



CONVENTION D'EXPÉRIMENTATION

Solution FireGard de détection précoce des départs de feu

Commune de Portivechju – SIS2A – MidGard – Perseus



ENTRE LES SOUSSIGNÉS

La Commune de Portivechju, dont le siège est situé 5 Rue Fred Scamaroni, 20137 Porto-Vecchio, représentée par son Maire Jean-Christophe ANGELINI, dûment habilité aux fins des présentes, ci-après dénommée « la Commune » ou « le Porteur du projet »,

Le Service d'Incendie et de Secours de la Corse-du-Sud (SIS2A), dont le siège est situé 3 Av. Docteur Noël Franchini, 20090 Ajaccio, représenté par sa Présidente Véronique ARRIGHI, dûment habilitée aux fins des présentes, ci-après dénommé « le SIS2A »,

La société MidGard SAS, dont le siège social est situé 2 boulevard Charles Bonaparte, 20090 Ajaccio, représentée par Madame Anne-Sophie Cadre, Présidente, ou tout représentant dûment habilité, ci-après dénommée « MidGard »,

La société Perseus, dont le siège social est situé port de Toga a Vela 20200 Bastia représentée par son Directeur Général, Stanislas Finocchi, dûment habilitée aux fins des présentes, ci-après dénommée « Perseus »,

Ci-après individuellement une « Partie » et collectivement les « Parties ».

PRÉAMBULE

La Commune souhaite expérimenter sur son territoire la solution FireGard, développée par MidGard, afin d'évaluer l'apport d'un dispositif de détection précoce des départs de feu et de visualisation d'images dans des conditions proches du réel.

Le SIS2A a donné un accord de principe à l'accueil de cette expérimentation, sous réserve notamment que le dispositif n'affecte pas ses missions opérationnelles, que l'exploitation quotidienne des images et des alertes ne soit pas la responsabilité du CTA-CODIS, que les contraintes d'implantation, de systèmes d'information, de cybersécurité et de conformité réglementaire soient respectées, et que les responsabilités de chacune des Parties soient explicitement définies.

MidGard, éditeur de la solution FireGard, a confirmé sa volonté d'accompagner la Commune et le SIS2A dans cette démarche expérimentale. Dans ce cadre, MidGard met à disposition la solution FireGard et assure l'accompagnement applicatif associé pendant la période d'expérimentation de six (6) mois. Cet accompagnement est réalisé à titre gracieux pour la Commune et le SIS2A, dans le périmètre défini par la présente convention et ses annexes.

Perseus, prestataire technique chargé des opérations d'installation associées au dispositif, a confirmé sa volonté d'accompagner la Commune et le SIS2A dans cette démarche expérimentale. Dans ce cadre, Perseus assure, dans son périmètre, la préparation technique et l'installation du dispositif. Cet accompagnement est également réalisé à titre gracieux pour la Commune et le SIS2A, dans le périmètre défini par la présente convention et ses annexes.

La présente convention n'emporte aucune modification des compétences légales respectives des parties et ne constitue pas une délégation de service public.

ARTICLE 1 – OBJET DE LA CONVENTION

La présente convention a pour objet de définir les conditions juridiques dans lesquelles est conduite l'expérimentation de la solution FireGard à Portivechju, ainsi que les rôles et responsabilités respectifs de la Commune, du SIS2A, de MidGard et de Perseus.

Elle encadre notamment l'installation et la mise en service du dispositif, l'exploitation de la solution pendant la période d'essai, les modalités d'accès aux images, le traitement des alertes, la sécurité des systèmes d'information, la protection des données, la maintenance, le suivi de l'expérimentation et les conditions de clôture.

ARTICLE 2 – PÉRIMÈTRE DE L'EXPÉRIMENTATION

Le périmètre prévisionnel de l'expérimentation comprend :

- l'installation d'une caméra de marque Axis sur un emplacement à valider au sein de la caserne de Portivechju ;
- la mise à disposition et le paramétrage de la plateforme FireGard ;
- la récupération sécurisée du flux vidéo de la caméra par FireGard ;
- la détection automatisée de fumées ou événements susceptibles de correspondre à un départ de feu ;
- la visualisation du flux et des événements par les utilisateurs habilités ;
- la réception et la consultation, à seules fins d'évaluation, des signalements générés par FireGard par les participants autorisés, sans obligation de surveillance permanente ni de traitement opérationnel ;
- la mise en place d'un accès sécurisé aux images et aux fonctions de contrôle de la caméra pour les seules personnes habilitées ;
- la formation des utilisateurs désignés, dispensée par Perseus dès l'achèvement de l'installation du système expérimental ;
- le suivi des performances et la réalisation d'un retour d'expérience en fin de période.

ARTICLE 3 – DURÉE ET CALENDRIER

L'expérimentation est prévue pour une durée de six (6) mois à compter de la date de mise en service opérationnelle, constatée par un procès-verbal de recette ou tout document équivalent validé par les Parties concernées.

Toute prolongation au-delà des six mois fera l'objet d'un accord écrit entre les Parties, formalisé par avenant ou par tout acte écrit juridiquement valable convenu entre elles.

ARTICLE 4 – DÉROULÉ DE L'EXPÉRIMENTATION

L'expérimentation est organisée en cinq phases principales :

- **Cadrage et préparation** : validation du périmètre, des interlocuteurs, de l'implantation, de l'architecture réseau, des modalités de réception des signalements, de prise de contrôle de la caméra et du cadre juridique/RGPD.
- **Installation et intégration** : préparation du site, pose et raccordement de la caméra, configuration de la transmission du flux vidéo et intégration à FireGard.
- **Recette et formation** : tests techniques et fonctionnels, vérification des accès, tests d'alertes, validation des habilitations et formation des utilisateurs dès que l'installation du système expérimental est terminée.
- **Exploitation expérimentale pendant six mois** : utilisation de FireGard par les personnels habilités à des fins d'évaluation, sans organisation d'une surveillance permanente, collecte d'indicateurs, suivi des incidents et ajustements autorisés.
- **Clôture et retour d'expérience** : analyse des résultats, bilan partagé, restitution des enseignements et décision éventuelle sur les suites à donner

ARTICLE 5 – GOUVERNANCE ET INTERLOCUTEURS

Pour assurer le pilotage et le bon déroulement de l'expérimentation, chaque Partie désigne un référent projet principal, chargé de coordonner les actions relevant de son périmètre et d'assurer le lien avec les autres Parties.

Les référents projet désignés à la date de signature de la présente convention sont :

- pour la commune de Portivechju : Olivier PORTAZ, Chargé de mission risques majeurs ;
- pour le SIS2A : Commandant Paul TAFANI, Chef du groupement territorial Sud ;
- pour MidGard : Anne-Sophie Cadre, Présidente de MidGard ;
- pour Perseus : Stanislas Finocchi, Directeur General de Perseus ;

Chaque Partie peut également désigner des référents techniques, opérationnels, SI, cybersécurité ou juridiques en fonction des sujets traités.

Tout changement de référent est communiqué sans délai aux autres Parties, sans qu'il soit nécessaire de modifier la présente convention par avenant.

Un comité de suivi de l'expérimentation est mis en place dès la signature de la présente convention. Il constitue l'instance principale de pilotage du projet.

Il se réunit :

- toutes les deux semaines pendant les phases de préparation, d'installation et de mise en service ;
- une fois par mois pendant les six (6) mois d'exploitation expérimentale ;
- et, en tant que de besoin, à la demande de l'une des Parties lorsqu'un sujet technique, opérationnel, juridique ou de sécurité nécessite une coordination spécifique.

Convention d'expérimentation FireGard

Le comité de suivi réunit, a minima, les référents projet des Parties. Les interlocuteurs techniques, opérationnels, systèmes d'information, juridiques ou tout autre expert utile, peuvent être associés en fonction de l'ordre du jour.

Le comité de suivi est notamment chargé de :

- suivre l'avancement global de l'expérimentation et le respect du calendrier ;
- piloter la levée des prérequis techniques, opérationnels, SI, cybersécurité et juridiques ;
- suivre les actions décidées, leurs responsables et leurs échéances ;
- examiner les incidents, difficultés ou risques susceptibles d'affecter l'expérimentation ;
- décider et suivre la mise en œuvre des actions correctives ou ajustements nécessaires ;
- suivre les indicateurs de performance et critères de succès définis pour l'expérimentation ;
- partager les retours d'usage des utilisateurs et identifier les éventuels besoins d'évolution ;
- préparer et valider les éléments nécessaires au bilan et au retour d'expérience final.

À l'issue de chaque comité de suivi, un relevé de décisions et un plan d'actions sont établis par MidGard et partagés avec l'ensemble des Parties. Ils précisent notamment les actions à mener, leur responsable, leur échéance et leur statut d'avancement.

ARTICLE 6 – RÔLES ET OBLIGATIONS DES PARTIES

Commune de Portivechju – Porteur du projet

La Commune, en qualité de Porteur du projet, s'engage notamment à :

- coordonner l'expérimentation avec MidGard, le SIS2A et Perseus ;
- s'assurer de l'obtention des autorisations administratives, domaniales, techniques et réglementaires nécessaires à l'installation et à l'exploitation du dispositif ;
- désigner, avec le référent du SIS2A, les personnes autorisées à recevoir et consulter les signalements générés par FireGard à seules fins d'évaluation, sans leur confier une mission de surveillance permanente ni une obligation de traitement opérationnel ;
- organiser les accès au site et veiller au respect des consignes de sécurité et des contraintes opérationnelles du SIS2A ;
- s'assurer du respect de la réglementation applicable à la captation et au traitement des images et des données à caractère personnel ;
- participer au suivi des indicateurs et au retour d'expérience final.

MidGard

MidGard s'engage notamment à :

- mettre à disposition la solution FireGard pour la durée de l'expérimentation selon les modalités convenues avec la Commune ;
- assurer l'intégration du flux de la caméra à FireGard, sous réserve de la disponibilité et de la conformité des accès et flux nécessaires ;
- participer à la définition et à la mise en œuvre de l'architecture technique de récupération du flux vidéo ;
- configurer les comptes, profils et habilitations selon les règles validées par les Parties ;
- organiser, pour les fonctionnalités propres à FireGard, la formation des utilisateurs désignés ;

Convention d'expérimentation FireGard

- assurer le support et la maintenance applicative de FireGard pendant l'expérimentation, selon les modalités définies en annexe ;
- signaler dans les meilleurs délais les incidents significatifs affectant la disponibilité, l'intégrité ou la sécurité de la solution ;
- participer au suivi des performances et fournir, à l'issue de l'expérimentation, un rapport de synthèse comprenant notamment les événements détectés, les performances observées, les faux positifs identifiés et les pistes d'amélioration.

FireGard étant utilisé dans un cadre expérimental, MidGard ne garantit pas la détection exhaustive de tout départ de feu. La solution constitue un outil d'aide à la détection et à la décision et ne se substitue ni aux dispositifs réglementaires d'alerte, ni aux procédures opérationnelles de secours, ni à l'appréciation humaine.

Perseus

Perseus s'engage notamment à :

- préparer et réaliser, dans son périmètre technique, l'installation et le raccordement des équipements qui lui sont confiés ou qu'il apporte à l'expérimentation ;
- réaliser ses interventions techniques dans le respect des règles de l'art, des consignes du site et des validations préalables des Parties concernées ;
- assurer, pour les matériels et interventions relevant de son périmètre, le support technique convenu pendant l'expérimentation ;
- signaler dans les meilleurs délais tout incident ou anomalie significative constaté dans le cadre de ses interventions.

SIS2A

Le SIS2A s'engage, dans les limites de ses missions, de ses moyens et des réserves exprimées dans la présente convention, à :

- faciliter l'accès au site pour les opérations préalablement autorisées et coordonnées, sous réserve des contraintes opérationnelles du centre ;
- participer aux ateliers nécessaires à la validation de l'implantation et, le cas échéant, de l'architecture SI lorsqu'une connexion à ses réseaux serait envisagée ;
- désigner les interlocuteurs nécessaires pour le suivi du projet ;
- préciser les modalités selon lesquelles un accès ponctuel et sécurisé aux images pourrait être mis à disposition de certains personnels habilités ;
- participer, selon ses disponibilités, au retour d'expérience sur l'intérêt opérationnel du dispositif.

Il est expressément convenu que le SIS2A n'assure pas la veille continue, la surveillance permanente des images, l'exploitation quotidienne de FireGard, la détection des événements ni le traitement courant des alertes générées par le dispositif. Cette absence d'obligation de surveillance vaut également pour la Commune, MidGard, Perseus et, plus généralement, pour l'ensemble des participants autorisés à l'expérimentation : aucune Partie ni aucun participant n'est tenu d'assurer une permanence de surveillance, pendant ou en dehors des heures ouvrables.

ARTICLE 7 – CHAÎNE OPÉRATIONNELLE ET TRAITEMENT DES ALERTES

Le présent article précise les modalités opérationnelles applicables pendant toute la durée de l'expérimentation. Elles ont pour seul objet d'organiser les conditions de test et d'évaluation du dispositif, sans créer d'obligation de surveillance permanente ni modifier les procédures habituelles d'alerte et de secours. À ce titre, il définit les principes relatifs à la surveillance, à la réception des signalements, à la réaction en cas de départ de feu réel, à la prise de contrôle de la caméra et à la formation des utilisateurs.

Surveillance

Pendant toute la durée de l'expérimentation, aucune responsabilité de surveillance, et notamment aucune obligation de permanence de la surveillance, n'est mise à la charge des Parties ou des participants autorisés. Ni le SIS2A ni la Commune ne sont, à la date de signature, en capacité de confier cette responsabilité à une structure permanente de surveillance. Aucune garantie de surveillance continue n'est donc apportée, que ce soit pendant les heures ouvrables ou en dehors de celles-ci.

Réception des signalements

Les signalements de départs de feu détectés par FireGard peuvent être reçus et consultés, uniquement à des fins d'évaluation de l'expérimentation, par les personnes autorisées par les référents du SIS2A et de la Commune. La réception d'un signalement n'emporte, pour son destinataire, ni prise en charge d'une mission de surveillance, ni obligation de permanence, ni obligation de traitement opérationnel autre que celle prévue ci-après en cas de constat d'un départ de feu réel.

Les personnes habilitées peuvent notamment recevoir des notifications sur mobile et consulter l'interface web FireGard selon leur profil. Ces outils constituent des moyens d'évaluation du système et ne créent aucune obligation de consultation immédiate, de levée de doute systématique ou de disponibilité continue.

Réaction à un départ de feu réel

Lorsqu'un départ de feu réel est constaté ou apparaît suffisamment caractérisé à partir d'un signalement FireGard, la seule réaction attendue au titre de la présente expérimentation est l'appel au numéro d'urgence 18, de la même manière que pour tout départ de feu repéré par la police municipale, la gendarmerie, les équipes du SIS2A, les services techniques, une collectivité ou tout autre témoin. À compter de cet appel, le SIS2A apprécie la situation et décide de l'engagement et de la coordination des moyens de secours selon ses procédures propres.

Prise de contrôle de la caméra

Les fonctions de prise de contrôle de la caméra sont accessibles au moyen de profils « administrateur », « gestionnaire » et « opérateur » aux seules personnes autorisées par les référents du SIS2A et de la Commune.

- En situation de départ de feu réel, la priorité de prise de contrôle de la caméra revient au SIS2A, lorsqu'un personnel habilité est disponible pour l'exercer ;
- pendant la première phase de l'expérimentation, la caméra est configurée pour un balayage à 360°, à raison d'environ six (6) minutes par rotation ;
- dans une phase ultérieure, ce balayage a vocation à être réduit à 180°, à raison d'environ trois (3) minutes par rotation, afin de se rapprocher de la configuration susceptible d'être déployée à terme sur chaque site.

Les modalités ci-dessus constituent le fonctionnement de référence de l'expérimentation. Elles peuvent être ajustées par le comité de suivi pour les seuls besoins de l'évaluation, sans qu'un tel ajustement puisse avoir pour effet de créer une obligation de surveillance permanente ou de transférer aux participants une responsabilité opérationnelle de détection ou de traitement des incendies.

ARTICLE 8 – PROTECTION DES DONNÉES, IMAGES ET RGPD

Principes

Les Parties s'engagent à respecter la réglementation applicable à la protection des données à caractère personnel, notamment le règlement (UE) 2016/679 (RGPD) et la loi n° 78-17 du 6 janvier 1978. Elles respectent aussi, le cas échéant, les dispositions du code de la sécurité intérieure sur la captation d'images. Le dispositif est vidéo et son champ de vision peut inclure des personnes, les images sont donc susceptibles de contenir des données à caractère personnel.

Qualification des Parties

Pour le traitement mis en œuvre dans le cadre de l'expérimentation :

- la Commune en est le responsable de traitement : elle en détermine les finalités et les moyens essentiels ;
- MidGard en est le sous-traitant au sens de l'article 28 du RGPD. Elle traite les données uniquement pour le compte de la Commune et sur ses instructions documentées, pour la mise à disposition, l'hébergement, l'analyse automatisée, le paramétrage, le support et la maintenance de FireGard ;
- le SIS2A n'intervient ni comme responsable conjoint ni comme sous-traitant de ce traitement. Ses personnels habilités qui accèdent ponctuellement aux images sont des destinataires. Ils accèdent aux images selon les modalités définies par la Commune et respectent les règles de confidentialité et de traçabilité prévues au présent article. Les informations transmises au CODIS selon les procédures habituelles relèvent ensuite des traitements propres au SIS2A, dont il est seul responsable.

Rattachement des clauses de protection des données

Les obligations de MidGard en qualité de sous-traitant sont définies dans l'annexe « Clauses de protection des données – contrat de sous-traitance RGPD », conclue entre la Commune et MidGard. Cette annexe est ci-après dénommée « l'Annexe RGPD ».

- Valeur contractuelle : l'Annexe RGPD fait partie intégrante de la présente convention. Elle est signée par la Commune et MidGard, seules parties à cette annexe.
- Contenu : elle précise notamment :
 - L'objet, la nature, les finalités et la durée du traitement ;
 - Les catégories de données et de personnes concernées ;
 - Les durées de conservation ;
 - Les mesures de sécurité ;
 - Les sous-traitants ultérieurs autorisés ;
 - Les modalités d'assistance, de notification des violations de données et de restitution ou de suppression des données.
- Ordre de priorité : en cas de contradiction, l'Annexe RGPD prévaut, pour tout ce qui concerne la protection des données, sur les stipulations de la présente convention et sur tout document émanant de MidGard (conditions générales, conditions d'utilisation, politique de confidentialité).
- Modifications : l'Annexe RGPD peut être mise à jour par accord écrit entre la Commune et MidGard, sans avenant à la présente convention, à condition que ces mises à jour n'aient pas d'effet sur les obligations du SIS2A.

Conditions préalables à la mise en service

La mise en service opérationnelle mentionnée à l'article 3 ne peut intervenir qu'après :

- la signature de l'Annexe RGPD ;
- l'inscription du traitement au registre des activités de traitement de la Commune ;
- la réalisation de l'analyse d'impact relative à la protection des données, si elle est requise ;
- l'obtention des autorisations administratives nécessaires à la captation d'images, notamment l'autorisation préfectorale si le champ de la caméra couvre la voie publique ou des lieux ouverts au public ;
- la mise en place de l'information des personnes concernées.

La Commune coordonne ces démarches avec son délégué à la protection des données. MidGard lui fournit, dans les délais prévus à l'Annexe RGPD, les informations techniques nécessaires.

Limitation des finalités et des usages

Les images et les données à caractère personnel ne peuvent être utilisées que pour les finalités de l'expérimentation définies dans l'Annexe RGPD. Leur durée de conservation est limitée au strict nécessaire et fixée par cette annexe. Les accès sont réservés aux personnes nominativement habilitées et sont tracés.

Convention d'expérimentation FireGard

Sont interdits, sauf validation juridique préalable de la Commune, base légale appropriée et garanties spécifiques formalisées par écrit :

- Toute utilisation des images à des fins de communication, de démonstration, de recherche ou commerciales ;
- Tout entraînement ou amélioration de modèles d'intelligence artificielle avec ces données à caractère personnel ;
- Toute utilisation pour une finalité différente de l'expérimentation.

Sont interdits dans tous les cas : tout traitement biométrique, toute reconnaissance faciale et toute utilisation du dispositif pour surveiller des personnes.

Autres intervenants

Si un tiers intervenant sur le dispositif (notamment Perseus) accède aux données :

- S'il intervient pour le compte de MidGard, il ne peut le faire que comme sous-traitant ultérieur autorisé, selon les conditions de l'Annexe RGPD ;
- S'il intervient directement pour le compte de la Commune, il doit conclure avec elle un contrat conforme à l'article 28 du RGPD.

Sort des données et durée des engagements

À la fin de l'expérimentation ou en cas de résiliation anticipée, les données à caractère personnel sont restituées ou supprimées selon les modalités et délais prévus à l'Annexe RGPD. MidGard remet alors une attestation écrite. Les obligations du présent article et de l'Annexe RGPD restent en vigueur jusqu'à la suppression ou la restitution effective de toutes les données à caractère personnel, y compris chez les sous-traitants ultérieurs.

ARTICLE 9 – MAINTENANCE, SUPPORT ET DISPONIBILITÉ

MidGard assure la maintenance applicative et le support de FireGard selon les modalités convenues avec la Commune. Perseus assure, dans le périmètre de ses propres matériels et interventions techniques, le support qui lui incombe au titre de la présente convention. Les incidents susceptibles d'affecter la continuité de l'expérimentation font l'objet d'un suivi partagé.

L'expérimentation n'emporte aucune garantie de disponibilité permanente. Une indisponibilité du dispositif ne saurait avoir pour effet de transférer à l'une quelconque des Parties une obligation de surveillance supplétive, de permanence ou de mobilisation de moyens spécifiques pour compenser cette indisponibilité.

ARTICLE 10 – RESPONSABILITÉS

Chaque Partie demeure responsable de l'exécution de ses obligations propres au titre de la présente convention, dans le périmètre placé sous son contrôle.

Matériels apportés par les Parties

Chaque Partie est responsable des matériels, équipements, logiciels ou accessoires qu'elle apporte ou met à disposition pour les besoins de l'expérimentation, notamment quant à leur conformité, leur installation lorsqu'elle lui incombe, leur garde, leur entretien, leur maintenance et leur retrait, sous réserve des obligations expressément confiées à une autre Partie.

Interventions techniques

Chaque Partie intervenant techniquement sur le système est responsable de la bonne exécution de ses propres actions et interventions, notamment de préparation, installation, raccordement, paramétrage, intégration, maintenance ou modification, dans la limite de son périmètre d'intervention. Elle répond des conséquences directement imputables à une faute ou à un manquement dans l'exécution de ces interventions.

Absence d'obligation de surveillance et départ de feu réel

Aucune Partie, ni aucun participant autorisé à l'expérimentation, n'assume au titre de la présente convention une obligation de surveillance permanente, de consultation continue des images ou notifications, de détection exhaustive, de levée de doute systématique ou de traitement opérationnel des alertes.

En conséquence, sous réserve des dispositions d'ordre public et des responsabilités pouvant résulter d'une faute directement imputable à une Partie dans l'exécution de ses propres obligations, aucune Partie ni aucun participant autorisé ne pourra voir sa responsabilité engagée du seul fait de la survenance ou de l'évolution d'un incendie réel, d'une absence ou d'un retard de détection, d'une absence de consultation d'un signalement, ou de l'absence de permanence de surveillance dans le cadre de l'expérimentation.

Décisions opérationnelles de secours

Lorsqu'un événement est signalé par un appel au 18, le SIS2A conserve l'entière maîtrise de l'appréciation opérationnelle, de la décision d'engagement des moyens et de la conduite des opérations de secours. Les informations issues de FireGard constituent des éléments d'aide à l'appréciation et ne sauraient lier la décision du SIS2A.

Responsabilité de MidGard et de Perseus

MidGard est responsable de l'exécution de ses obligations propres relatives notamment au paramétrage, à l'intégration et au support applicatif de FireGard, dans les limites du périmètre technique placé sous son contrôle. Perseus est responsable de l'exécution de ses obligations propres relatives notamment aux opérations techniques d'installation, de raccordement et, à ses matériels éventuels. Ni MidGard ni Perseus ne répondent d'un dysfonctionnement imputable à un équipement, une alimentation, une liaison réseau, un service tiers ou une intervention hors de leur contrôle respectif, sous réserve de leurs obligations d'alerte et de coopération.

La Commune demeure responsable de l'obtention des autorisations et du respect de la réglementation relevant de son périmètre, notamment en matière d'images et de données à caractère personnel. L'accueil du dispositif sur un site du SIS2A et la participation de ses personnels à l'expérimentation n'importent aucun transfert au SIS2A des responsabilités techniques ou organisationnelles incombant aux autres Parties.

ARTICLE 11 – CONDITIONS FINANCIÈRES

La présente expérimentation est réalisée à titre gracieux pour la Commune de Portivechju et le SIS2A pendant toute la durée de l'expérimentation prévue par la présente convention. MidGard et Perseus interviennent dans les conditions définies ci-après.

À ce titre :

- la mise à disposition de la solution FireGard par MidGard pendant la période d'expérimentation ne donne lieu à aucune facturation ;
- l'accompagnement de MidGard relatif au paramétrage, à la mise en service applicative, au support et au suivi de l'expérimentation est réalisé à titre gracieux dans le périmètre défini par la présente convention ;
- l'accompagnement de Perseus pour la préparation technique et l'installation du dispositif est également réalisé à titre gracieux dans le périmètre convenu entre les Parties ;
- aucune obligation financière n'est mise à la charge du SIS2A au titre de l'acquisition, de l'installation, de l'exploitation, de la maintenance ou du support du dispositif dans le cadre de cette expérimentation.

Toute prestation, fourniture, travaux ou intervention qui sortirait du périmètre de l'expérimentation défini dans la présente convention devra faire l'objet d'un accord préalable et distinct entre les parties concernées.

La présente expérimentation n'emporte enfin aucun engagement d'achat, de contractualisation ou de déploiement ultérieur de la solution FireGard à l'issue de la période de test.

ARTICLE 12 – CONFIDENTIALITÉ

Les Parties s'engagent à préserver la confidentialité des informations techniques, opérationnelles, de sécurité, organisationnelles ou commerciales identifiées comme confidentielles ou dont la nature justifie raisonnablement un traitement confidentiel.

Cette obligation ne fait pas obstacle aux obligations légales de communication des documents administratifs, aux demandes des autorités compétentes ni aux obligations réglementaires propres à chaque Partie.

ARTICLE 13 – PROPRIÉTÉ INTELLECTUELLE ET DROIT D'USAGE

La solution FireGard, ses logiciels, algorithmes, modèles, interfaces, documentations et éléments préexistants restent la propriété de MidGard ou de leurs titulaires respectifs.

Pour les seuls besoins de l'expérimentation, les utilisateurs habilités bénéficient d'un droit d'usage personnel, non exclusif, non transférable et limité à la durée et au périmètre de l'expérimentation.

La présente convention n'emporte aucune cession de droits de propriété intellectuelle entre les Parties.

ARTICLE 14 – COMMUNICATION

Toute communication externe nominative relative à l'expérimentation, incluant l'utilisation du nom, du logo ou de l'image d'une autre Partie, est soumise à son accord préalable, sauf obligation légale ou communication institutionnelle préalablement convenue.

ARTICLE 15 – SUSPENSION ET RÉSILIATION

Le SIS2A peut demander la suspension immédiate de tout ou partie du dispositif lorsque la sécurité des personnes, la continuité de ses missions, les contraintes opérationnelles du centre, la cybersécurité ou l'intégrité de ses installations le justifient. Les Parties se concertent alors afin de déterminer les conditions d'une éventuelle reprise.

Chaque Partie peut résilier la présente convention, sans indemnité, moyennant un préavis écrit de quinze (15) jours. En cas de risque grave pour la sécurité, de manquement substantiel non corrigé ou d'exigence d'une autorité compétente, la suspension ou la résiliation peut prendre effet sans délai.

À l'issue de l'expérimentation ou en cas de résiliation anticipée, les Parties organisent la désactivation des accès, la restitution ou le retrait des matériels concernés par leur propriétaire ou la Partie qui en a la charge, ainsi que le traitement des données conformément aux règles de conservation et de suppression définies dans l'annexe RGPD.

Sauf accord distinct, la fin de l'expérimentation n'emporte aucun droit au maintien de FireGard, à l'accès aux services ou à la conservation des équipements sur le site.

SIGNATURES

Fait à _____, le _____

en 4 exemplaires originaux ou par signature électronique.

Pour la Commune de Portivechju	Pour le SIS2A	Pour MidGard SAS	Pour Perseus
Jean-Christophe ANGELINI	Véronique ARRIGHI	Anne-Sophie CADRE	Stanislas FINOCCHI
Maire	Présidente	Présidente	Directeur General
Signature :	Signature :	Signature :	Signature :

ANNEXE

CLAUSES DE PROTECTION DES DONNÉES

CONTRAT DE SOUS-TRAITANCE RGPD

Expérimentation de la solution FireGard – détection précoce des départs de feu

ENTRE LES SOUSSIGNÉES :

La **Commune de Porto-Vecchio (Portivechju)**, collectivité territoriale, enregistrée sous le numéro SIREN 212 002 471 et ayant son siège social en l'Hôtel de Ville, 5 rue Fred Scamaroni, 20137 Porto-Vecchio, représentée par Monsieur Jean-Christophe ANGELINI en sa qualité de Maire, dûment habilité aux fins des présentes par délibération n° _____ du _____, ayant tous pouvoirs pour les besoins des présentes.

Ci-après dénommée « **le Client** » ou le « **Responsable de traitement** »,

D'UNE PART,

ET

La société **MIDGARD**, société par actions simplifiée (SAS), immatriculée au registre du commerce et des sociétés d'Ajaccio sous le numéro 851 642 280, ayant son siège social c/o Inizià, Port de l'Amirauté, boulevard Charles Bonaparte, 20000 Ajaccio, représentée par Madame Anne-Sophie CADRE, en sa qualité de Présidente, ayant tous pouvoirs pour les besoins des présentes.

Ci-après désignée par le « **Prestataire** » ou le « **Sous-traitant** »,

D'AUTRE PART,

Ci-après désignées ensemble les « **Parties** ».

EXPOSÉ

La Commune de Porto-Vecchio, le Service d'Incendie et de Secours de la Corse-du-Sud (SIS2A) et MidGard ont conclu une convention d'expérimentation de la solution FireGard de détection précoce des départs de feu, pour une période d'exploitation de six (6) mois à compter de la mise en service opérationnelle (ci-après le « **Contrat** »). Dans ce cadre, MidGard met à disposition la plateforme FireGard, récupère et analyse de manière automatisée le flux vidéo d'une caméra installée sur la caserne de Porto-Vecchio, génère des alertes et assure le paramétrage, la formation, le support et la maintenance applicative de la solution. Les images captées étant susceptibles de contenir des données à caractère personnel, MidGard agit, pour ces opérations, **pour le compte** de la Commune, en qualité de sous-traitant au sens de l'article 4.8 du RGPD.

Les présentes clauses RGPD constituent l'« annexe RGPD » visée aux articles 8 et 15 du Contrat. Elles viennent se greffer au Contrat conclu entre les Parties et ont pour objet de garantir leur conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Table des matières

SECTION I – DÉFINITIONS ET CHAMP D'APPLICATION	3
ARTICLE 1 – DÉFINITIONS	3
ARTICLE 2 – OBJET ET CHAMP D'APPLICATION	3
ARTICLE 3 – INVARIABILITÉ DES CLAUSES & INTERPRÉTATION	4
SECTION II – OBLIGATIONS DES PARTIES	5
ARTICLE 4 – OBLIGATIONS DES PARTIES	5
ARTICLE 5 – ASSISTANCE AU RESPONSABLE DE TRAITEMENT	8
ARTICLE 6 – NOTIFICATION DE VIOLATIONS DE DONNÉES	9
SECTION III – DISPOSITIONS FINALES	10
ARTICLE 7 – NON-RESPECT DES CLAUSES ET RÉSILIATION	10
ARTICLE 8 – LOI APPLICABLE ET COMPÉTENCE JURIDICTIONNELLE	11
ANNEXE I – LISTE DES PARTIES	12
ANNEXE II – DESCRIPTION DU TRAITEMENT	13
ANNEXE III – MESURES TECHNIQUES ET ORGANISATIONNELLES	15
ANNEXE IV – LISTE DES SOUS-TRAITANTS ULTÉRIEURS	18

Légende : les mentions surlignées en vert sont à compléter ou à valider par le Responsable de traitement ; les mentions surlignées en jaune sont à compléter ou à confirmer par le Sous-traitant avant signature.

SECTION I – DÉFINITIONS ET CHAMP D'APPLICATION

ARTICLE 1 – DÉFINITIONS

Les termes et expressions ci-dessous auront, pour l'application et l'interprétation des présentes clauses, lorsque leur première lettre apparaît en majuscule, la signification qui leur est assignée ci-après :

- « **RGPD** » désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit « Règlement Général sur la Protection des Données », entré en vigueur le 25 mai 2016 et applicable depuis le 25 mai 2018.
- « **LIL** » désigne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite également « loi Informatique et Libertés ».
- « **Législation applicable** » désigne l'ensemble constitué de la LIL et du RGPD, ainsi que, pour les dispositifs de captation d'images, les dispositions applicables du code de la sécurité intérieure.
- « **Contrat** » désigne la convention d'expérimentation de la solution FireGard conclue entre la Commune de Porto-Vecchio, le SIS2A et MidGard, ses annexes et avenants éventuels.
- « **Solution** » ou « **FireGard** » désigne la plateforme logicielle de détection précoce des départs de feu éditée par MidGard, comprenant notamment les modules d'analyse automatisée par intelligence artificielle, l'interface web et les notifications associées.
- « **Donnée à caractère personnel** » ou « **Données** » désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, comme par exemple un nom, un prénom, une image ou une vidéo, un numéro de plaque d'immatriculation, un identifiant de connexion ou une adresse IP.
- « **Personne concernée** » désigne la personne à laquelle se rapportent les données qui font l'objet du Traitement.
- « **Traitement de données à caractère personnel** » ou « **Traitement** » désigne toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, l'effacement ou la destruction.
- « **Finalité** » désigne l'objectif poursuivi par le Traitement, autrement dit les raisons pour lesquelles les données sont collectées.
- « **Responsable de traitement (ou « RT »)** » désigne la personne physique ou morale, autorité publique, service ou tout autre organisme qui détermine les finalités et les moyens du Traitement.
- « **Sous-traitant (ou « ST »)** » désigne la personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
- « **CNIL** » désigne la Commission Nationale de l'Informatique et des Libertés.
- « **Destinataire des données** » désigne la personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication de Données à caractère personnel, qu'il s'agisse ou non d'un tiers.
- « **DPO** » (de l'anglais « Data Protection Officer ») désigne le délégué à la protection des données, institué par les articles 37 et suivants du RGPD.

ARTICLE 2 – OBJET ET CHAMP D'APPLICATION

Le responsable du traitement et le sous-traitant énumérés à l'annexe I ont accepté ces clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679.

- Les présentes clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II, réalisé par le sous-traitant pour le compte du responsable du traitement dans le cadre du Contrat.
- Les annexes I à IV font partie intégrante des clauses.
- Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679.
- Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et seront complétées par de nouvelles dispositions, le cas échéant.
- En cas de contradiction entre les présentes clauses et les stipulations du Contrat (notamment ses articles 8, 10, 12 et 15) ou tout autre document émanant du sous-traitant (conditions générales, conditions d'utilisation, politique de confidentialité), les présentes clauses prévalent pour tout ce qui concerne la protection des données à caractère personnel.
- Le SIS2A, partie au Contrat, n'est pas partie aux présentes clauses. Lorsque des personnels habilités du SIS2A accèdent aux images ou reçoivent des informations issues de FireGard, ils agissent en qualité de destinataires, selon les modalités définies par le responsable du traitement.

ARTICLE 3 – INVARIABILITÉ DES CLAUSES & INTERPRÉTATION

Les parties s'engagent à ne pas modifier les clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent. Les parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Lorsque des termes définis dans le règlement (UE) 2016/679 figurent dans les clauses, ils s'entendent comme dans ce règlement.

Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679.

Les présentes clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

SECTION II – OBLIGATIONS DES PARTIES

ARTICLE 4 – OBLIGATIONS DES PARTIES

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'annexe II.

4.1. Instructions

Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

Le responsable du traitement s'engage à documenter par écrit toute instruction relative au traitement des données. Constituent notamment des instructions documentées : les présentes clauses et leurs annexes, les règles de gestion des comptes, profils et habilitations validées par la Commune, le protocole opérationnel de traitement des alertes, ainsi que les relevés de décisions du comité de suivi établis par MidGard dès lors qu'ils ont été validés par écrit par le référent de la Commune.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

4.2. Limitation de la finalité

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'annexe II, sauf instruction complémentaire du responsable du traitement.

Il est expressément convenu que le sous-traitant s'interdit, sauf instruction écrite préalable du responsable du traitement assortie d'un cadre juridique distinct :

- toute réutilisation des images, séquences ou métadonnées à caractère personnel à des fins d'entraînement, de ré-entraînement, d'amélioration ou d'évaluation de ses modèles d'intelligence artificielle au-delà du seul paramétrage de la Solution pour le site expérimenté ;
- toute utilisation à des fins de communication, de démonstration, de recherche ou commerciales ;
- toute mise en œuvre de traitement biométrique, de reconnaissance faciale, de suivi ou d'identification de personnes ;
- toute utilisation du dispositif à des fins de vidéoprotection, de surveillance de personnes ou de constatation d'infractions. Toute réutilisation non autorisée ferait du sous-traitant un responsable de traitement au sens de l'article 28, paragraphe 10, du RGPD.

4.3. Durée du traitement des données à caractère personnel

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'annexe II. Pendant cette durée, le sous-traitant applique les durées de conservation fixées par le responsable du traitement et précisées à l'annexe II, et purge automatiquement les données à caractère personnel à l'expiration de ces durées. Au terme du Contrat, quelle qu'en

Convention d'expérimentation FireGard

soit la cause (échéance, résiliation anticipée ou suspension définitive), le Prestataire s'engage, au choix du Client et dans un délai maximal de trente (30) jours, à :

- Détruire toutes les Données à caractère personnel ou
- Renvoyer toutes les Données à caractère personnel au Client, dans un format structuré, couramment utilisé et lisible par machine, ou
- Transférer les Données à caractère personnel au tiers désigné par le Client.

Le renvoi ou le transfert doit s'accompagner de la destruction de toutes les copies existantes des Données dans les systèmes d'information du Prestataire et de ses sous-traitants ultérieurs, y compris les sauvegardes, à l'expiration de leur cycle de rotation. Une fois détruites, le Prestataire doit justifier par écrit de cette destruction au Client, au moyen d'une attestation de suppression précisant la nature des données, les systèmes concernés et la date de l'opération. Le caractère gracieux de l'expérimentation ne saurait en aucun cas conditionner, limiter ou retarder la restitution ou la destruction des Données.

4.4. Sécurité du traitement

Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel).

Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.

Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel 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 et que ces engagements soient formalisés par écrit (clause de confidentialité du contrat de travail ou engagement spécifique).

Le sous-traitant prend en compte, s'agissant de la Solution, les principes de protection des données dès la conception et par défaut (article 25 du RGPD) : paramétrage par défaut le plus protecteur (champ de vision limité aux zones utiles à la détection, masquage des zones privatives lorsque techniquement possible, absence d'enregistrement continu du flux hors alerte, comptes nominatifs et profils limités au besoin d'en connaître), minimisation du contenu des notifications et traçabilité des accès.

Le sous-traitant tient par écrit, conformément à l'article 30, paragraphe 2, du RGPD, un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant a minima : le nom et les coordonnées du sous-traitant, du responsable du traitement et, le cas échéant, de leurs DPO ; les catégories de traitements effectués pour le compte du responsable du traitement ; le cas échéant, les transferts vers un pays tiers et les garanties appropriées ; une description générale des mesures de sécurité techniques et organisationnelles. Ce registre est communiqué au responsable du traitement sur simple demande.

Le sous-traitant aide et conseille le responsable du traitement pour la sécurité des traitements. Il l'informe sans délai de toute vulnérabilité, évolution technique ou modification de la Solution susceptible d'avoir une incidence sur la sécurité ou la conformité du traitement. Le sous-traitant s'engage également à respecter, pour les accès et

interconnexions réalisés sur les systèmes du responsable du traitement ou du SIS2A, les règles de sécurité qui lui auront été communiquées par écrit.

4.5. Données sensibles

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions (« données sensibles »), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

Le traitement n'a pas pour objet de collecter de telles données. Les images captées pouvant néanmoins, de manière incidente, en révéler certaines, les limitations et garanties décrites à l'annexe II s'appliquent.

4.6. Documentation et conformité

Les parties doivent pouvoir démontrer la conformité avec les présentes clauses.

Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes clauses.

Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement du règlement (UE) 2016/679, et notamment, sur simple demande : le document d'architecture technique (DAT) de la Solution et de la chaîne de récupération du flux vidéo, sa politique de sécurité des systèmes d'information (PSSI) ou tout document équivalent, son plan d'assurance sécurité (PAS), ses plans de continuité et de reprise d'activité (PCA/PRA), ses certifications et attestations éventuelles, ainsi qu'une documentation décrivant le fonctionnement général des algorithmes de détection (logique de détection, données d'entrée, indicateurs de performance, taux de faux positifs observés), sans que cette obligation n'emporte communication du code source protégé au titre de la propriété intellectuelle. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant, tenu à une obligation de confidentialité. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

Les parties mettent à la disposition de l'autorité de contrôle compétente, dès que celle-ci en fait la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

4.7. Recours à des sous-traitants ultérieurs

AUTORISATION ÉCRITE GÉNÉRALE :

Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base de la liste convenue figurant à l'annexe IV. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs dans un délai de 15 jours avant le recrutement envisagé, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour

Convention d'expérimentation FireGard

lui permettre d'exercer son droit d'opposition (identité, localisation des traitements, prestations confiées, garanties offertes, transferts éventuels hors de l'Union européenne).

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679.

À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle, dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

4.8. Transferts internationaux

Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du règlement (UE) 2016/679.

Le sous-traitant informe préalablement et par écrit le responsable du traitement de tout transfert, y compris par voie d'accès à distance (maintenance, support, supervision), de données vers un pays situé hors de l'Espace économique européen ou vers une organisation internationale, en précisant le pays concerné, le mécanisme de transfert utilisé (décision d'adéquation, notamment le cadre de protection des données UE–États-Unis, ou clauses contractuelles types) et les mesures supplémentaires mises en œuvre. Les données vidéo (flux, séquences et captures d'images) sont hébergées et traitées exclusivement au sein de l'Union européenne.

Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la clause 4.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'article 46, paragraphe 2, du règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

ARTICLE 5 – ASSISTANCE AU RESPONSABLE DE TRAITEMENT

Le sous-traitant informe sans délai, et au plus tard dans un délai de quarante-huit (48) heures ouvrées, le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée par le biais de l'adresse de contact suivante : dpd@portivechju.corsica. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du

Convention d'expérimentation FireGard

traitement des données ne l'y ait autorisé par écrit ; dans ce cas, le sous-traitant répond au nom et pour le compte du responsable du traitement, dans les délais et selon les modalités fixés par ce dernier.

Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits (droit d'accès, de rectification, d'effacement, à la limitation du traitement, d'opposition, à la portabilité le cas échéant, droit de ne pas faire l'objet d'une décision individuelle automatisée, et droit de définir des directives relatives au sort des données après le décès), en tenant compte de la nature du traitement, notamment en permettant la recherche, l'extraction, le floutage de tiers et, le cas échéant, l'effacement des séquences concernées. Dans l'exécution de ses obligations, le sous-traitant se conforme aux instructions du responsable du traitement.

Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement, le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

- L'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel (« analyse d'impact relative à la protection des données ») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques ; à ce titre, le sous-traitant fournit, dans un délai de quinze (15) jours à compter de la demande, la description technique de la Solution, de ses flux et de ses mesures de sécurité ;
- L'obligation de consulter l'autorité de contrôle compétente préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ;
- L'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes ;
- Les obligations prévues à l'article 32 du règlement (UE) 2016/679 ;
- Les parties définissent à l'annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise.

ARTICLE 6 – NOTIFICATION DE VIOLATIONS DE DONNÉES

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du règlement (UE) 2016/679, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant. Le Prestataire s'engage à notifier au Client toute violation de Données dans un délai maximum de **24 heures** après en avoir eu connaissance par le biais de l'adresse de contact suivante : dpd@portivechju.corsica, avec copie au référent projet de la Commune désigné à l'annexe I. Cette notification écrite est doublée, en cas de violation susceptible d'engendrer un risque élevé, d'un appel téléphonique au référent projet de la Commune.

6.1. Violation de données en rapport avec des données traitées par le responsable de traitement

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

- Aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas

Convention d'expérimentation FireGard

échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques) ;

- Aux fins de l'obtention des informations suivantes qui, conformément à l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :
 - La nature des 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 ;
 - Les conséquences probables de la violation de données à caractère personnel ;
 - Les mesures prises ou les mesures 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.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

- Aux fins de la satisfaction, conformément à l'article 34 du règlement (UE) 2016/679, de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Cette communication décrit, en des termes clairs et simples, la nature de la violation et contient au moins le nom et les coordonnées du DPO, les conséquences probables de la violation et les mesures prises ou envisagées pour y remédier. Le sous-traitant ne procède lui-même à cette communication qu'après accord écrit préalable du responsable du traitement et selon ses instructions.

6.2. Violation de données en rapport avec des données traitées par le sous-traitant

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance, et en tout état de cause dans le délai de 24 heures fixé au présent article. Cette notification contient au moins :

- Une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés) ;
- Les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel ;
- Les conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Le sous-traitant ne notifie pas lui-même la violation à la CNIL, sauf instruction écrite contraire du responsable du traitement. Il documente toute violation (faits, effets, mesures prises) et tient cette documentation à la disposition du responsable du traitement.

SECTION III – DISPOSITIONS FINALES

ARTICLE 7 – NON-RESPECT DES CLAUSES ET RÉSILIATION

Sans préjudice des dispositions du règlement (UE) 2016/679, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit. Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

- Le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au premier alinéa du présent article et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
- Le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 ;
- Le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679.

Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la clause 4.1, le responsable du traitement insiste pour que ses instructions soient suivies. À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

Les limitations de responsabilité stipulées au Contrat (notamment à son article 10) ne sauraient faire obstacle à la responsabilité du sous-traitant telle qu'elle résulte de l'article 82 du RGPD, lorsqu'il n'a pas respecté les obligations qui lui incombent spécifiquement ou qu'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Convention d'expérimentation FireGard

ARTICLE 8 – LOI APPLICABLE ET COMPÉTENCE JURIDICTIONNELLE

Le présent contrat est régi par le droit français. Il doit être appliqué et interprété conformément à ce droit. En cas de litige, et après recherche d'une solution amiable, le tribunal compétent pour en statuer est le **tribunal administratif de Bastia**.

Paraphe sur chaque page, y compris les pages en annexe,

Fait en deux exemplaires originaux ou par signature électronique, à Porto-Vecchio, le

Le Responsable de traitement :

Commune de Porto-Vecchio (Portivechju) ;
Représentée légalement par :
Jean-Christophe ANGELINI, Maire

Signature et cachet :

olivier

Le Sous-traitant :

MIDGARD SAS ;
Représentée légalement par :
Anne-Sophie CADRE, Présidente

Signature et cachet :

Convention d'expérimentation FireGard

ANNEXE I – LISTE DES PARTIES

Responsable du traitement :

Nom	Commune de Porto-Vecchio (Portivechju) – SIREN 212 002 471 – SIRET 212 002 471 00010
Adresse	Hôtel de Ville, 5 rue Fred Scamaroni, 20137 Porto-Vecchio
Représentant légal	Jean-Christophe ANGELINI, Maire
Délégué à la protection des données	Délégué à la protection des données de la Commune – dpd@portivechju.corsica – Mairie de Porto-Vecchio, DPD, BP A129, 20537 Porto-Vecchio Cedex – Tél. : 04 95 70 95 30
Nom, fonction et coordonnées de la personne de contact	Olivier PORTAZ, Chargé de mission Risques majeurs, référent projet – olivier.portaz@portivechju.corsica – Tel. : 04 95 70 91 66
Signature et date d'adhésion	

Sous-traitant :

Nom	MIDGARD – SAS – RCS Ajaccio 851 642 280 – SIRET 851 642 280 00024 – NAF 62.01Z
Adresse	c/o Inizià, Port de l'Amirauté, boulevard Charles Bonaparte, 20000 Ajaccio
Représentant légal	Anne-Sophie CADRE, Présidente
Délégué à la protection des données	Anne-Sophie CADRE
Nom, fonction et coordonnées de la personne de contact	Anne-Sophie CADRE, Présidente, référente projet – anne-sophie.cadre@midgard-ai.com – +33 6 59 31 85 03
Contact sécurité / violations de données	anne-sophie.cadre@midgard-ai.com +33 6 59 31 85 03
Signature et date d'adhésion	

ANNEXE II – DESCRIPTION DU TRAITEMENT

Catégories de personnes concernées dont les données à caractère personnel sont traitées :

- Personnes physiques présentes ou circulant dans le champ de la caméra (promeneurs, randonneurs, riverains, touristes, conducteurs et passagers de véhicules, exploitants agricoles ou forestiers, intervenants sur site), y compris, le cas échéant, des mineurs ;
- Personnels et visiteurs du centre d'incendie et de secours de Porto-Vecchio se trouvant, le cas échéant, dans le champ de la caméra ;
- Utilisateurs habilités de FireGard : opérateurs locaux et agents désignés par la Commune, personnels habilités du SIS2A bénéficiant d'un accès ponctuel ;
- Référents et membres du comité de suivi, participants aux formations et interlocuteurs du support.

Catégories de données à caractère personnel traitées :

- **Images et vidéos** : flux vidéo en direct de la caméra, séquences et captures d'images associées aux détections et alertes, susceptibles de faire apparaître des silhouettes, visages, véhicules, plaques d'immatriculation ou abords d'habitations ;
- **Métadonnées de détection** : horodatage, orientation de la caméra, géolocalisation estimée de l'événement, score de confiance, statut de qualification de l'alerte (faux positif, levée de doute, transmission au CODIS) ;
- **Données d'identification des utilisateurs** : nom, prénom, fonction, service de rattachement, adresse électronique professionnelle, numéro de téléphone mobile professionnel, identifiant de compte (dont identifiant Slack) ;
- **Données de connexion et de traçabilité** : identifiants, profils et habilitations, journaux de connexion, de consultation, d'export et d'actions de qualification, adresses IP, type de terminal ;
- **Données de suivi du projet** : relevés de décisions, listes d'émargement des formations, échanges de support.

Les données sensibles traitées (le cas échéant) et les limitations ou garanties appliquées :

Aucune donnée sensible n'est intentionnellement collectée. Les images peuvent toutefois révéler de manière incidente des informations sensibles (par exemple l'état de santé apparent d'une personne ou sa présence dans un lieu). Garanties appliquées :

- Interdiction de tout traitement biométrique, de reconnaissance faciale, de lecture automatisée de plaques d'immatriculation, de suivi ou d'identification de personnes ;
- Orientation et cadrage de la caméra limités aux zones utiles à la détection de fumées ; masquage des zones privatives (habitations, jardins, cours) lorsque techniquement possible ;
- Accès aux images réservé aux personnes nominativement habilitées et formées, avec journalisation des accès et des exports ;
- Interdiction de toute extraction, copie ou diffusion des images hors du cadre de la levée de doute ou d'une réquisition d'une autorité compétente ;
- Absence de réutilisation des images à caractère personnel pour l'entraînement des modèles ou toute autre finalité (clause 4.2) ; hébergement des données vidéo au sein de l'Union européenne clause 4.8).

Convention d'expérimentation FireGard

Nature du traitement :

- Récupération sécurisée et transmission du flux vidéo de la caméra (marque Axis) installée sur la caserne de Porto-Vecchio vers la plateforme FireGard ;
- Analyse automatisée du flux par des algorithmes d'intelligence artificielle (détection de fumées et d'événements susceptibles de correspondre à un départ de feu), géolocalisation de l'événement ;
- Génération d'alertes, conservation des séquences et captures associées, et mise à disposition via l'interface web FireGard ;
- Envoi de notifications aux opérateurs habilités (notifications Slack sur PC de la commune) ;
- Création et gestion des comptes, profils et habilitations ; journalisation des accès ;
- Hébergement, sauvegarde, support et maintenance applicative (y compris accès ponctuels aux données pour résolution d'incidents) ;
- Formation des utilisateurs, suivi des performances et production d'un rapport de synthèse de fin d'expérimentation (données agrégées, images anonymisées ou floutées le cas échéant) ;
- Restitution et/ou suppression des données au terme de l'expérimentation.

Finalité(s) pour laquelle (lesquelles) les données à caractère personnel sont traitées pour le compte du responsable du traitement :

- Détection précoce des départs de feu sur le territoire communal et aide à la qualification et à la levée de doute des alertes par les opérateurs locaux, dans le cadre des missions de prévention des incendies relevant de la police municipale (article L. 2212-2, 5°, du code général des collectivités territoriales) – base légale : exécution d'une mission d'intérêt public (article 6.1.e du RGPD) ;
- Transmission de l'information au CODIS du SIS2A lorsque l'événement présente un caractère opérationnel ;
- Évaluation de l'expérimentation : suivi des indicateurs de performance, analyse des faux positifs, retour d'expérience ;
- Gestion des accès, sécurité et traçabilité de la Solution ; support et maintenance.

Sont exclues : la vidéoprotection et la surveillance des personnes, la constatation d'infractions, l'identification de personnes, l'entraînement ou l'amélioration des modèles d'IA de MidGard, ainsi que toute utilisation à des fins de communication, de démonstration ou commerciales.

Durée du traitement :

Durée du Contrat : phases de cadrage, d'installation et de recette, puis exploitation expérimentale de six (6) mois à compter de la date de mise en service opérationnelle constatée par procès-verbal de recette prolongeable uniquement par accord écrit ; suivie de la phase de restitution/suppression des données dans un délai maximal de trente (30) jours (clause 4.3).

Durées de conservation fixées par le responsable du traitement:

Catégorie de données	Durée de conservation
Flux vidéo ne donnant lieu à aucune détection	Aucun enregistrement : traitement en mémoire le temps strictement nécessaire à l'analyse
Séquences et captures associées à une alerte	30 jours maximum à compter de l'alerte, sauf extraction sur instruction de la Commune pour transmission à une autorité compétente (conservation alors limitée à la durée de la procédure)

Convention d'expérimentation FireGard

Catégorie de données	Durée de conservation
Métadonnées de détection (sans image)	Durée de l'expérimentation, pour les besoins du retour d'expérience ; anonymisation dans le rapport de synthèse
Journaux de connexion et de traçabilité	6 mois glissants (recommandation CNIL relative à la journalisation)
Comptes utilisateurs	Désactivation à la fin de l'habilitation ; suppression au terme du Contrat
Rapport de synthèse	Remis à la Commune ; ne contient pas de données personnelles identifiantes

Pour le traitement par les sous-traitants (ultérieurs), préciser également l'objet, la nature et la durée du traitement : voir l'annexe IV. La durée du traitement par les sous-traitants ultérieurs n'excède pas celle du Contrat.

ANNEXE III – MESURES TECHNIQUES ET ORGANISATIONNELLES

Description des mesures de sécurité techniques et organisationnelles mises en œuvre par le ou les sous-traitants (y compris toute certification pertinente) visant à garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Le tableau ci-dessous fixe les exigences minimales du responsable du traitement. Le sous-traitant décrit, de manière concrète et non générique, la mesure effectivement mise en œuvre en regard de chaque exigence avant la mise en service.

Domaine	Exigence minimale du responsable du traitement	Mesure mise en œuvre par MidGard
Hébergement	Hébergement des données (flux, séquences, métadonnées, sauvegardes) au sein de l'Union européenne, chez un hébergeur présentant des garanties reconnues (certification ISO/IEC 27001 ; qualification SecNumCloud appréciée).	MidGard héberge la plateforme FireGard sur ses propres serveurs, installés dans le centre de données Français Azur Datacenter AZ01, situé à Croissy-Beaubourg, en Seine-et-Marne, France, au sein de l'Union européenne. L'exploitant détient une certification ISO 27001 pour ce site. Le centre dispose d'une architecture Tier3+, d'alimentations électriques et de systèmes de refroidissement redondants, ainsi que de dispositifs de contrôle d'accès, de vidéosurveillance et de protection incendie.
Chiffrement	Chiffrement du flux vidéo en transit entre la caméra et la plateforme (tunnel VPN ou TLS 1.2 minimum) ; chiffrement des données au repos (AES-256 ou équivalent) ; gestion sécurisée des clés.	Les échanges avec la plateforme FireGard sont chiffrés en transit via HTTPS afin de protéger la confidentialité et l'intégrité des données transmises. Le flux vidéo entre la caméra et la plateforme est acheminé à travers un tunnel VPN, qui protège les communications contre leur interception et leur consultation par des tiers non autorisés.
Pseudonymisation et minimisation	Absence d'enregistrement continu hors alerte ; masquage des zones privatives ; contenu des notifications Slack limité aux informations nécessaires à la pré-qualification (horodatage, localisation estimée, vignette d'image de résolution réduite) ; floutage des personnes dans le rapport de synthèse.	MidGard limite les données traitées aux informations nécessaires à la détection et à la pré-qualification des départs de feu. Le flux vidéo est analysé sans enregistrement continu hors alerte ; seules les séquences et captures associées aux alertes sont conservées, selon les durées définies à l'annexe II. Les zones privatives présentes dans le champ de la caméra font l'objet d'un masquage. Les notifications Slack sont limitées à l'horodatage, à la localisation estimée de l'événement et à une vignette d'image de résolution réduite, nécessaires à la pré-qualification de l'alerte. Les personnes apparaissant sur les images intégrées au rapport de synthèse sont floutées afin de limiter les possibilités d'identification.
Identification et autorisation	Comptes nominatifs, sans compte générique partagé ; authentification forte (MFA) pour l'interface web et les accès d'administration ; profils d'accès fondés sur le besoin d'en connaître, validés par la Commune ; revue des habilitations à chaque comité de suivi	Les utilisateurs disposent de comptes nominatifs assortis de droits d'accès différenciés selon leurs fonctions et leurs besoins opérationnels. Les profils d'accès sont définis selon le principe du besoin d'en connaître et validés par la Commune, afin de limiter l'accès de chaque utilisateur aux seules données et fonctionnalités nécessaires à sa mission.

Convention d'expérimentation FireGard

Domaine	Exigence minimale du responsable du traitement	Mesure mise en œuvre par MidGard
	mensuel ; révocation sans délai des accès en fin de mission.	Les habilitations sont revues à chaque comité de suivi mensuel afin de vérifier leur adéquation avec les missions des utilisateurs. Les accès sont révoqués sans délai en fin de mission.
Journalisation	Traçabilité des connexions, consultations, exports et actions de qualification ; conservation des journaux 6 mois ; mise à disposition des journaux à la Commune sur demande.	MidGard assure la journalisation des connexions, des consultations de données, des exports et des actions de qualification des alertes réalisés sur la plateforme FireGard. Ces journaux permettent de retracer les opérations effectuées par les utilisateurs habilités. Ils sont conservés pendant six (6) mois glissants et mis à la disposition de la Commune sur demande.
Sécurité de la caméra et du réseau	Durcissement de la caméra (changement des identifiants par défaut, mises à jour du micrologiciel, désactivation des services inutiles) ; cloisonnement du flux vis-à-vis des réseaux du SIS2A ; aucune interconnexion avec les réseaux du SIS2A sans validation préalable de son service SI.	La caméra fait l'objet de mesures de durcissement comprenant le remplacement des identifiants par défaut, la mise à jour du micrologiciel et la désactivation des services inutiles. Un tunnel VPN est mis en place entre la caméra et l'infrastructure MidGard afin de sécuriser la transmission du flux vidéo. Le flux vidéo est cloisonné vis-à-vis des réseaux du SIS2A. Toute interconnexion avec ces réseaux est soumise à la validation préalable du service des systèmes d'information du SIS2A.
Confidentialité, intégrité, disponibilité, résilience	Architecture redondée ou procédure de reprise documentée ; surveillance de la disponibilité ; information de la Commune en cas d'indisponibilité ; PCA/PRA communiqués sur demande (objectifs de reprise à préciser).	La plateforme FireGard repose sur une architecture Kubernetes permettant le redémarrage automatique des composants applicatifs en cas de défaillance. Un mécanisme de retour à une version antérieure (rollback) est également disponible afin de rétablir une version précédente de l'application en cas de dysfonctionnement lié à un déploiement.
Tests et évaluation	Tests de sécurité avant mise en service (recette) ; gestion des vulnérabilités et application des correctifs ; revue au moins annuelle des mesures ; test d'intrusion ou audit de sécurité de la plateforme (résultats de synthèse communicables).	MidGard réalise des tests de sécurité avant la mise en service de la plateforme FireGard, dans le cadre de la recette. Les vulnérabilités identifiées font l'objet d'un suivi et de l'application de correctifs adaptés. Les mesures de sécurité sont revues au moins une fois par an afin d'évaluer leur adéquation et de déterminer les améliorations nécessaires.
Sécurité physique	Sécurité physique des centres de données (contrôle d'accès, protection incendie) ; protection de la caméra et du boîtier contre l'accès non autorisé sur site.	Les serveurs de MidGard sont hébergés dans le centre de données Azur Datacenter AZ01, qui dispose d'un gardiennage 24 h/24, de dispositifs de vidéosurveillance et de contrôle d'accès par badge et biométrie, ainsi que de systèmes de détection et d'extinction incendie. La caméra et son boîtier sont installés sur un site sécurisé par le SIS2A, qui assure la protection des lieux contre les accès non autorisés.
Gouvernance de la sécurité	PSSI ou document équivalent ; PAS ; DAT de la Solution et de la chaîne de récupération du flux ; référent sécurité désigné ; engagements de	MidGard dispose d'une politique de sécurité des systèmes d'information (PSSI) et d'un document d'architecture technique (DAT) décrivant la solution FireGard ainsi que la chaîne de récupération et de transmission du flux vidéo.

Convention d'expérimentation FireGard

Domaine	Exigence minimale du responsable du traitement	Mesure mise en œuvre par MidGard
	confidentialité et sensibilisation RGPD du personnel.	Un référent sécurité est désigné pour coordonner la mise en œuvre et le suivi des mesures de sécurité. Les membres du personnel autorisés à accéder aux données sont soumis à des engagements écrits de confidentialité et bénéficient d'une sensibilisation à la protection des données personnelles et aux obligations du RGPD. La documentation de sécurité est communiquée à la Commune sur demande.
Intelligence artificielle	Documentation du fonctionnement général du modèle (données d'entrée, logique de détection, indicateurs de performance et taux de faux positifs) ; supervision humaine systématique des alertes (aucune décision automatisée produisant des effets à l'égard des personnes) ; absence de réutilisation des données à caractère personnel pour l'entraînement ; traçabilité des versions du modèle déployées.	MidGard documente le fonctionnement général du modèle utilisé par FireGard, notamment les données d'entrée, la logique de détection, les indicateurs de performance et les taux de faux positifs. Les alertes générées font systématiquement l'objet d'une supervision humaine pour leur qualification et la détermination des suites opérationnelles. Aucune décision entièrement automatisée produisant des effets à l'égard des personnes n'est prise par la solution. Les données à caractère personnel traitées dans le cadre de l'expérimentation ne sont pas réutilisées pour l'entraînement des modèles. MidGard assure la traçabilité des versions du modèle déployées afin de permettre l'identification de la version utilisée pendant chaque période d'exploitation.
Portabilité et effacement	Export des données dans un format ouvert et structuré à la demande de la Commune ; procédure d'effacement sécurisé et attestation de suppression (clause 4.3).	MidGard assure, à la demande de la Commune, l'export des données dans un format ouvert, structuré et lisible par machine. Une procédure d'effacement sécurisé permet la suppression des données à caractère personnel et de leurs copies, y compris celles détenues par les sous-traitants ultérieurs, les sauvegardes étant supprimées à l'expiration de leur cycle de rotation. Au terme du Contrat, MidGard procède, selon le choix de la Commune, à la restitution, au transfert ou à la destruction des données à caractère personnel dans les conditions et délais prévus à la clause 4.3. Une attestation de suppression est remise à la Commune après destruction, précisant la nature des données supprimées, les systèmes concernés et la date de l'opération.
Certifications / codes de conduite	Communication de toute certification ou adhésion à un code de conduite pertinent (ISO/IEC 27001, etc.).	MidGard ne dispose à ce jour d'aucune certification.

Pour les transferts vers des sous-traitants (ultérieurs), le sous-traitant s'assure que chaque sous-traitant ultérieur met en œuvre des mesures au moins équivalentes à celles décrites ci-dessus pour le périmètre qui le concerne, et qu'il est en mesure de l'assister, dans les délais prévus aux présentes clauses, pour la gestion des demandes d'exercice de droits, des violations de données et des audits.

Convention d'expérimentation FireGard

Description des mesures techniques et organisationnelles spécifiques que le sous-traitant doit prendre pour pouvoir prêter assistance au responsable du traitement :

- Désignation d'un point de contact unique « protection des données et sécurité » joignable pendant toute la durée de l'expérimentation, y compris pendant les plages d'exploitation définies par la Commune ;
- Fonctionnalités de recherche, d'extraction, de floutage et d'effacement ciblé des séquences permettant de répondre aux demandes d'exercice de droits dans le délai d'un mois prévu à l'article 12 du RGPD ;
- Procédure écrite de gestion des incidents et des violations de données permettant de respecter le délai de notification de 24 heures, et fiche de notification reprenant les éléments de l'article 33, paragraphe 3, du RGPD ;
- Fourniture, sous quinze (15) jours à compter de la demande, des éléments nécessaires à l'inscription au registre des traitements de la Commune et à la réalisation de l'analyse d'impact relative à la protection des données ;
- Participation au comité de suivi sur les sujets de protection des données (revue des habilitations, incidents, évolutions de la Solution) et inscription de ces points dans les relevés de décisions ;
- Remise d'une attestation de suppression ou de restitution des données au terme du Contrat.

Convention d'expérimentation FireGard

ANNEXE IV – LISTE DES SOUS-TRAITANTS ULTÉRIEURS

La présente annexe constitue la liste convenue des sous-traitants ultérieurs au sens de la clause 4.7 (autorisation écrite générale). Toute modification est soumise à la procédure d'information préalable et d'opposition prévue à cette clause.

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

Sous-traitant ultérieur n°1.

Nom	Azur Data Center - SAS - SIRET 52267835800055
Adresse	4, rue des Vieilles Vignes, Immeuble Volta, 77183 Croissy-Beaubourg
Nom, fonction et coordonnées de la personne de contact	Gregory Tourneaux gregory.tourneux@azurdatacenter.fr +33 (0)6 86 13 42 47
Description du traitement	Hébergement de la plateforme FireGard, stockage des séquences, métadonnées, comptes et journaux, sauvegardes. Pas d'accès aux données en clair hors opérations d'infrastructure. Durée : durée du Contrat. Transfert hors UE : aucun.

Sous-traitant ultérieur n°2.

Nom	Slack Technologies Limited (groupe Salesforce)
Adresse	Salesforce Tower, 60 R801, North Dock, Dublin 1, Irlande
Nom, fonction et coordonnées de la personne de contact	Délégué à la protection des données de Slack — dpo@slack.com .
Description du traitement	Acheminement des notifications d'alerte vers les téléphones mobiles des opérateurs habilités (identifiants des utilisateurs, contenu des notifications). Durée : durée du Contrat ; suppression de l'espace de travail ou des messages au terme. Transferts possibles vers les États-Unis et d'autres pays tiers encadrés par les clauses contractuelles types de la Commission et, le cas échéant, par le cadre de protection des données UE-États-Unis. Contenu des notifications minimisé conformément à l'annexe III. Titulaire de l'espace de travail Slack utilisé.

Sous-traitant ultérieur n°3.

Nom	PERSEUS – SAS – SIREN 899 926 588
Adresse	Port de Toga A Vela, 20200 Bastia
Nom, fonction et coordonnées de la personne de contact	Joseph Antoine FABRI, Président +33 6 81 67 08 39
Description du traitement	Préparation technique, pose et raccordement de la caméra, configuration de la transmission du flux vidéo vers FireGard ; accès aux images limité aux opérations de réglage et de test. Durée : phases d'installation et de recette, et interventions de maintenance éventuelles. Aucun transfert hors UE.

Les présentes clauses de protection des données sont conformes aux clauses contractuelles types adoptées par la Commission européenne le 4 juin 2021 par la décision d'exécution (UE) 2021/915, au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679. Elles encadrent les différentes responsabilités en matière de protection des données entre un Responsable de traitement et ses Sous-traitants.