



**Annexe 2 : CONTRAT DE SOUS-TRAITANCE SUR LE TRAITEMENT
DES DONNEES A CARACTERE PERSONNEL
(Conformément à l'article 28 du RGPD)**

Entre :

Le Sénat, Palais du Luxembourg, 15 rue de Vaugirard, 75006 Paris

Ci-après dénommé « le Sénat » ou « le responsable de traitement »

Et

L'attributaire du marché afférent au CCAP auquel le présent document est annexé

Ci-après dénommée « la Société » ou « le sous-traitant »

La présente annexe a pour objet de décrire les obligations respectives de la Société et du Sénat en matière de données personnelles et fait partie intégrante du CCAP.

Préambule : Définitions spécifiques

Données personnelles désigne toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro de téléphone, une adresse email, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Traitement désigne toute opération ou tout ensemble d'opérations qui est réalisé sur les données à caractère personnel, de manière automatisée ou non, tels que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, le verrouillage, l'effacement ou la destruction.

Fichier désigne tout ensemble structuré de données personnelles, accessible, que cet ensemble soit centralisé, décentralisé, ou réparti de manière fonctionnelle ou géographique.

Instruction désigne toute instruction écrite ou par saisie de données reçue par la Société de la part du Sénat en vertu du marché, et ayant pour objet le traitement de données personnelles.

Responsable de Traitement désigne 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 ; dans le cadre des présentes, le responsable de traitement est le Sénat.

Sous-traitant désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte du responsable du traitement; dans le cadre des présentes, le sous-traitant est la Société.

1. Objet et réglementation applicable

Les présentes clauses ont 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.

Dans le cadre des présentes, les parties s'engagent à respecter leurs obligations, respectivement en leur qualité de responsable de traitement et de sous-traitant telles que prévues notamment par :

- Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, ci-après, « le RGPD » et par la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique ;
- En toute hypothèse et, le cas échéant, par les lois locales susceptibles d'affecter et de s'appliquer aux données personnelles en fonction du lieu d'hébergement des dites données personnelles ;
- Les textes et décisions émanant d'autorités administratives indépendantes et notamment ceux de la Commission Nationale de l'Informatique et des Libertés (CNIL) ;
- La jurisprudence émanant des tribunaux nationaux et communautaires applicable en matière de données personnelles.

Ci-après « la réglementation concernant les données personnelles ».

2. Durée

Le présent accord entre en vigueur à compter de la notification du présent marché et jusqu'à sa date de fin.

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

Le Sénat confie à la Société le(s) traitement(s) ayant les caractéristiques suivantes :

	Objet	Finalité	Durée	Type de données à caractère personnel	Catégories de personnes concernées
Traitement N°1	<i>Conservation, classement, utilisation, et consultation de données à caractère personnel</i>	<i>Missions d'assistance, conseil aux utilisateurs et maintenance de niveau 1 des équipements pour l'ensemble des utilisateurs du Sénat, telles que décrit à l'article 4.1 du CCTP</i>	Durée du marché	<i>Données liées à l'identification des personnes, données de connexion (logs)</i>	<i>Ensemble des utilisateurs des systèmes d'information du Sénat</i>
Traitement N°2	<i>Conservation, classement, utilisation, et consultation de données à caractère personnel</i>	<i>Missions de gestion des équipements informatiques fournis par le Sénat, telles que décrit à l'article 4.2 du CCTP</i>	Durée du marché	<i>Données liées à l'identification des personnes, données de connexion (logs)</i>	<i>Ensemble des utilisateurs des systèmes d'information du Sénat</i>
Traitement N°3	<i>Conservation, classement, utilisation, et consultation de données à caractère personnel</i>	<i>Opérations d'analyses statistiques et relevés d'usage</i>	Durée du marché	<i>Données liées à l'identification des personnes, données de connexion (logs)</i>	<i>Ensemble des utilisateurs des systèmes d'information du Sénat</i>

4. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

- Traiter lesdites données personnelles uniquement sur la base d'instructions du Sénat et dans la mesure raisonnablement nécessaire ou appropriée pour l'exécution des présentes ;
- Ne pas divulguer ces données personnelles excepté dans les conditions prévues aux présentes ou sous réserve du consentement écrit du Sénat ;
- Ne pas vendre, céder, louer ou exploiter commercialement ces données personnelles ;
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :
 - 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.
- 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 ;
- Ne pas effectuer d'études statistiques sur les données personnelles ou de traitement sans l'accord préalable du Sénat pour chaque type d'étude ;
- Respecter la durée de conservation des données personnelles au regard des finalités pour lesquelles elles ont été collectées ou transmises et à supprimer les données personnelles à expiration de la durée de conservation et fournir un certificat de suppression des dites données ;
- Mettre à disposition du Sénat les informations nécessaires pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le Sénat ou un autre auditeur qu'il aura mandaté ;
- Notifier immédiatement toute modification ou changement pouvant impacter le traitement des données personnelles ;
- Communiquer au Sénat, dès la notification du marché, 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 RGPD.

Le sous-traitant s'interdit par ailleurs :

- La consultation, le traitement de données personnelles autres que celles concernées par le présent marché et ce, même si l'accès à ces données est techniquement possible ;
- De prendre copie ou de stocker, quelles qu'en soient la forme et la finalité, tout ou partie des données personnelles qui lui ont été transmises ou qu'il a collectées au cours de l'exécution du marché en dehors de l'exécution du présent Marché ;

5. Sous-traitance ultérieure

Le sous-traitant 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 informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur 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 ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

Le sous-traitant initial s'oblige à :

- Signer un contrat écrit avec son sous-traitant, lequel fera expressément référence aux présentes et mettra à la charge du sous-traitant des obligations identiques à celles contenues à la présente annexe et qui lui incombent; le titulaire s'engage à communiquer à ses sociétés affiliées l'ensemble de leurs obligations résultant de la présente annexe ;
- Mettre à la charge de son sous-traitant toutes obligations incombant au sous-traitant définies dans la présente annexe pour que soient respectées la confidentialité, la sécurité et l'intégrité des données personnelles, et pour que lesdites données personnelles ne puissent être ni cédées ou louées à un tiers à titre gratuit ou non, ni utilisées à d'autres fins que celles définies au marché ;
- Informer le Sénat de tout projet de modification des dispositions du contrat signé et/ou des obligations relatives à la protection des données personnelles mises à la charge du sous-traitant ;
- En cas de sous-traitance ultérieure, le Sénat se réserve le droit de procéder à toutes vérifications qui lui paraîtraient utiles pour constater le respect par le titulaire des obligations précitées, et notamment au moyen d'audits. Le sous-traitant s'engage à répondre aux demandes d'audits du Sénat, effectuées par lui-même ou par un tiers de confiance qu'il aura sélectionné et missionné à cette fin. Les audits doivent permettre une analyse du respect par la Société des termes de la présente annexe et des dispositions applicables en matière de protection des données personnelles, notamment de s'assurer que des mesures de sécurité et de confidentialité adéquates sont mises en œuvre, qu'elles ne peuvent pas être contournées sans que cela ne soit détecté et que, dans une telle hypothèse ou dans toute autre hypothèse de survenance d'une faille de sécurité, une procédure de notification et de traitement est mise en œuvre par le prestataire pour y remédier sans délai ;
- Le titulaire tient à jour une liste des sous-traitants auquel il fait appel dans le cadre du marché qu'il maintient à disposition du Sénat et lui communique à première demande de ce dernier.

Le sous-traitant initial, en cas de sous-traitance ultérieure autorisée, informera également le Sénat de toute modification prévue concernant l'ajout ou le remplacement de sous-traitants et s'engage à informer et à signer un contrat écrit avec tout nouveau sous-traitant.

6. Droit d'information des personnes concernées

Il appartient au Sénat d'informer les personnes concernées par les traitements de données à caractère personnel. Le sous-traitant s'engage à faire figurer, pour le compte du Sénat, une mention d'information à destination des personnes concernées comprenant les informations prescrites par l'article 13 et/ou 14 du RGPD. La formulation et le format de l'information doivent être convenus avec le Sénat avant la collecte des données.

7. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le Sénat 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 ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

Dès lors, si une personne concernée devait contacter directement le titulaire pour exercer ses droits, ce dernier communiquera au Sénat dans un délai de trois (3) jours ouvrés les demandes d'exercice de ces droits qui lui seront parvenues à l'adresse suivante :

dpd@senat.fr

8. Notification des violations de données et des incidents de sécurité

Le sous-traitant s'engage à notifier dès qu'il en a connaissance et dans un délai de 24 heures au Sénat, et en

particulier au Responsable de la sécurité des systèmes d'informations (RSSI) et au Délégué à la protection des données (DPD) du Sénat (rssi@senat.fr, dpd@senat.fr) tout incident entraînant accidentellement ou de manière licite la perte, l'altération, la divulgation ou l'accès non autorisé à des données personnelles faisant l'objet du traitement.

Cette notification doit préciser :

- La nature et, si elles sont connues, les conséquences probables de l'incident ;
- Les mesures déjà prises par titulaire ou celles qui sont proposées pour y remédier dans la mesure où elles relèvent de sa responsabilité;
- Les personnes auprès desquelles des informations supplémentaires peuvent être obtenues;
- Lorsque cela est possible, une estimation du nombre de personnes susceptibles d'être impactées par l'incident.

Dès qu'il est informé d'un incident dont il est à l'origine, le titulaire procède à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dans un délai aussi rapide que possible et de faire en sorte d'en diminuer l'impact pour les personnes concernées.

Le titulaire s'engage à informer le Sénat de ses investigations et ce de manière régulière.

Les parties s'engagent à collaborer activement pour qu'elles soient en mesure de répondre à leurs obligations réglementaires et contractuelles.

Il revient au Sénat, en tant que responsable du traitement, de notifier cette violation de données personnelles à l'autorité de contrôle compétente ainsi que, le cas échéant, à la personne concernée dans un délai raisonnable après en avoir pris connaissance.

9. Mesures de sécurité

Le sous-traitant s'engage à assurer la sécurité -à savoir la disponibilité, la confidentialité, l'intégrité et la traçabilité- des données personnelles qui lui sont confiées et auxquelles il pourrait avoir accès dans son environnement (poste de travail par exemple).

Les dispositions du présent article visent expressément les mesures associées à un accès aux données personnelles sur le ou les systèmes d'information du sous-traitant.

À ce titre, le sous-traitant s'engage à mettre en place des mesures de sécurité organisationnelles ainsi que des mesures de sécurité techniques appropriées pour préserver les données personnelles et les protéger contre toute déformation, altération, destruction fortuite ou illicite, endommagement, perte, divulgation ou accès par des tiers non autorisés, telles que décrites dans les sous-paragraphes (a) et (b) ci-dessous.

Le sous-traitant s'engage à maintenir ces mesures et moyens pour toute la durée du marché et à défaut, à en informer immédiatement le Sénat et notamment le RSSI. En tout état de cause, le sous-traitant s'engage, en cas de changement des moyens visant à assurer la sécurité des données personnelles, à les remplacer par des moyens équivalents ou d'une qualité supérieure.

a) Mesures de sécurité organisationnelles

Le sous-traitant s'engage à mettre en place a minima les mesures de sécurité organisationnelles suivantes :

- Présence et mise en œuvre d'une politique de gestion des habilitations et de sécurité appropriées pour restreindre l'accès aux données personnelles aux seules personnes qui ont le droit d'en connaître ;
- Mise en place d'un engagement de confidentialité visant à ce que les personnes autorisées à traiter les données personnelles soient soumises à une obligation de confidentialité étant entendu que cette obligation peut être prise par le biais du contrat de travail de la personne concernée ;
- Mise en place de mesures pour empêcher le transfert des données personnelles à toute personne/entité non autorisée ;
- Mise en place de campagnes de sensibilisation de son personnel à la sécurité des données, notamment au moyen de procédures internes, chartes, engagements de confidentialité, etc.

b) Mesures de sécurité techniques

De manière générale, il est formellement interdit au sous-traitant de faire transiter des données personnelles sans que le canal de communication de celles-ci soit sécurisé ou sans que les données personnelles soient chiffrées. Par ailleurs, le Sous-traitant s'engage à ce que les mesures de sécurité techniques mises en place répondent à minima aux exigences suivantes :

- Mise en place d'outils permettant de s'assurer que les données personnelles ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation au cours de leur transfert électronique, de leur transport ou de leur stockage, et que les entités destinataires de tout transfert de données personnelles via les installations servant au transfert de données peuvent être identifiées et vérifiées ;
- Mise en place de contrôles permettant de s'assurer que les données personnelles sont protégées contre les destructions ou les pertes accidentelles ;
- Mise en place de mesures permettant de cloisonner les données personnelles traitées dans le cadre des présentes des données personnelles de ses autres clients ;
- Mise en place de mesures sécurisées d'authentification pour l'accès à ses équipements ;
- Mises en place d'un système de journalisation des activités des utilisateurs, des anomalies et des événements liés à la sécurité ;
- Mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications.

Le Sous-traitant s'engage également à :

- Mettre en place 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 ;
- Engager une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

10. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à renvoyer toutes les données à caractère personnel au responsable de traitement.

Le sous-traitant s'engage à supprimer dans un délai de quinze (15) jours au terme du marché l'intégralité des données personnelles qu'il traite dans le cadre des présentes et de détruire toutes les copies existantes dans ses systèmes d'information, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation de ces données à caractère personnel. Une fois les données détruites, le sous-traitant justifie par écrit de la destruction et l'adresse au Sénat.

11. Transfert de données personnelles en dehors de l'Union européenne

Les parties reconnaissent que l'exécution des prestations selon les modalités envisagées par le Sénat n'implique pas de transfert de données hors de l'Union européenne.

12. Coopération avec les autorités de contrôle

En cas de contrôle d'une autorité compétente en relation avec les données personnelles traitées dans le cadre des présentes, les parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concerne que les traitements mis en œuvre par le sous-traitant en tant que responsable du traitement, le sous-traitant fait son affaire d'un tel contrôle et s'interdit de communiquer ou de faire état des données personnelles traitées pour le compte du Sénat.

Dans le cas où le contrôle mené chez le sous-traitant concerne les traitements mis en œuvre au nom et pour le compte du Sénat, le sous-traitant s'engage à en informer immédiatement ce dernier, dans la mesure permise par la loi, et à ne prendre aucun engagement pour lui.

13. Obligations particulières du sous-traitant

a) Tenue du registre

Le sous-traitant du Sénat, s'engage à tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, conformément au RGPD et 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 RGPD, 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.

b) Analyse d'impact (PIA)

Conformément à l'article 28.3 du RGPD, le titulaire s'engage à collaborer avec le Sénat pour permettre à celui-ci de réaliser toute analyse d'impact conformément à l'article 35 du RGPD, que ce dernier décidera de mener afin d'évaluer la probabilité et la gravité des risques inhérents à un traitement de données à caractère personnel, compte tenu de sa nature, de sa portée, de son contexte, de ses finalités et des sources du risque. Le sous-traitant assiste le Sénat efficacement afin que cette analyse puisse comporter obligatoirement les éléments suivants :

- Une description systématique des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- Une évaluation des risques sur les droits et libertés des personnes concernées ;
- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

c) Code de conduite / Certification

Le sous-traitant fera ses meilleurs efforts pour appliquer un code de conduite approuvé au titre du RGPD ou pour obtenir une certification.

14. Obligations du responsable de traitement vis à vis du sous-traitant

Le Sénat s'engage à :

- 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 RGPD de la part du sous-traitant ;
- Superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant ;
- De manière générale, respecter les obligations à sa charge conformément à la réglementation applicable sur la protection des données à caractère personnel.