mandaté par la DGSCGC s'engage à :

- Traiter les données à caractère personnel uniquement pour les seules finalités, explicitées à l'article 2 de la présente convention, qui font l'objet de la sous-traitance
- Traiter les données à caractère personnel conformément aux instructions documentées de la DGSCGC. Si le prestataire mandaté par la DGSCGC considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement.
- En outre le prestataire mandaté par la DGSCGC est tenu de ne procéder à aucun transfert de données vers un pays tiers ou à une organisation internationale.
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre de la présente convention
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu de la présente convention:
    - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
    - reçoivent la formation nécessaire en matière de protection des données à caractère personnel

Droit d'information des personnes concernées

Conformément aux articles 13 et 14 du RGPD, il appartient au SIS de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Exercice des droits des personnes concernées

Le prestataire mandaté par la DGSCGC doit aider la DGSCGC à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).
Lorsque les personnes concernées exercent auprès de la DGSCGC des demandes d'exercice de leurs droits, la DGSCGC doit adresser ces demandes dès réception par courrier électronique, si son assistance est nécessaire, au prestataire mandaté par la DGSCGC. Si le prestataire mandaté par la DGSCGC reçoit directement de telles demandes, il devra immédiatement les adresser par courrier électronique à l'adresse dgscgc-obsis@interieur.gouv.fr. Si la demande concerne une donnée pour laquelle le SIS est responsable de traitement, la DGSCGC en informe le SIS concerné.

Aide du prestataire dans le cadre du respect par le responsable de traitement de ses obligations

Le prestataire aide la DGSCGC pour la réalisation d'analyses d'impact relative à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle.

Notification des violations de données à caractère personnel

Le prestataire mandaté par la DGSCGC notifie sans délai au responsable de traitement par mail (dgscgc-obsis@interieur.gouv.fr) toute violation de données à caractère personnel après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. La notification contient au moins :

- La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- La description des conséquences probables de la violation de données à caractère personnel ;
- La description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

La DGSCGC en informe le SIS concerné, qui communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

Registre des catégories d'activités de traitement de données à caractère personnel

Le prestataire mandaté par la DGSCGC déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du SIS comprenant :

- Le nom et les coordonnées de son délégué à la protection des données
- Le nom et les coordonnées de ses éventuels sous-traitants
- Les catégories de traitements effectués et le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des

transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
- Une description générale des mesures de sécurité techniques et organisationnelles

Détection et alerte des incidents de sécurité

Le prestataire doit disposer, sur le périmètre de la prestation, d'un processus formalisé et opérationnel de gestion des incidents de sécurité qui lui permette de recueillir, d'analyser et d'alerter les parties ou participer au traitement de l'incident le cas échéant.

Article 6 - Arrivée et départ des collaborateurs du prestataire

Le prestataire mandaté par la DGSCGC s'engage à mettre à disposition une liste mise à jour des personnels autorisés à intervenir sur le système ainsi que leur niveau d'habilitation (type d'accès et ressources concernées).
L'arrivée impose la formation et la sensibilisation préalables ainsi que la signature de l'engagement de confidentialité de chacun de ses collaborateurs avant l'ouverture des droits.
Le départ impose la fermeture immédiate des droits. Une liste des sous-traitants précisant le type d'accès et les ressources autorisées sera également fournit sur demande.

Article 7 - Formation et sensibilisation du personnel du prestataire

Des séances de sensibilisation, au minima annuelles, seront conduites à l'ensemble des personnels du prestataire. La fréquence de ces séances devra également tenir compte de la progression des incidents, du contexte global mondial (cyber attaques de grandes envergure), ou de tout autre aspect qui le justifierait. Un rappel des règles élémentaires de sécurité doit être fait régulièrement, par tout moyen à disposition (message électronique généralisé sur un thème choisi ou sur un incident de sécurité, fiches réflexes, fiches de bonnes pratiques etc.).

Article 8 - Engagement de confidentialité

Les intervenants du prestataire, ainsi que les sous-traitants du prestataire s'il y a lieu, doivent être liés par un engagement de confidentialité avec leur employeur pendant toute la durée de l'exécution de la présente convention et après celle-ci. Cet engagement doit notamment mentionner :
- L'obligation du respect des règles de confidentialité du prestataire,
- La non-divulgation des informations accédées dans le cadre de sa mission,
- Le devoir de réserve,
- La prolongation de l'engagement au-delà de sa mission et/ou du départ du collaborateur de l'entreprise du prestataire.

Protection du système

Article 9 - Mesures techniques et organisationnelles spécifique au Règlement Général sur la Protection des Données (RGPD)

Le prestataire mandaté par la DGSCGC s'engage à mettre en œuvre les mesures de sécurité suivantes :

Description générale des mesures de sécurité techniques et organisationnelles	
Thématique	Mesure
Sensibiliser les utilisateurs	Les collaborateurs sont sensibilisés à la protection des données et à la sécurité des systèmes d'information.
	Une charte informatique à valeur contraignante est établie au sein de la société.
Authentifier les utilisateurs	Chaque collaborateur est identifié sur la base d'un identifiant unique et personnel.
	Les mots de passe des collaborateurs sont définis à partir d'une politique de mots de passe conforme aux recommandations de la CNIL.

	Les collaborateurs doivent modifier leurs mots de passe après réinitialisation.
	Le nombre de tentatives d'accès au compte de chaque collaborateur est limité.
	Les logiciels édités par la société permettent à leurs administrateurs de déterminer la politique de mots de passe qu'ils souhaitent appliquer à leurs utilisateurs.
Thématique	Mesure
Gérer les habilitations	Différentes profils d'habilitations sont définis pour chaque collaborateur en fonction des nécessités de ses missions.
	Les permissions d'accès obsolètes sont supprimées en cas de changement de poste ou de départ d'un collaborateur.
	Une revue annuelle des habilitations des collaborateurs est effectuée.
	Les logiciels édités par la société intègrent des fonctionnalités de détermination et de gestion des habilitations de leurs utilisateurs.
Tracer les accès et gérer les incidents	Des systèmes de journalisation sont déployés sur les différents systèmes de la société.
	Les collaborateurs sont informés des systèmes de journalisation déployés.
	Les accès aux journaux collectés sur les différents systèmes de la société sont contrôlés.
	Des procédures de gestion des incidents et de notification des violations sont établies au sein de la société.
Sécuriser les postes de travail	Un verrouillage automatique des sessions est activé sur les postes de la société.
	Les antivirus des postes de la société sont régulièrement mis à jour.
	Différents systèmes de pare-feux sont déployés au sein de la société.
	Les interventions de prise en main à distance sur les postes des collaborateurs requièrent leur accord.
Sécuriser l'informatique mobile	Les ordinateurs portables de la société sont chiffrés par Bitlocker .
	Un secret est exigé pour le déverrouillage des téléphones portables de la société.
Protéger le réseau informatique interne	Les flux des réseaux internes de la société sont limités au strict nécessaire.
	Les accès distants des appareils informatiques nomades de la société sont sécurisés par VPN.
	Les protocoles utilisés pour les réseaux Wi-Fi de la société sont sécurisés.
Sécuriser les serveurs	Les accès aux outils et interfaces d'administration des serveurs sont limités aux seuls collaborateurs habilités.
	Des outils de gestion des vulnérabilité et des mises à jour sont déployés au sein des principaux systèmes d'information de la société.
	Une politique de sauvegarde organise la sauvegarde des serveurs de la société.
Sécuriser les sites web	Les protocoles TLS 1.2 et 1.3 sont activés pour tous les sites de la société
	Des vérifications qu'aucun mot de passe ou identifiant ne transite dans les url des sites de la société sont effectuées.
	Des mécanismes de contrôles du format des entrées des utilisateurs sont déployés au sein des sites de la société.
	Des bandeaux de consentement pour les cookies non nécessaires au services sont déployés au sein des sites de la société.
Sauvegarder et prévoir la continuité d'activité	Des sauvegardes régulières des principaux systèmes d'information de la société sont organisées.
	Les sauvegardes sont stockées au sein des infrastructures principales et de secours de la société.
	Les sauvegardes transitant entre les infrastructures principales et de secours de la société sont chiffrées par le protocole AES 56 et transitent par l'intermédiaire de fibres dédiées.
	Des tests de restauration des sauvegardes de la société sont effectués régulièrement par échantillonnage.
	Des prestations de PRA et de sauvegarde, le cas échéant dupliquée et externalisée, peuvent être fournis aux clients de la société en fonction de leurs com-

	mandes.
Sécuriser les archives	Des habilitations particulières sont nécessaires pour accéder aux archives de la société.
	Les archives obsolètes de la société sont détruites de manière sécurisée.

Thématique	Mesure
Encadrer la maintenance et la destruction des données	Les opérations de maintenance sont consignées dans diverses main courantes.
	Les interventions de tiers sur les systèmes d'information de la société sont effectuées sous le contrôle d'un responsable.
	Des procédures de mise au rebut sécurisée des supports de données de la société sont établies.
	Les interventions de prise en main à distance réalisées via l'utilitaire de la société nécessitent l'accord préalable de l'utilisateur, qui peut y mettre fin à tout moment.
	Les interventions de prise en main à distance réalisées via l'utilitaire de la société permettent à l'utilisateur de les visualiser en temps réel.
	Les communications engendrées par l'utilisation de l'utilitaire de prise en main à distance de la société sont chiffrées de bout en bout.
Gérer la sous-traitance	Les contrats de la société avec ses sous-traitants intègrent les clauses imposées par la règlementation relative à la protection des données.
	Les contrats de la société avec ses sous-traitants intègrent les clauses requises en matière de restitution et, le cas échéant, de destruction des données.
	Des vérifications des garanties de sécurité des sous-traitants auxquels recourt la société sont effectuées.
Sécuriser les échanges avec d'autres organismes	Un espace de stockage temporaire de fichiers en https et ftps est mis à la disposition des collaborateurs afin d'effectuer des transferts de fichiers si nécessaire.
	Sauf fichier public, les utilisateurs et bénéficiaires de l'espace de stockage temporaire de la société doivent s'y authentifier afin d'y récupérer tout fichier.
	En cas de transmission d'un fichier chiffré par la société, son secret est communiqué par un envoi distinct et via un canal différent.
Protéger les locaux	Des portes verrouillées restreignent les accès aux locaux de la société.
	Des alarmes anti-intrusion sont installées dans les locaux de la société et testées périodiquement.
Encadrer les développements	Des étapes de vérifications en matière de sécurité et de protection des données sont intégrées aux processus de développement des logiciels de la société.
Utiliser le chiffrement	Les mots de passe des logiciels développés par la société sont hachés en base.
	Des systèmes de gestion de clés sont déployés au sein de la société.

Article 10 - Stockage des données

Le prestataire mandaté par la DGSCGC doit assurer la protection des données sensibles sur le système dans l'objectif principal de limiter le risque d'atteinte au système par une connaissance de son fonctionnement. Ces données sensibles comprennent notamment :

- Toutes les documentations sur l'architecture et son évolution,
- Les échanges avec le SIS et les autres clients du prestataire qui contiendraient des éléments de compréhension.

Cette protection doit s'appliquer aux zones de stockage de ces éléments, que ce soit des fichiers ou des messages.

Article 11 - Cloisonnement des données

Le prestataire mandaté par la DGSCGC s'engage, dans le cadre de la prestation, à mettre en place les moyens techniques et organisationnels pour couvrir les besoins de sécurité des données et notamment assurer que les informations traitées sur instruction de la DGSCGC ne sont en aucune façon accessibles ou visibles par les autres clients du prestataire. Même à des fins de tests ou de résolution d'incident, le prestataire mandaté par la DGSCGC s'engage à ne pas déplacer les données dans des environnements moins sécurisés, même s'il en a la maitrise.

Article 12 - Sécurité des sauvegardes

Le prestataire mandaté par la DGSCGC doit prendre toutes les mesures qui s'imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé, dans les limites des commandes passées à cet effet par la DGSCGC.
Cette sauvegarde doit permettre la restauration complète du système dans l'état sauvegardé sur un environnement matériel vierge. Doivent notamment, être sauvegardés : système d'exploitation, middleware, logiciels, paramétrage, données.

Article 13 - Destruction des données

Le prestataire mandaté par la DGSCGC doit disposer d'une procédure de destruction définitive (logique ou physique) des données qui ont été mises à sa disposition en dehors de l'environnement de production. Cette procédure comprend notamment :

- La destruction des données présentes sur tous les environnements utilisés, notamment les données de production lors de leur utilisation suite à incident ou pour tests,
- La destruction des données présentes sur des supports de sauvegardes, même si ceux-ci sont mutualisés.

Le prestataire mandaté par la DGSCGC doit fournir une attestation de destruction sur simple demande.

Sécurité des environnements

Article 14 - Protection contre les codes malveillants

Le prestataire mandaté par la DGSCGC s'engage dans le cadre de sa prestation, à installer des systèmes de protection contre les codes malveillants (virus, vers, chevaux de troye, spyware, keyloger…). Une politique antivirale stricte devra être notamment mise en place au niveau des postes de travail dont le prestataire mandaté par la DGSCGC a la charge. La mise à jour des signatures devra être automatique et d'une fréquence quotidienne. En cas d'alerte virale importante (alerte particulière de l'éditeur Antivirus) pouvant affecter le système, une mise à jour immédiate pourra être effectuée.
La politique antivirale appliquée sur le système devra être précisée (postes de travail des exploitants notamment). Le prestataire mandaté par la DGSCGC fournira une description des solutions antivirus, décrira la modalité et la fréquence de mise à jour du service. Un suivi de la mise à jour des signatures antivirales et des librairies associées sera effectué et tracé.

Article 15 - Mise à jour de la sécurité

Le prestataire mandaté par la DGSCGC applique les correctifs de sécurité recommandés par les fournisseurs de solutions matérielles ou logicielles après validation sur plateforme de test. En cas d'alerte grave (attaque virale, faille critique), le prestataire mandaté par la DGSCGC alertera la DGSCGC dans les meilleurs délais. Un plan d'actions est défini avec les parties afin de pallier la faille ou de se prémunir des risques exposés en attendant la validation de la solution de sécurité préconisée.

Sécurité des accès logiques

Article 16 - Gestion des identifiants

Sur le périmètre dédié à la prestation, le prestataire mandaté par la DGSCGC s'engage à mettre en place une politique de gestion des identifiants conforme aux bonnes pratiques, notamment l'utilisation d'identifiants nominatifs. Tous les comptes d'accès aux serveurs du prestataire doivent être individualisés. Les comptes d'accès partagés sont interdits.

Article 17 - Gestion des authentifications

Une politique de définition des mots de passe doit exister. Celle-ci doit préciser à minima :

- Une taille de mot de passe de 12 caractères
- Un niveau de complexité de type lettre + chiffre + symbole + minuscule + majuscule
- Une fréquence de changement de mot de passe de 365 jours

Article 18 - Gestion des flux d'authentification

L'utilisation de protocoles dont l'authentification est en clair est interdite. Sauf exception dûment justifiée par des obligations techniques et un niveau de risques maitrisé, les flux d'authentification doivent être chiffrés conformément à l'état de l'art. L'authentification des outils internes : accès VPN avec authentification à deux facteurs. L'authentification à ObSIS : page d'authentification chiffrée (https) et gestionnaire de compte centralisé assurant la traçabilité des connexions (KeyCloak).

Le prestataire mandaté par la DGSCGC indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux d'administration.

Sécurité des logiciels développés et intégrés

Article 19 - Audits de code

La DGSCGC pourra demander un audit de code auprès de la DGSCGC de l'application dans le respect de la propriété intellectuelle du prestataire ainsi que des politiques de sécurité et de confidentialité de celui-ci.

Article 20 - Mise à jour des logiciels

Le besoin de mise à jour des logiciels doit être détecté par le prestataire mandaté par la DGSCGC par la découverte de failles, par l'ajout de fonctionnalités, par l'évolution des composants et de l'environnement, par l'amélioration des performances, par l'obsolescence d'un composant (l'arrêt de la maintenance par son éditeur…). Le prestataire mandaté par la DGSCGC doit s'assurer en priorité que les versions en cours d'utilisation sont maintenues, et anticiper toute obsolescence de composant. La détection de faille sera également traitée de façon prioritaire. Une fois le besoin détecté, le prestataire doit proposer l'évolution à la DGSCGC dans le cadre du marché de maintenance.

Sécurité réseaux

Article 21 - Utilisation des protocoles sécurisés

L'utilisation de protocoles sécurisés contribue à la défense en profondeur. Les protocoles non sécurisés (telnet, FTP, POP, SMTP, HTTP, etc.) sont proscrits sur le système et remplacés par leurs équivalents sécurisés (SSH, SFTP, POPS, SMTPS, HTTPS, etc.).

Article 22 - Connexion d'équipements personnels

Les équipements personnels (tablettes, smartphones, lecteurs MP3, clés USB etc.) étant difficilement maitrisables, leur connexion est interdite sur système.

Article 23 - Protection contre les intrusions

Dans le cadre de la prestation, le prestataire mandaté par la DGSCGC mettra en œuvre les moyens nécessaires afin d'assurer que les informations mises à sa dispositions ou intégrées au service de la prestation, ne soient pas mises en péril ou inutilement exposées à des malveillances, cela se traduit par une sécurité logique périmétrique. Les règles de filtrage des pare-feu, sous la responsabilité du prestataire, sous le contrôle du RSSI de la DGSCGC doivent répondre au principe de « tout ce qui n'est pas explicitement autorisé est interdit ».

Gestion du changement

Toute intervention sur le système qui le modifie (patch de sécurité, montée de version…), que ce soit sur le matériel, le firmware, les middlewares ou les logiciels doit suivre un processus qui assure la sécurité et la sûreté de fonctionnement. En conséquence, les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité. En cas d'évolution, le prestataire mandaté par la DGSCGC devra vérifier que sa mise en œuvre est conforme aux exigences de la convention.

Sécurité physique

Article 24 - Bâtiments du prestataire

Les bâtiments du prestataire doivent être équipés d'un dispositif de contrôle d'accès individuel. Le mécanisme de contrôle d'accès mis en œuvre dans les bâtiments du prestataire doit être l'état de l'art afin d'assurer qu'il ne puisse pas être contourné aisément par un attaquant. Les lieux où sont localisées les données objet de la prestation doivent bénéficier de systèmes de protection contre les intrusions physiques.

Article 25 - Bâtiments du SIS

Les prestations réalisées dans les locaux du SIS appliquent les directives sécurité du SIS conformément aux réglementations en vigueur. Le SIS fourni les moyens nécessaires aux intervenants du prestataire pour accéder aux locaux (badges, clés si nécessaire, etc.). Lors du départ d'un intervenant, le chef de projet s'assure que les moyens fournis sont restitués au SIS.

Audit de sécurité

Article 26 - Audits externes

La DGSCGC doit pouvoir, à tout moment, contrôler que les exigences de sécurité et de protection des données personnelles sont satisfaites par les dispositions prises par le prestataire mandaté par la DGSCGC. En conséquence, la DGSCGC pourra demander un audit du système sur les aspects suivants :

- Tests d'intrusion avec accord du prestataire et sous responsabilité de la société ou personnels effectuant l'audit ainsi que de la DGSCGC,
- Conformité du présent PASPDP,
- Architecture et configuration du système,
- Audit du code avec accord du prestataire.

Le prestataire mandaté pour effectuer l'audit devra être qualifié « prestataires d'audit de la sécurité des systèmes d'information » (PASSI) par l'ANSSI. Le résultat de l'audit sera analysé conjointement et les manquements marqués conformes au présent PASPDP seront corrigés par le prestataire mandaté par la DGSCGC (Oxio-Ciril group) dans un délai négocié avec la DGSCGC.
La DGSCGC met à la disposition du SIS la documentation nécessaire pour démontrer le respect des obligations prévues à l'article 28 du RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) et pour permettre la réalisation d'audits et contribuer à ces audits.

Télémaintenance

Est considéré comme télémaintenance la connexion volontaire d'un personnel du prestataire via le lien VPN dédié à cet effet vers n'importe quel équipement (matériel actif, ordinateur, serveur etc.) du SIS. La télémaintenance ne doit pas impacter l'activité opérationnelle. En conséquence, toute intervention de télémaintenance doit être acceptée par le SIS avant exécution et tracée (ouverture, objet, étapes de la résolution, clôture).
Si l'intervention se fait à la demande du SIS, elle doit être formulée, ou accompagnée à minima d'un email, ou d'une déclaration d'incident a posteriori en cas d'accord oral préalable (astreinte). Une demande fait office d'autorisation de connexion et les étapes de la résolution y seront inscrites.

Si une intervention standard se fait à l'initiative du prestataire, elle doit être précédée à minima d'un email, et doit être acceptée formellement par le SIS avant d'être exécutée.
Si une intervention sur détection d'incident par le prestataire mandaté par la DGSCGC est nécessaire, elle doit faire l'objet d'une demande auprès du SIS, et en obtenir l'autorisation a minima verbale si urgence, et confirmé par email (éventuellement a posteriori en cas d'astreinte).

Organisation

En tant que maître d'œuvre, le prestataire mandaté par la DGSCGC désignera un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet, notamment la prise en compte et le suivi des exigences de sécurité et de protection des données du présent PASPD. Le prestataire mandaté par la DGSCGC reconnait être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. Cette obligation de conseil pourra être assurée par l'interlocuteur responsable de la sécurité.
Chacune des Parties désigne une personne qui est responsable du suivi du document. Il s'agit de :

- Pour la DGSCGC : olivier.euverte@interieur.gouv.fr
- Pour le Prestataire : fsimonin@cirilgroup.com

Responsabilité liées au PASPDP

Le PASPDP s'applique à l'ensemble des équipes de la maîtrise d'œuvre et aux sous-traitants éventuels. Sa bonne exécution est de la responsabilité du prestataire en tant que maître d'œuvre.

Modification du PASPDP

Des modifications peuvent être apportées au PASPDP, sous forme d'avenants, dans les cas d'évolutions significatives. Par exemple :

- Évolution du système d'information (configuration logicielle ou matérielle) ;
- Évolution de l'environnement du système d'information (locaux, personnels, procédures, etc.) ;
- Évolution du périmètre de la prestation

En cas d'évolution du système, de son environnement, ou du périmètre, le prestataire mandaté par la DGSCGC vérifie si le PASPDP doit être modifié. Si tel est le cas, il propose une modification à la DGSCGC. Si cette modification est acceptée, le PASPDP est révisé et soumis à la DGSCGC pour validation formelle. L'application d'éventuelles nouvelles exigences de sécurité prend effet dès la signature par les deux parties d'un avenant au présent PASPDP.
Toute modification unilatérale des présentes dispositions engage la responsabilité de la partie qui en est à l'origine, à l'égard de l'autre partie. Toute modification du présent document ne sera acceptée que si elle fait l'objet d'un accord écrit et signé par les représentants autorisés des parties.

Réversibilité

Le prestataire mandaté par la DGSCGC s'engage à apporter l'assistance nécessaire dans le cas où la DGSCGC déciderait de confier à un autre fournisseur la prestation. Le prestataire mandaté par la DGSCGC s'engage à garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations. La phase de réversibilité ne doit pas modifier la qualité, les termes, et les conditions des services fournis durant le contrat.
À la fin du contrat, le titulaire met en œuvre les processus visant à restituer à la DGSCGC :

- Les données, codes et documents que le titulaire héberge pour le compte de la DGSCGC.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du prestataire. Une fois détruites, le prestataire mandaté par la DGSCGC doit justifier par écrit de la destruction.