Annexe à l'accord-cadre n°2026AC000078

Missions d'audits sur des programmes de ressources externes. LOT 2

Traitements de données à caractère personnel

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le Titulaire effectue pour le compte de l'ADEME les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « **le règlement européen sur la protection des données** »).

II. Description du traitement des données à caractère personnel

Le Titulaire est autorisé à traiter pour le compte de l'ADEME les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

Description des opérations réalisées sur les données[1] : Interventions ponctuelles de missions d'audit et de vérification des dépenses réalisées. Ces audits entrent dans le cadre de projets faisant l'objet de financements externes de l'Union Européenne, de dispositifs de Certificats d'économie d'Energie (CEE), ou d'autres organismes exigeants ce type de contrôle.
Finalité(s) du traitement[2] : Les données sont traitées à des fins de contrôle.
Type de données à caractère personnel traitées[3] : Informations économiques et financières sur les aides.
Catégories de personnes concernées[4] : Porteurs de projet pour les aides.
Autres précisions ou interdictions[5] :

[1] Préciser ce que le prestataire va faire avec les données. Par exemple si prestation de réservation de voyages : vérification des données, réservation des billets, courriel de confirmation, facturation, encaissement…

[2] Raison pour laquelle les données sont traitées. Par exemple, réservation de voyages, gestion des inscriptions à une conférence, organisation et suivi des élections professionnelles …

[3] Les types de données sont principalement : Etat civil, Vie personnelle, Vie professionnelle, Informations économiques et financières, Revenus, Données de connexion, N° de sécu., Données biométriques, Difficultés sociales, Données de santé...

[4] Les catégories de personnes sont principalement : Salariés ADEME, Salariés d'entreprises extérieures sur site ADEME / intérimaires, Stagiaires, Clients, Fournisseurs, Visiteurs, Sujets de recherche, Grand public...

[5] Préciser, par exemple, si les données ne sont accessibles que sur site ADEME.

III. Obligations du Titulaire vis-à-vis de l'ADEME

Le Titulaire s'engage à :

1. traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la prestation ;
2. traiter les données **conformément aux instructions documentées** de l'ADEME. Si le Titulaire considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en **informe immédiatement** l'ADEME. En outre, si le Titulaire est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer l'ADEME de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;
3. **garantir la confidentialité** des données à caractère personnel traitées dans le cadre du présent marché ;
4. veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent marché :
   - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité,
   - reçoivent la formation nécessaire en matière de protection des données à caractère personnel
5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de **protection des données dès la conception** et de **protection des données par défaut**
6. **Sous-traitance**

Le Titulaire est autorisé à faire appel à un sous-traitant pour mener les activités de traitement suivantes :

Le sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions de l'ADEME. Il appartient au Titulaire de s'assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Titulaire demeure pleinement responsable devant l'ADEME de l'exécution par le sous-traitant de ses obligations.

7. **Droit d'information des personnes concernées**

Le Titulaire, au moment de la collecte des données, fournit aux personnes concernées l'information relative aux traitements de données qu'il réalise.

8. **Exercice des droits des personnes**

Dans la mesure du possible, le Titulaire doit aider l'ADEME à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Le Titulaire doit répondre, au nom et pour le compte de l'ADEME et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la prestation prévue par le présent marché.

9. **Notification des violations de données à caractère personnel**

Le Titulaire notifie à l'ADEME toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance en adressant un email avec accusé de réception à : rgpd@ademe.fr. Cette notification est accompagnée de toute documentation utile afin de permettre à l'ADEME, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

10. **Aide du Titulaire dans le cadre du respect par l'ADEME de ses obligations**

Le Titulaire aide l'ADEME, le cas échéant, pour la réalisation d'analyses d'impact relative à la protection des données.

Le Titulaire aide l'ADEME, le cas échéant, pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. **Mesures de sécurité**

Le Titulaire s'engage à mettre en œuvre les mesures de sécurité suivantes :

Pseudonymisation des données à caractère personnel (si applicable)[6]
Chiffrement des données à caractère personnel[7]
Moyens permettant de garantir la confidentialité et l'intégrité des données[8]
Moyens permettant de rétablir la disponibilité des données et leur accès dans des délais appropriés en cas d'incident physique ou technique[9]
Procédure visant à tester, analyser, évaluer l'efficacité des mesures de sécurité

12. **Sort des données**

Au terme du marché, le Titulaire s'engage à renvoyer toutes les données à caractère personnel à l'ADEME sauf instruction différente reçue de l'ADEME. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Titulaire. Une fois détruites, le Titulaire doit justifier par écrit de la destruction.

---

[6] La « pseudonymisation » consiste à remplacer les noms/prénoms des personnes par un numéro d'identifiant. La pseudonymisation peut être obligatoire : par exemple, pour les traitements à des fins de recherche qui contiennent des données de santé ou des données génétiques.

[7] A minima, il faut chiffrer les données lors de la transmission de données personnelles

[8] Guide de la CNIL : https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles

Vérifier a minima :

- Accès aux locaux contrôlés (alarmes anti-intrusion, détecteurs de fumée, contrôle d'accès dédié à la salle informatique, règles d'accès des visiteurs)
- Accès aux données limitées aux seules personnes habilitées, accès par identifiant / mot de passe régulièrement modifié (https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires)
- Protection du réseau interne (gestion des connexions wi-fi, VPN si accès à distance, limitation des flux réseaux)
- Postes de travail sécurisés avec verrouillage automatique des sessions, pare-feu, antivirus,
- Journalisation des données

[9] Guide de la CNIL : https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles

Vérifier a minima :

- Stockage sur réseau
- Sauvegardes régulières dans un endroit distinct
- Plan de reprise des données en cas d'incident

13. **Délégué à la protection des données**

Le Titulaire communique à l'ADEME **le nom et les coordonnées de son délégué à la protection des données,** s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

14. **Registre des catégories d'activités de traitement**

Le Titulaire déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte de l'ADEME comprenant les éléments imposés par le règlement européen sur la protection des données.

15. **Documentation**

Le Titulaire met à la disposition de l'ADEME **la documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par l'ADEME ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

III. Obligations de l'ADEME vis-à-vis du Titulaire

L'ADEME s'engage à :

1. fournir au Titulaire les données visées au II des présentes clauses ;

2. documenter par écrit toute instruction concernant le traitement des données par le Titulaire ;

3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du Titulaire ;

4. superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire ».