ANNEXE — PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Cette annexe complète l'article du règlement de la consultation (et/ou du CCAP) relatif à la protection des données à caractère personnel. Elle a pour objet de formaliser, conformément à l'article 28 du RGPD, les conditions dans lesquelles le titulaire du marché, agissant en qualité de sous-traitant au sens du RGPD, traite des données à caractère personnel pour le compte du pouvoir adjudicateur, responsable de traitement.

1. Objet

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire s'engage à effectuer, pour le compte du pouvoir adjudicateur, les opérations de traitement de données à caractère personnel définies ci-après, nécessaires à la réalisation de la mission d'élaboration et de rédaction de l'étude de risque régionale Feux de forêt , incluant la tranche ferme (cartographie du risque, des aléas et enjeux) et, le cas échéant, la tranche optionnelle (PIDPFCI).

2. Description du traitement faisant l'objet de la sous-traitance

Rubrique	Précision
Nature des opérations réalisées sur les données	Collecte, structuration, hébergement, cartographie (SIG), analyse, transmission et restitution de données à caractère personnel dans le cadre de l'élaboration du diagnostic, de la cartographie aléa/enjeux et, en tranche optionnelle, de la démarche de gouvernance du PIDPFCI.
Finalité(s) du traitement	Réalisation de la mission de diagnostic, de cartographie et d'accompagnement à la gouvernance et à la rédaction du PIDPFCI, telle que définie au CCTP.
Catégories de personnes concernées	Propriétaires forestiers ; élus et représentants des structures porteuses associées à la gouvernance ; personnes ressources et contacts institutionnels identifiés dans le cadre de la mission.
Catégories de données traitées	Données d'identification (nom, prénom, qualité), coordonnées de contact (adresse, téléphone, courriel), données de localisation associées aux parcelles ou structures concernées. À l'exclusion de toute donnée sensible au sens de l'article 9 du RGPD.
Durée du traitement	Durée d'exécution du marché, augmentée, le cas échéant, de la durée de conservation nécessaire au respect des obligations légales et comptables du pouvoir adjudicateur.

3. Obligations du pouvoir adjudicateur (responsable de traitement)

Le pouvoir adjudicateur s'engage à :

- documenter par écrit toute instruction concernant le traitement des données par le titulaire ;
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du titulaire ;
- superviser le traitement, y compris en réalisant les audits et les inspections auprès du titulaire ;

- s'assurer que le titulaire dispose des garanties nécessaires quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

4. Obligations du titulaire (sous-traitant au sens du RGPD)

Le titulaire s'engage à :

- traiter les données uniquement pour la ou les seule(s) finalité(s) définie(s) à l'article 2 de la présente annexe ;
- traiter les données conformément aux instructions documentées du pouvoir adjudicateur ; si le titulaire considère qu'une instruction constitue une violation du RGPD, il en informe immédiatement le pouvoir adjudicateur ;
- garantir la confidentialité des données traitées, et veiller à ce que les personnes autorisées à traiter les données s'engagent à respecter cette confidentialité ou soient soumises à une obligation légale de confidentialité ;
- veiller à ce que les personnes autorisées à traiter les données reçoivent la formation nécessaire en matière de protection des données ;
- mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées, précisées à l'article 6 de la présente annexe ;
- respecter les conditions de recours à un autre sous-traitant (sous-traitance ultérieure) précisées à l'article 5 ;
- aider le pouvoir adjudicateur, dans la mesure du possible, à répondre aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, opposition, limitation, portabilité) ;
- notifier au pouvoir adjudicateur toute violation de données à caractère personnel dans un délai maximal de 48 heures après en avoir eu connaissance ;
- aider le pouvoir adjudicateur à réaliser, le cas échéant, les analyses d'impact relatives à la protection des données (AIPD) ;
- sur demande, mettre à la disposition du pouvoir adjudicateur toute la documentation nécessaire pour démontrer le respect de ses obligations ;
- à la fin du marché, selon le choix exprimé par le pouvoir adjudicateur, supprimer ou restituer toutes les données à caractère personnel traitées, et détruire toute copie existante, sauf obligation légale de conservation.

5. Sous-traitance ultérieure

Le titulaire ne peut faire appel à un autre sous-traitant (sous-traitant ultérieur au sens du RGPD) qu'avec l'autorisation écrite préalable, spécifique ou générale, du pouvoir adjudicateur. Dans ce dernier cas, le titulaire informe le pouvoir adjudicateur de tout changement envisagé concernant l'ajout ou le remplacement d'un sous-traitant ultérieur, permettant ainsi au pouvoir adjudicateur d'émettre une objection dans un délai de 15 jours à compter de la date d'information.

Le sous-traitant ultérieur est tenu de respecter les mêmes obligations que celles imposées au titulaire par la présente annexe. Le titulaire demeure pleinement responsable, à l'égard du pouvoir adjudicateur, de l'exécution des obligations du sous-traitant ultérieur.

6. Sécurité des données

Le titulaire s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles suivantes, adaptées à la nature des données traitées et au niveau de risque :

- hébergement des données au sein de l'Union européenne (ou, à défaut, dans un pays disposant d'une décision d'adéquation ou de garanties appropriées au sens du RGPD) ;
- gestion des habilitations et contrôle des accès aux données, limités aux personnes dont l'intervention est strictement nécessaire à l'exécution du marché ;
- chiffrement ou pseudonymisation des données lorsque cela est pertinent au regard de la nature du traitement ;
- sauvegardes régulières et procédures de restauration en cas d'incident ;
- traçabilité des accès et des opérations réalisées sur les données ;
- sécurisation des échanges de fichiers (protocoles chiffrés) lors de la transmission des données entre le titulaire et le pouvoir adjudicateur ou les structures porteuses associées à la gouvernance.

7. Sort des données au terme du marché

Au terme du marché, quelle qu'en soit la cause, le titulaire s'engage, au choix du pouvoir adjudicateur formalisé par écrit :

- à restituer l'intégralité des données à caractère personnel traitées, dans un format structuré, couramment utilisé et lisible par machine, puis à les détruire de ses systèmes d'information et de ceux de ses éventuels sous-traitants ultérieurs ; ou
- à détruire l'intégralité des données à caractère personnel traitées, et à justifier de cette destruction par écrit auprès du pouvoir adjudicateur,

sous réserve des dispositions légales imposant la conservation desdites données pour une durée déterminée.

8. Documentation et responsabilité

Le titulaire tient à la disposition du pouvoir adjudicateur, sur simple demande, toute documentation utile permettant de démontrer le respect des obligations prévues par la présente annexe et par l'article 28 du RGPD, et permet la réalisation d'audits, y compris des inspections, à ce titre.

Tout manquement du titulaire aux obligations prévues par la présente annexe est susceptible d'engager sa responsabilité, y compris au titre des sanctions prévues par le RGPD et la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

9. Contact

Délégué à la protection des données (DPO) du pouvoir adjudicateur : *[nom, fonction, coordonnées à compléter]*

Correspondant RGPD/référent désigné par le titulaire : *[à compléter par le candidat lors de la remise de l'offre ou à la notification]*