

FICHE DE POSTE – JURISTE RGPD ET CYBERSÉCURITÉ

Intitulé du poste : Juriste RGPD et cybersécurité

Catégorie : A (ou B confirmé selon expérience)

Temps de travail : Temps complet

Rattachement hiérarchique : Responsable de la sécurité des systèmes d'information (RSSI) – Délégué à la protection des données (DPO).

Direction de rattachement : Direction Ingénierie Informatique, Télécom et Usages Numériques (Direction mutualisée)

1. Identité du poste

- **Intitulé :** Juriste RGPD et cybersécurité
- **Catégorie :** A (ou B confirmé selon expérience) –
- **Rattachement hiérarchique :** RSSI-DPO
- **Direction de rattachement :**
Direction Ingénierie Informatique, Télécom et Usages Numériques

2. Contexte et finalité

Dans un environnement de transformation numérique accélérée, la Direction mutualisée des Systèmes d'Information renforce sa maîtrise des risques liés aux données et à la cybersécurité. Le ou la juriste RGPD et cybersécurité garantit la conformité aux textes applicables et soutient la stratégie de sécurité numérique de l'ensemble des entités membres de la mutualisation. Le ou la juriste RGPD et cybersécurité assure une conformité durable aux textes européens et nationaux (RGPD, loi Informatique et Libertés, directive NIS 2, règlements CER, et Cyber Resilience Act tout en pilotant la maîtrise des risques juridiques attachées aux projets numériques et à la sécurité de l'information. Sa mission contribue directement à la stratégie digitale de la collectivité, à la protection des finances publiques et à la réputation des entités membres.

3. Missions principales

- Protection des données personnelles :

- L'agent tient et enrichit le registre des traitements, conduit et valide les analyses d'impact, supervise le guichet unique des droits des personnes, gère les violations de données, anime la culture « privacy by design » et assure la relation avec la CNIL.
- Conformité et cybersécurité :
 - L'agent décline opérationnellement la directive NIS 2 et le règlement CER, déploie le cadre DORA pour les activités financières, anticipe le Cyber Resilience Act, applique les prescriptions de la LPM aux systèmes d'importance vitale, organise la remontée des incidents dans le délai imparti et maintient à jour une matrice de conformité unifiée.
- Analyse de risque juridique numérique et SSI :
 - L'agent définit la méthodologie d'identification et de hiérarchisation des risques, alimente une cartographie partagée, propose des plans de traitement et d'atténuation, rapporte périodiquement au comité de pilotage et contribue à l'amélioration continue du système de management de la sécurité de l'information.

4. Activités techniques, spécifiques au métier

- Piloter, coordonner et évaluer la conformité de la collectivité aux règles relatives à la protection des données.
- Informer et conseiller les élus, directions et agents sur les obligations issues de la réglementation « informatique et libertés ».
- Contrôler le respect, par l'ensemble des services et des prestataires, du cadre légal et des règles internes en matière de protection des données (notamment personnelles).

5. Activités secondaires

- Participation aux comités projets.
- Contribution aux exercices de gestion de crise cyber.
- Représentation dans les réseaux professionnels (AFCDP, CLUSIR, CNFPT, etc.).

6. Compétences requises

- **Savoirs** : droit des données personnelles, droit des contrats publics, cadre légal cyber, fonctionnement des collectivités territoriales.
- **Savoir-faire** : rédaction d'actes opposables, conduite d'AIPD, cartographie des risques, pédagogie juridique.
- **Savoir-être** : rigueur, sens de la confidentialité, autonomie, esprit d'équipe, pédagogie.

7. Compétences ou connaissances souhaitées

- Droit de l'Union européenne et droit français relatifs à la protection des données.
- Techniques de communication écrite et orale auprès de publics variés.
- Règles spécifiques de collecte et de traitement des données de la collectivité ou de l'établissement public.
- Modes de traitement et de structuration des données, conduite de projets
- Systèmes de gestion et d'exploitation de bases de données, politique de confidentialité et de sécurité de l'information.
- Élaboration de tableaux de bord et d'indicateurs de suivi.
- Méthodes et techniques de communication

8. Profil recherché

- **Formation** : Master 2 Droit du numérique / Droit public, ou équivalent.
- **Expérience** : première mission RGPD ou cybersécurité dans une structure publique ou parapublique.
- **Aptitudes personnelles** : sens du relationnel et de l'écoute, curiosité technico-juridique, esprit d'analyse.