COMMUNE DE BEYNOST
Place de la Mairie
BP 411
01704 - BEYNOST CEDEX

Accord-cadre à bons de commande mono-attributaire de fournitures et services informatiques

---

Marché global pour la gestion du système d'information communal, des équipements, des télécommunications et de la conformité réglementaire

Appel d'offres ouvert

En application des articles R2124-1, R2124-2 et R2161-2 à R2161-5 du code de la commande publique.

CAHIER DES CLAUSES TECHNIQUES PARTICULIÈRES (CCTP)

LOT 4 - Mission d'audit RGPD et DPO externalisé

SOMMAIRE

1. OBJET DU MARCHÉ 3
2. CONTEXTE 3
3. PRESTATIONS ATTENDUES 3
   3.1. Phase 1 - Audit de conformité 3
   3.2. Phase 2 - Mise en conformité 3
   3.3. Phase 3 : Mise à disposition d'un DPO externalisé 3
4. LIVRABLES ATTENDUS 4
5. MODALITES DE SUIVI ET D'EVALUATION 4
6. COMPETENCES ET QUALIFICATIONS REQUISES POUR LA MISSION RGPD 4
   6.1. Compétences exigées 4
   6.2. Qualifications obligatoires 5
   6.3. Qualifications recommandées (non obligatoires mais valorisées) 5
   6.4. Justificatifs attendus 5
7. CALENDRIER DE REALISATION 5
8. CLAUSE DE RÉVERSIBILITÉ 5

1. OBJET DU MARCHE

Le présent marché porte sur :

- La réalisation d'un audit complet de conformité au Règlement Général sur la Protection des Données (RGPD).
- La mise à disposition d'un Délégué à la Protection des Données (DPO) externe, conformément aux exigences précisées dans les articles 37 à 39 du RGPD.

2. CONTEXTE

La mairie souhaite garantir sa pleine conformité au RGPD et renforcer ses pratiques relatives à la protection des données personnelles. À cet effet, elle entend recourir à un prestataire externe capable de l'accompagner durablement dans ses obligations réglementaires en matière de protection des données personnelles.

3. PRESTATIONS ATTENDUES

3.1. Phase 1 - Audit de conformité

- Cartographier exhaustivement les traitements de données à caractère personnel réalisés par la mairie.
- Évaluer les dispositifs techniques et organisationnels de sécurité mis en place actuellement.
- Analyser les procédures internes existantes permettant l'exercice des droits des personnes concernées.
- Identifier précisément les éventuels écarts par rapport aux obligations imposées par le RGPD.
- Remettre un rapport d'audit complet accompagné de recommandations opérationnelles pour garantir la mise en conformité.

3.2.Phase 2 - Mise en conformité

- Élaborer un plan d'action détaillé visant à rectifier les non-conformités relevées lors de l'audit.
- Mettre à jour ou rédiger les documents obligatoires prévus par le RGPD, notamment : registre des traitements, politiques de confidentialité, procédures internes de gestion des demandes des personnes concernées, etc.
- Assurer une formation adaptée et une sensibilisation du personnel municipal sur les enjeux du RGPD et les bonnes pratiques en matière de protection des données personnelles.

3.3.Phase 3 : Mise à disposition d'un DPO externalisé

Le prestataire assurera les missions suivantes en qualité de DPO externe :

- Fournir un accompagnement permanent et des conseils juridiques et techniques sur les problématiques liées à la protection des données personnelles.

- Vérifier régulièrement la conformité des traitements réalisés par la mairie, assurer leur suivi et proposer les ajustements nécessaires.
- Coopérer activement avec l'autorité de contrôle compétente (CNIL) en cas de sollicitations ou de contrôles.
- Constituer le point de contact principal pour les personnes concernées, gérer les demandes d'exercice des droits et assurer leur suivi.

4. LIVRABLES ATTENDUS

Les livrables devront inclure, sans que cette liste soit exhaustive :

- Rapport d'audit détaillé avec recommandations précises.
- Plan d'action détaillé pour la mise en conformité.
- Documents obligatoires mis à jour ou créés : registre des traitements, politiques de confidentialité, procédures internes.
- Supports et comptes-rendus de formations réalisées.
- Rapports périodiques d'activité du DPO externalisé détaillant les actions menées et les points d'attention identifiés.

5. MODALITES DE SUIVI ET D'EVALUATION

- Réunions régulières de suivi entre le prestataire et la mairie afin d'évaluer l'avancement des travaux.
- Rapports périodiques remis à la mairie pour permettre un suivi transparent des actions engagées et des résultats obtenus.
- Évaluation annuelle du prestataire sur la base d'indicateurs définis conjointement afin de mesurer l'efficacité de l'accompagnement et l'atteinte des objectifs de conformité au RGPD.

6. COMPETENCES ET QUALIFICATIONS REQUISES POUR LA MISSION RGPD

Le titulaire devra justifier de compétences juridiques, techniques et organisationnelles avérées en matière de protection des données à caractère personnel, conformément aux exigences du Règlement (UE) 2016/679 (RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée.

6.1. Compétences exigées

Le titulaire devra démontrer les compétences suivantes :

- Une maîtrise du cadre juridique applicable à la protection des données à caractère personnel, notamment le RGPD, la loi Informatique et Libertés modifiée, et les lignes directrices de la CNIL ;
- Une connaissance des systèmes d'information et des mesures de sécurité informatique permettant de garantir la confidentialité, l'intégrité et la disponibilité des données ;
- Une expérience significative d'audit de conformité RGPD, idéalement dans des collectivités territoriales ou établissements publics ;
- Une capacité à assurer le rôle de Délégué à la Protection des Données (DPO) externalisé, conformément aux articles 37 à 39 du RGPD ;
- Des aptitudes pédagogiques permettant de sensibiliser et former les agents et élus de la collectivité.

6.2.Qualifications obligatoires

Le prestataire devra fournir, au sein de son équipe intervenante au moins un consultant ou juriste certifié DPO selon la norme ISO/IEC 17024 (par un organisme accrédité tel que AFNOR, Bureau Veritas, PECB, CNPP, etc.) ;

6.3.Qualifications recommandées (non obligatoires mais valorisées)

Les certifications ou qualifications suivantes seront appréciées dans l'analyse des offres :

- Certification ISO 27001 ou ISO 27701 relative à la sécurité de l'information ou à la gestion de la vie privée ;
- Expérience ou certification dans la conduite de AIPD (analyse d'impact relative à la Protection des Données) ;
- Références attestées dans des missions RGPD au sein d'au moins trois collectivités territoriales sur les cinq dernières années.

6.4. Justificatifs attendus

Les offres devront inclure :

- Les CV détaillés des intervenants pressentis avec leurs diplômes, certifications et expériences ;
- Les attestations de certifications ou de formation mentionnées ci-dessus ;
- Une liste de références comparables, accompagnée de contacts référents si possible.

7. CALENDRIER DE REALISATION

Le calendrier prévisionnel suivant est proposé :

- Phase 1 (Audit) : à réaliser dans les 2 mois suivant la notification du marché.
- Phase 2 (Mise en conformité) : à engager immédiatement après validation de l'audit et à finaliser dans les 4 mois suivants.
- Phase 3 (DPO externalisé) : mission continue, à débuter dès validation de la mise en conformité, avec une durée initiale de 12 mois renouvelable.

8. CLAUSE DE REVERSIBILITE

Le prestataire s'engage à garantir une totale réversibilité à l'issue du marché ou en cas de résiliation anticipée. À cet effet, il devra :

- Remettre à la mairie l'ensemble des documents, données et informations nécessaires pour assurer la continuité de service et la conformité RGPD.
- Collaborer pleinement avec la mairie ou un prestataire successeur pendant une période de transition définie contractuellement.
- Fournir un rapport final de réversibilité précisant clairement les actions effectuées et les recommandations pour maintenir la conformité au RGPD.