FICHE DE POSTE	**Fonction :** DPO : Délégué à la Protection des données Mutualisé Code RIFSSEP :
	Affectation : Direction Générale des Services
	Responsable de Pôle :
	Supérieur hiérarchique direct :

Conditions d'exercice du poste

Lieu : Siège CAMVS Maubeuge, Communes de la CAMVS

Quotité horaire : temps complet

Filière / Catégorie / Grade :
Technique / A / Ingénieur

Habilitations, permis, formations obligatoires :

- Connaissances spécialisées du droit et des pratiques en matière de protection des données (RGPD art. 37, 5)
- Diplôme(s), formation(s) et expériences continues en lien avec les compétences et connaissances mentionnées.
- Permis B

Description des missions :

Délégué·e à la Protection des Données (DPO), désigné·e par délibération et publication et transmission à la CNIL (Décret 2019-536, art. 83), pour les entités suivantes :

- La Communauté d'Agglomération Maubeuge - Val de Sambre (CAMVS)
- Les communes membres de la CAMVS adhérentes au dispositif prévu par le Schéma de Mutualisation (Délibération 4394 de la CAMVS)

Conformément aux articles 38 et 39 du RGPD, le rôle du DPO est d'accompagner, conseiller, contrôler et animer la politique de protection des données à caractère personnel, dans le respect des règlementations et des textes applicables :

- **Informer et conseiller** le responsable de traitement (maire, président, DGS, etc.) ainsi que les agents sur leurs obligations en matière de protection des données.
- **Contrôler le respect** du RGPD, de la Loi Informatique & Libertés, des règles internes et des bonnes pratiques au sein des collectivités.
- **Participer à la réalisation des analyses d'impact** (AIPD) sur la sécurité des traitements.
- **Coopérer avec la CNIL** et être le point de contact privilégié de l'autorité de contrôle.
- **Animer la politique de protection des données** et diffuser une culture « Informatique et Libertés » auprès des agents et directions.
- **Contrôler la tenue du registre des traitements** : vérifier le recensement, la conformité, conseiller sur la légalité et la sécurité, proposer des actions correctives.
- **Assurer une veille juridique et technique** sur la protection des données.
- **Recevoir et traiter les réclamations** des personnes concernées, veiller au respect de leurs droits et assurer la médiation si besoin.
- **Contrôler, auditer, investiguer** les traitements et procédures, et s'assurer de la bonne application des recommandations.
- **Informer régulièrement le responsable de traitement** des manquements, problèmes constatés et immédiatement en cas de violation de données.

- **Former et accompagner :**
    - **Les référents DPO** dans les communes, notamment à l'utilisation des outils (ex : logiciel MADIS).
    - **Les agents** de la CAMVS, notamment en structurant des démarches internes.

Concernant la tenue du registre et conformément à l'article 30 du RGPD, le DPO :

- Vérifie le recensement des traitements.
- Contrôle leur conformité.
- Conseille sur leur légalité et sécurité.
- Fait des propositions d'actions correctives.

Il contrôle la bonne tenue des informations et assure leur accessibilité à l'autorité de contrôle.

Le DPO rend uniquement compte au responsable de traitement ou au plus au niveau de l'organisation (Direction Générale). Il établit un rapport d'activité annuel et interne, conformément aux recommandations de la CNIL. À aucun moment, il ne peut être décisionnaire, responsable ou partie prenante de la chaîne de mise en œuvre d'un traitement à caractère personnel pour lequel il réalise ses missions. En revanche, il s'assure d'apporter en toute indépendance et objectivité les éléments qui permettront au responsable de traitement de respecter ses obligations et de piloter sa conformité.

Relations (internes / externes) :

Internes : Responsable de traitement (élu), direction générale, tous les services et agents de la CAMVS.
Externes :

- Responsables de traitements (élus), Référents DPO des communes, DG/SG des mairies, agents communaux.
- CNIL, sous-traitants, prestataires, partenaires institutionnels.

Compétences et savoirs requis :

Compétences juridiques et réglementaires

- Maîtrise du RGPD (UE 2016/679), Loi Informatique & Libertés, Décret 2019-536, Data Act, NIS2, AI Act, guides CNIL, G29, RGS, ANSSI.
- Connaissance des principes de licéité, limitation des finalités, minimisation, exactitude, conservation limitée, intégrité, confidentialité et responsabilité.
- Capacité à identifier la base juridique d'un traitement et à déterminer les mesures d'information à fournir aux personnes concernées.
- Maîtrise du cadre juridique de la sous-traitance et des transferts de données hors UE.
- Savoir établir et contrôler les procédures d'exercice des droits des personnes concernées.

Compétences techniques et organisationnelles

- Maîtrise des techniques de sécurité, cybersécurité, gestion des risques, normes ISO, RGS.
- Capacité à mener des audits réseaux, audits de sécurité et audits organisationnels en matière de protection des données.
- Savoir identifier et recommander des mesures de protection des données dès la conception et par défaut.
- Savoir organiser et participer à des audits, élaborer et mettre en œuvre des politiques internes de protection des données.
- Savoir déterminer la nécessité d'une AIPD, en vérifier l'exécution et conseiller sur la méthodologie.
- Savoir gérer les relations avec la CNIL, répondre à ses sollicitations et faciliter les contrôles.
- Savoir élaborer, dispenser et suivre des programmes de formation et de sensibilisation.
- Savoir assurer la traçabilité de ses activités (outils de suivi, bilans annuels).

Compétences transversales

- Excellente capacité à développer différents niveaux de communication (agents, techniciens, juristes, DG, élus, CNIL, usagers).
- Aisance rédactionnelle, objectivité, indépendance, probité, discrétion, résistance au stress.
- Pratique de l'anglais, au minimum le niveau technique et métier (cf. Réglementation européennes, technologies).
- Connaissance du fonctionnement des collectivités territoriales et des procédures administratives (ex : compétences EPCI, Communales....)
- Proactivité et force de proposition dans l'amélioration continue de la protection des données.
- Culture de la data : compréhension des enjeux liés à la collecte, au traitement et à l'utilisation des données.
- Anticipation des nouvelles technologies/usages, veille prospective, capacité à penser "risque" et "éthique".

Conditions matérielles :

Moyens bureautiques
Moyens de communication
Moyens de déplacements

Conditions particulières et contraintes du poste

Secret professionnel renforcé, obligation de confidentialité pour l'ensemble des missions
Horaires variables selon l'activité.

Fonctions étrangères :