# Annexe 1 AU CCAP (ACCORD-CADRE N° 24M032-01H LOT 1) : protection Des données À caractère personnel

1. **objet et champ d’application**

Dans le cadre de leurs relations contractuelles, les parties s’engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

Les présentes clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

Les clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

En cas d'évolution de la réglementation sur la protection des données à caractère personnel en cours d'exécution du marché, les modifications nécessaires pour se conformer aux règles nouvelles, donnent lieu à la signature d'un avenant par les parties au marché ou, en l'absence d'accord entre les parties, à une modification unilatérale par l'acheteur.

Dans le cas où le titulaire a accès à des données à caractère personnel lors de la réalisation des prestations, il agit en qualité de sous-traitant au sens de l’article 4 du RGPD, et ce pour le compte de l’Assemblée nationale qui demeure le responsable de traitement.

La présente annexe a pour objet de définir les conditions dans lesquelles le sous-traitant s’engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

1. **Invariabilité des clauses**

Les parties s’engagent à ne pas modifier les clauses, sauf en ce qui concerne l’ajout d’informations aux annexes ou la mise à jour des informations qui y figurent.

Les parties ne sont pour autant pas empêchées d’inclure les clauses contractuelles types définies dans les présentes clauses dans un contrat plus large, ni d’ajouter d’autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses ou qu’elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

1. **Terminologie**

Le « responsable du traitement » (article 4.7 du RGPD : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (...)* ») : l’acheteur au sens du code de la commande publique ;

Le « sous-traitant » (article 4.8 du RGPD : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement*») : le titulaire du marché public ;

Le sous-traitant du sous-traitant ou sous-traitant ultérieur (article 28.2 du RGPD : lorsque le « *sous-traitant recrute un autre sous-traitant* ») : le sous-traitant au sens du droit de la commande publique ;

L’« autorité de contrôle » (article 4.21 du RGPD : « *une autorité publique indépendante qui est instituée par un État membre en vertu de l’article 51* ») : la Commission nationale de l’informatique et des libertés (CNIL).

1. **Propriété intellectuelle**

Il est rappelé que les « données » auxquelles le titulaire a accès dans le cadre des présentes, constituent des connaissances antérieures.

Ces données sont et demeurent la propriété exclusive de l’Assemblée nationale qui restera l’unique propriétaire des traitements, enrichissements et améliorations qui pourraient leur être apportées.

1. **Interprétation**

Lorsque des termes définis dans le règlement (UE) 2016/679 figurent dans les clauses, ils s’entendent comme dans le règlement en question.

Les présentes clauses doivent être lues et interprétées à la lumière des dispositions du règlement (UE) 2016/679 et de la loi Informatique et libertés respectivement.

Les présentes clauses ne doivent pas être interprétées d’une manière contraire aux droits et obligations prévus par le règlement (UE) 2016/679 et/ou par la loi Informatique et libertés, ou d’une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

1. **Description du traitement faisant l’objet de la sous-traitance**

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour l’exécution du présent marché.

La nature des opérations réalisées sur les données est la consultation, la collecte, l’enregistrement, l’organisation, la conservation, l’envoi des données et la destruction des données. Les appels ne sont pas enregistrés.

Les données à caractère personnel traitées sont les suivantes :

* Pour les agents de l’Assemblée nationale en charge du marché : le nom, le prénom, le numéro téléphonique et le courriel (e-mail) ;
* Pour les autres catégories de personnes concernées bénéficiant de la cellule d’écoute : l’identité (nom, prénom) ou le pseudonyme (au choix de l’agent), les coordonnées (au choix de l’agent), les informations fournis sur la vie professionnelle et personnelle.

Les catégories de personnes concernées par le traitement des données à caractère personnel sont les députés, leurs collaborateurs de droit privé, leurs stagiaires, les fonctionnaires, les agents contractuels de droit public, les apprentis et les stagiaires de l’Assemblée nationale, les agents contractuels de droit privé de l’AGRAN et de l’association gérant la Boutique de l’Assemblée nationale ainsi que les personnels du titulaire en charge de l’exécution du marché.

La base légale du traitement est l’article 6 (1) f du règlement général sur la protection des données – RGPD. Ce traitement de données est nécessaire aux fins des intérêts légitimes poursuivis par l’Assemblée nationale.

Les finalités du traitement sont :

* Pour les données issues des agents de l’Assemblée nationale en charge du marché :
  + la gestion des demandes de formation et le suivi,
  + la réception des livrables,
  + la réalisation des actions de coordination et de pilotage le cas échéant,
  + l’assistance technique, le cas échéant,
  + la destruction ou la transmission des données afin de protéger ces données,
  + et toutes autres finalités nécessaires à la bonne exécution du marché ;
* Pour les données issues des autres catégories de personnes concernées bénéficiant de la cellule d’écoute :
  + la gestion des entretiens téléphoniques et des signalements au Déontologue de l’Assemblée nationale,
  + la mise en place de statistiques sur les données anonymisées.

Les données seront conservées au maximum un an à compter du dernier entretien téléphonique réalisé avec la personne concernée ou au plus tard jusqu’au traitement du dossier.

Pour l’exécution du service objet du présent contrat, le responsable met à la disposition du titulaire les pièces du marché.

1. **Obligations du sous-traitant vis-à-vis du responsable de traitement**

Le sous-traitant s'engage à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet de la sous-traitance, sauf instruction complémentaire du responsable de traitement.

2. traiter les données conformément aux instructions documentées du responsable de traitement. Si le sous-traitant 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 États membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant 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’État membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement.

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 (« privacy by design »).**

6. **La sous-traitance ultérieure**

Le sous-traitant, titulaire du marché, peut faire appel à un autre sous-traitant (ci-après, « ***le sous-traitant ultérieur***») pour mener des activités de traitement spécifiques. Dans ce cas, il doit recueillir l’accord préalable écrit spécifique du responsable du traitement concernant l’ajout ou le remplacement d’autres prestataires. Pour ce faire, il remplit une déclaration relative à la présentation d’un sous-traitant ultérieur, en vertu de l’article L. 2193-5 du code de la commande publique (imprimé DC4). Le formulaire doit indiquer clairement les activités de traitement concernées, l'identité et les coordonnées du sous-traitant ultérieur et les dates du contrat de sous-traitance ultérieur. Le sous-traitant soumet la demande d’autorisation spécifique au moins six (6) jours avant le recrutement du sous-traitant ultérieur en question. La liste des sous-traitants ultérieurs autorisés par le responsable du traitement figure à l’annexe I-bis que les parties tiennent à jour.

Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d’un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés.

À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure nécessaire à la protection des secrets d’affaires ou d’autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d’en diffuser une copie.

Le sous-traitant demeure pleinement responsable, à l’égard du responsable du traitement, de l’exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

Le sous-traitant convient avec le sous-traitant ultérieur d’une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d’exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d’effacer ou de renvoyer les données à caractère personnel.

7. **Transferts de données hors de l’Union européenne ou traitement par un prestataire soumis à un droit extraterritorial tiers**

Le sous-traitant s’engage à héberger les données exclusivement sur le territoire de l’un des États membres de l’Union européenne ou membre de l’Espace économique européen, qu’il prenne en charge lui-même cet hébergement ou fasse appel à un Sous-traitant ultérieur.

Les opérations d’administration et de supervision du service doivent être réalisées depuis l’Union européenne.

Le sous-traitant s’engage à informer le responsable de traitement de la localisation physique des serveurs hébergeant les données à caractère personnel.

Si le sous-traitant est localisé hors de l’Union européenne, ou s’il est localisé dans l’Union, mais soumis à un droit extraterritorial tiers, il doit préalablement fournir au responsable du traitement les garanties exigées par l’article 46 du règlement (UE) 2016/679 pour validation par le délégué à la protection des données de l’Assemblée nationale.

Le sous-traitant doit fournir au responsable de traitement une liste de l’ensemble des tiers qui peuvent accéder aux Données et des pays destinataires mise à jour. En cas de modification des pays destinataires par le sous-traitant, ce dernier doit en informer préalablement le responsable de traitement, afin qu’il puisse émettre des objections à cet égard.

En cas de requête provenant d’une autorité administrative ou judiciaire reçue par le sous-traitant, ce dernier s’engage à en informer immédiatement le Responsable de traitement.

8. **Le droit d’information des personnes concernées**

Il appartient au titulaire de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données. La formulation et le format de l’information doivent être convenus avec l’Assemblée nationale avant la collecte des données.

9. **L’exercice des droits des personnes**

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d’exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique au représentant du responsable de traitement (Annexe I-bis).

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

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les 48 heures après en avoir pris connaissance et par tout moyen permettant la traçabilité des échanges : courrier, courriel, télécopie. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l’autorité de contrôle compétente.

La notification contient au moins :

* la description de la nature de la violation de données à caractère personnel (catégories et nombre approximatif de personnes concernées par la violation et d'enregistrements de données) ;
* le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact ;
* la description des conséquences probables de la violation de données à caractère personnel ;
* la description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les mêmes éléments que la notification ci-dessus.

11. **Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations**

Le sous-traitant aide le responsable de traitement pour la réalisation d’analyses d’impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l’autorité de contrôle.

12. **Mesures de sécurité**

Le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

* la pseudonymisation et le chiffrement des données à caractère personnel ;
* les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
* les moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
* une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

13. **Le sort des données**

Dans un délai d’un (1) mois calendaire avant la date de fin du marché, le titulaire interroge le responsable de traitement sur le sort des données traitées. Au choix du responsable de traitement, le sous-traitant s’engage à :

* détruire toutes les données à caractère personnel ;
* à renvoyer toutes les données à caractère personnel au responsable de traitement ;
* à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

14. **Le délégué à la protection des données**

Le sous-traitant communique au responsable de traitement **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.

15. **Registre des catégories d’activités de traitement**

Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d’activités de traitement effectuées pour le compte du responsable de traitement comprenant :

* le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
* les catégories de traitements effectués pour le compte du responsable du traitement ;
* le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
* dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
* la pseudonymisation et le chiffrement des données à caractère personnel ;
* des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
* des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
* une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

16. **Documentation - Audit**

Le sous-traitant met à la disposition du responsable de traitement, dans le délai fixé par la demande, la documentation nécessaire pour démontrer le respect de toutes ses obligationset pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Chaque partie se réserve le droit de refuser de fournir à l’autre partie des secrets d’entreprise et de commerce, un savoir-faire opérationnel et toute information dont l’audit présenterait un risque de sécurité pour la Partie auditée.

17. **Non-respect des clauses et résiliation**

Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou de la loi Informatique et libertés, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu’à ce que ce dernier se soit conformé aux présentes clauses ou jusqu’à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s’il n’est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

Le responsable peut également enjoindre au sous-traitant de se mettre en conformité sous astreinte, conformément à l’article « pénalités » du CCAP. En outre, en cas d’inaction ou de mesures non probantes, le marché pourra être résilié aux torts du titulaire.

1. **Obligations du responsable de traitement vis-à-vis du sous-traitant**

Le responsable de traitement s’engage à :

* fournir au sous-traitant les données à caractère personnel nécessaires pour l’exécution du présent marché ;
* documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
* veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement de la part du sous-traitant ;
* superviser le traitement, y compris réaliser, le cas échéant des audits et des inspections auprès du sous-traitant.

# I-*bis* - Liste des parties ET DES SOUS-TRAITANTS ULTÉRIEURS

**Responsables du traitement** :

* 1. Responsable du traitement :
  2. Délégué à la protection des données du responsable du traitement :

1. Responsable du traitement :

Assemblée nationale

126, rue de l’Université

75355 PARIS 07 SP

1. Délégué à la protection des données du responsable du traitement pour tous les services de l’Assemblée nationale :

Monsieur le délégué à la protection des données, Assemblée nationale,

126, rue de l’Université

75355 PARIS 07 SP

[dpo@assemblee-nationale.fr](mailto:dpo@assemblee-nationale.fr)

**Sous-traitant(s)** [Identité et coordonnées du ou des sous-traitants et, le cas échéant, du délégué à la protection des données du sous-traitant]:

*Le tableau ci-dessous doit être complété par le candidat.*

|  |  |
| --- | --- |
| **Titulaire (ou mandataire du groupement)** | Nom :    Adresse :  Nom, fonction et coordonnées de la personne de contact : |
| **Cotraitant n°1** | Nom :  Adresse :  Nom, fonction et coordonnées de la personne de contact : |

**Sous-traitant(s) ultérieur(s)**

Cette partie doit être complétée en cas d’autorisation spécifique de sous-traitants ultérieurs.

Le responsable du traitement a autorisé le recours aux sous-traitants ultérieurs suivants :

|  |  |
| --- | --- |
| **Sous-traitant ultérieur n°1** | Nom :  Adresse :  Nom, fonction et coordonnées de la personne de contact :  Description du traitement : |
| **Sous-traitant ultérieur n°2** | Nom :  Adresse :  Nom, fonction et coordonnées de la personne de contact :  Description du traitement : |
| **Sous-traitant ultérieur n°3** | Nom :  Adresse :  Nom, fonction et coordonnées de la personne de contact :  Description du traitement : |

# I-*ter* - Mesures techniques et organisationnelles

Conformément aux dispositions du I, le sous-traitant doit décrire les mesures de sécurité techniques et organisationnelles mises en œuvre afin de garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

Le sous-traitant doit être en capacité d’apporter la preuve des mesures prises et de leur respect pour satisfaire aux différents besoins énumérés ci-après. Si jugées insuffisantes par le responsable de traitement, ce dernier pourra exiger du sous-traitant qu’il renforce certaines mesures.

**Le sous-traitant s’engage à mettre en œuvre les mesures suivantes[[1]](#footnote-1) :**

Mesures de chiffrement des données à caractère personnel ;

Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

Mesures de redondance et de sauvegardes assurant de disposer de moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique ;

Procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;

Mesures d’identification et d’autorisation de l’utilisateur ;

Mesures de protection des données pendant la transmission ;

Mesures de protection des données pendant le stockage ;

Mesures visant à garantir la sécurité physique des sites où les données à caractère personnel sont traitées ;

Mesures visant à garantir l’enregistrement des événements ;

Mesures visant à assurer la configuration des systèmes, y compris la configuration par défaut ;

Mesures de gouvernance et de gestion de l’informatique interne et de la sécurité informatique ;

Mesures de certification/assurance des procédés et produits ;

Mesures visant à garantir la qualité des données ;

Mesures visant à garantir une conservation limitée des données ;

Mesures visant à garantir la responsabilité ;

Mesures garantissant l’effacement.

Transmettre à l’Assemblée nationale sa politique de sécurité des systèmes d’information et l’informer de ses évolutions;

Documenter et mettre œuvre un plan de continuité d’activité prenant en compte la sécurité de l’information.

**Le sous-traitant s’engage à prendre les mesures supplémentaires suivantes :**

*Le candidat complète cette partie le cas échéant.*

**Description concrète des mesures prises par le** **sous-traitant :**

*Les mesures techniques et organisationnelles, pour lesquelles le candidat s’engage, doivent faire l’objet d’une description concrète, et non pas générique.*

1. Le candidat coche les cases correspondantes [↑](#footnote-ref-1)