

l'an deux mil vingt -cinq
le vingt-huit janvier à vingt-et-une heures
LE CONSEIL MUNICIPAL, légalement convoqué, s'est réuni en séance publique
ordinaire, en mairie de Cernay-la-Ville,
Sous la présidence de Madame Claire CHERET, Maire

Etaient présents : Mmes et MM. BOUSSIOUS, CHARIERAS, CHERET,
COSTEDOAT, CZEPCZAK, DIOP (arrivé en cours de séance), EVEN, FLOHIC,
FOUILLOT, GIBAUD-AZIZA, LAMIRAL, MILON, MUNIER, PASSET,
SANTINHO

Date de convocation
23 JANVIER 2025

formant la majorité des membres en exercice.

Pouvoirs : M. BONY a donné procuration à Mme CHERET
Mme GILLMANN a donné procuration à Mme MILON
Mme LEMOING a donné procuration à M. FOUILLOT
Mme RANCE a donné procuration à M. LAMIRAL

**Date d'affichage
de la convocation**
23 JANVIER 2025

Absent : ./.

**Date de publication
de la délibération**
31 JANVIER 2025

M. MUNIER a été élu secrétaire

Nombre de conseillers 19

Présents 15

Votants 19

**OBJET : Adhésion au groupement de commandes du Centre Interdépartemental de
Gestion de la Grande Couronne pour les assurances cyber-risques pour la
période 2026-2029**

Les quinze dernières années ont vu une augmentation des attaques sur les systèmes informatiques des entreprises, hôpitaux mais également sur celui des collectivités territoriales. Cette tendance s'est accrue depuis la pandémie de Covid19 et les conflits internationaux. Aucune organisation n'est aujourd'hui à l'abri d'une cyberattaque d'envergure. Selon les données de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en 2022, les collectivités locales constituent la deuxième catégorie de victime la plus affectée par des attaques par rançongiciel derrière les très petites entreprises (TPE), les petites et moyennes entreprises (PME) et les entreprises de taille intermédiaire (ETI). Elles représentent ainsi 23 % des incidents en lien avec des rançongiciels.

Les collectivités locales sont donc des cibles de choix pour les pirates informatiques. En effet, elles détiennent de nombreuses données à caractère financier, administratif et personnel. Ces informations peuvent être aisément monétisées et revendues par les cybercriminels (informations relatives à l'état civil et aux données personnelles des administrés, données bancaires des administrés et des agents...). Mais les attaques peuvent également prendre la forme du piratage d'un site officiel en diffusant des messages sans lien avec l'autorité publique. Ce ne sont plus les données qui sont ciblées mais l'image des institutions. Enfin les collectivités locales peuvent également être victimes d'un agent (ou ex-agent) malveillant ou d'une négligence qui peuvent amener à une fuite d'informations confidentielles.

Entre janvier 2022 et juin 2023, l'ANSSI a effectué l'enregistrement et le traitement de 187 cyberattaques d'ampleur visant directement des collectivités territoriales.

Le développement de la technologie et la réglementation tendent à faire peser de plus en plus d'obligations et augmentent le volume de données détenues par les collectivités locales.

Depuis le 25 mai 2018 le règlement du Parlement européen et du Conseil en date du 14 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 est entré en vigueur. Ce texte, également appelé Règlement Général sur la Protection des Données (RGPD), impose à l'ensemble des personnes publiques et privées de communiquer à la CNIL et de notifier aux victimes les fuites d'informations. La notification et le suivi seront à la charge de la collectivité et engendreront des coûts supplémentaires importants en complément de la réparation du système informatique.

Pour exemple, dans l'hypothèse d'une cyberattaque visant un établissement de santé dont le budget serait de 600 millions d'euros, les frais de notification légale avoisineraient à eux seuls les 1 500 000 euros. (*Source Relyens : Estimation de l'impact financier d'une cyberattaque par ransomware dans un établissement de santé*)

De plus depuis le mois d'octobre 2018, les marchés publics doivent être entièrement dématérialisés. Les collectivités disposent donc dans leur système informatique des informations relevant du secret des affaires des entreprises.

L'assurance cyber risques intervient après le sinistre en mettant à la disposition de la personne publique des moyens humains et financiers pour identifier et circonscrire les attaques. Cette mise à disposition de moyens permet également d'informer les victimes et de suivre l'utilisation frauduleuse des données. La dernière étape est la restauration du système informatique et la formulation de préconisation en matière de sécurité.

Mme la Maire expose à l'Assemblée :

Le CIG Grande Couronne va constituer un groupement de commandes pour les assurances Cyber-Risques qui a pour objet la passation, pour le compte des membres du groupement, des marchés de prestations de services d'assurances Cyber-Risques.

Je vous rappelle que depuis le 1998, les contrats d'assurances des collectivités sont des marchés publics. Ainsi, obligation est-elle faite aux collectivités de remettre régulièrement en concurrence leurs contrats en respectant le formalisme imposé par le Code de la Commande Publique.

Le groupement de commandes évite à chaque collectivité de lancer une consultation individuelle et permet de bénéficier des avantages de la mutualisation. Compte tenu du contexte assurantiel tendu, de la complexité du contenu technique du cahier des charges et de la procédure à conduire, cette démarche s'inscrit dans une logique de simplification administrative et d'économie financière.

À cette fin, une convention constitutive de ce groupement de commandes a été établie. Cette convention prend acte du principe et de la création du groupement de commandes. Elle désigne le Centre Interdépartemental de Gestion de la Grande Couronne comme coordonnateur. Ce dernier est notamment chargé de procéder à l'organisation de la procédure de choix du titulaire des marchés de prestations de services.

La convention prévoit que les membres du groupement habilite le coordonnateur à signer et notifier le marché au nom de l'ensemble des membres constituant le groupement. À ce titre, la commission d'appel d'offres compétente est celle du coordonnateur du groupement de commandes.

La convention précise que la mission du CIG Grande Couronne comme coordonnateur ne donne pas lieu à rémunération. Cependant, les frais de procédure de mise en concurrence et les autres frais occasionnés pour le fonctionnement du groupement font l'objet d'une refacturation aux membres du groupement selon les modalités suivantes :

Par strate de population et affiliation au centre de gestion	Montant de la participation aux frais de gestion du CIG
jusqu'à 1 000 habitants affiliés ou CCAS/CDE de 1 à 50 agents CDE	650 €
de 1 001 à 3 500 habitants affiliés	750 €
de 3 501 à 5 000 habitants affiliés ou EPCI de 1 à 50 agents ou CCAS/CDE de plus de 51 agents	850 €
de 5 001 à 10 000 habitants affiliés ou EPCI de 51 à 100 agents	950 €
de 10 001 à 20 000 habitants affiliés ou EPCI de 101 à 350 agents	1 050 €
plus de 20 000 habitants affiliés ou EPCI de plus de 350 agents	1 250 €
Collectivités et établissements non affiliés	1 550 €

Il est à noter que cette participation aux frais de gestion du CIG n'est exigée qu'une seule fois sur toute la durée de la convention.

Les prix appliqués, ainsi que les modalités de paiement des prestataires de services par l'ensemble des adhérents du groupement, seront fixés dans les marchés de services.

Enfin, la convention prévoit que chaque membre dispose d'un droit de retrait.

Il appartient donc à chaque membre du groupement d'examiner, d'adopter et d'autoriser son exécutif à signer cette convention constitutive du groupement de commandes.

Par conséquent, je vous propose de vous prononcer sur les engagements de la commune contenus dans ce document et de m'autoriser à signer cette convention.

Vu le Code Général des Collectivités Territoriales,

Vu le Code de la Commande Publique,

Vu la délibération n°2024-51 en date du 10 octobre 2024 portant sur le groupement de commandes « assurance Cyber Risques » 2026-2029 : Approbation du lancement d'une nouvelle consultation et autorisation donnée au président de signer les conventions constitutives de groupement avec chaque collectivité souhaitant intégrer la procédure,

Vu la convention constitutive du groupement de commandes pour les assurances Cyber-Risques,

Considérant l'intérêt de rejoindre ce Groupement de commandes, pour la période 2026-2029, en matière de simplification administrative et d'économie financière,

LE CONSEIL MUNICIPAL,

Après avoir délibéré,
À l'unanimité,

Mis en ligne le 31/01/2025 à 14h29

REÇU EN PREFECTURE
le 31/01/2025

Application agréée E-legalite.com

99_DE-078-217801281-20250128-DCH2025_006

DECIDE d'adhérer au groupement de commandes pour les assurances Cyber-Risques pour la période 2026-2029,

APPROUVE la convention constitutive du groupement de commandes désignant le Centre Interdépartemental de Gestion de la Grande Couronne coordonnateur du groupement et l'habilitant à signer et notifier le marché selon les modalités fixées dans cette convention,

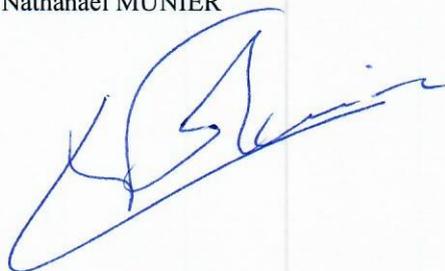
AUTORISE Mme la Maire ou son représentant à signer la convention constitutive du groupement de commandes ainsi qu'à prendre toutes les mesures nécessaires à l'exécution de la présente délibération,

DECIDE que les dépenses inhérentes à la mise en œuvre du groupement et de ces procédures seront imputées sur le budget de l'exercice correspondant.

Pour extrait conforme
Cernay-la-Ville, 31 janvier 2025

La Maire
Claire CHERET

Le secrétaire de séance
Nathanaël MUNIER



Mis en ligne le 31/01/2025 à 14h29

REÇU EN PREFECTURE
le 31/01/2025

Application agréée E-legalite.com

99_DE-078-217801281-20250128-DCH2025_006