



ANNEXE 1 AU CCAP 2024-020-DSI-NB

REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES

CLAUSES PARTICULIERES A LA PROTECTION DES DONNEES

PERSONNELLES

Dans le cadre de l'exécution du marché public, le titulaire du marché pourra être amené à avoir accès et traiter des données à caractère personnel, au sens du Règlement Général sur la Protection des Données (EU) 2016/679, pour le compte du CONSEIL D'ETAT.

Dans le cadre de la mise en œuvre de ce traitement de données à caractère personnel, le CONSEIL D'ETAT est le responsable du traitement et le titulaire du marché est le sous-traitant des données personnelles au sens du Règlement (UE) 2016/679. Le terme de sous-traitant en droit des données personnelles est à ne pas confondre avec le terme de sous-traitant au sens de la réglementation de la commande publique. Dès lors, les dispositions suivantes ont pour objectif d'encadrer les droits et obligations de chacune des parties au cours du traitement de données à caractère personnel tel que l'impose l'article 28. 3 du Règlement (UE) 2016/679.

1. Description du traitement faisant l'objet du présent marché

Le titulaire du marché est expressément autorisé par le CONSEIL D'ETAT à traiter pour son compte les données à caractère personnel nécessaires pour fournir les prestations spécifiées dans le marché.

La nature des opérations réalisées sur les données, la ou les finalité(s) du traitement, les données à caractère personnel traitées, et les catégories de personnes concernées sont spécifiées dans l'annexe 2 du CCAP relative aux données à caractère personnel à compléter.

2. Pouvoir d'instruction du Responsable de Traitement

Le titulaire du marché est tenu à tout moment de respecter les instructions générales et spécifiques du CONSEIL D'ETAT relatives au traitement des données. Le titulaire du marché s'engage à fournir sur demande du CONSEIL D'ETAT les informations requises aux fins de permettre un contrôle

effectif du CONSEIL D'ETAT des modalités de traitement des données et à rendre disponible la documentation s'y rapportant.

3. Transfert des données hors de l'Espace Economique Européen

Dans le cadre du traitement des Données pour le compte du CONSEIL D'ETAT, le titulaire du marché s'engage à ne réaliser aucun transfert desdites Données hors de l'Espace Economique Européen, au sens de la réglementation applicable, sauf à recueillir le consentement préalable exprès du CONSEIL D'ETAT.

Par exception à ce qui précède, si le titulaire du marché est tenu de procéder à un transfert des données vers un pays tiers à l'Espace Economique Européen 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 le CONSEIL D'ETAT de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

4. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le titulaire du marché s'engage à :

- Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la prestation et conformément aux instructions documentées du CONSEIL D'ETAT ;
Si le titulaire du marché considère qu'une instruction constitue une violation du Règlement (UE) 2016/679 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 le CONSEIL D'ETAT ;
- Garantir la confidentialité des données 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.
- Apporter au responsable de traitement toute information et appui utiles pour la réalisation, le cas échéant :
 - D'analyse d'impact relative à la protection des données ;
 - De consultation préalable auprès de l'autorité de contrôle compétente.

5. Recours à des tiers prestataires par le sous-traitant

Le titulaire du marché ne peut sous-traiter tout ou partie des prestations de traitements des données auprès de tiers (ci-après « sous-traitant ultérieur ») qu'après avoir obtenu l'autorisation écrite, préalable et spécifique du CONSEIL D'ETAT.

Si le CONSEIL D'ETAT accepte la sous-traitance proposée, il appartient au titulaire du marché de s'assurer que ce 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 (UE) 2016/679. Le titulaire du marché s'engage par ailleurs à conclure avec le sous-traitant ultérieur un contrat comportant les mêmes obligations quant à la protection des Données que celles convenues aux présentes entre le CONSEIL D'ETAT et le titulaire du marché.

Lorsque le titulaire du marché a recours à un sous-traitant ultérieur, le CONSEIL D'ETAT, dispose d'un droit d'audit et de contrôle de ce dernier.

Le titulaire du marché justifiera, à première demande du CONSEIL D'ETAT, des engagements contractuels de tout sous-traitant ultérieur participant au traitement des données, si nécessaire en communiquant une copie des documents contractuels s'y rapportant.

6. Droit des personnes concernées

Dans la mesure du possible, le titulaire du marché doit aider le CONSEIL D'ETAT à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Lorsque les personnes concernées exercent auprès du titulaire du marché des demandes d'exercice de leurs droits, celui-ci doit adresser ces demandes dès réception par courrier électronique à l'adresse : donneespersonnelles@conseil-etat.fr.

7. Mesures de sécurité

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

Le titulaire s'engage à maintenir ces mesures et moyens pour toute la durée du marché et à défaut, à en informer immédiatement le CONSEIL D'ETAT.

En tout état de cause, le titulaire du marché s'engage, en cas de changement des moyens visant à assurer la sécurité, l'intégrité et la confidentialité des données personnelles, à les remplacer par des moyens équivalents ou d'une performance supérieure.

(a) Mesures de sécurité organisationnelles

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

- Présence d'une politique d'habilitations individuelles et de sécurité appropriées pour restreindre l'accès aux données personnelles aux seules personnes qui ont à 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;
- Elaboration de mesures restrictives d'accès aux données personnelles permettant de s'assurer que les personnes habilitées à utiliser le système de traitement de données personnelles ne puissent accéder qu'aux données personnelles auxquelles elles sont habilitées à accéder conformément à leurs droits d'accès et que, dans le cadre du traitement et de l'utilisation après stockage, les données personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation ;
- 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 des utilisateurs des applications à la sécurité et à la confidentialité 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 titulaire de faire transiter des données personnelles sans que le canal de communication de celles-ci soit sécurisé.

Par ailleurs, le titulaire s'engage à ce que les mesures de sécurité techniques mises en place répondent a 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 veiller à ce que les données personnelles fournies par le Conseil d'Etat puissent être traitées distinctement des données personnelles de ses autres clients en utilisant des séparations logiques ;
- Mesures sécurisées d'authentification pour l'accès à ses équipements ;
- Mesures de sécurisation physique des locaux, du réseau interne, des matériels, des serveurs et des applications ;

- En tout état de cause, assurer les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ainsi que 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 évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin d'assurer la sécurité du traitement.

8. Notification des violations de données par le titulaire du marché.

Le titulaire du marché notifie au CONSEIL D'ETAT toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance. Cette notification ne pourra être valablement effectuée que dans la mesure où elle sera réalisée par courriel à l'adresse : donneespersonnelles@conseil-etat.fr.

Cette notification doit être accompagnée de toute documentation utile afin de permettre au CONSEIL D'ETAT, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Cette documentation comprendra les éléments suivants :

- La description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées ainsi que le volume de données compromises ;
- Tous éléments nécessaires au CONSEIL D'ETAT (ou personne désignée par celui-ci) pour évaluer les risques et impacts de cette violation des données et lui permettant de prendre toutes décisions et mesures utiles quant à sa gestion et suites à donner ;
- La description des mesures prises ou que le titulaire du marché 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.

Le titulaire du marché doit informer le CONSEIL D'ETAT dans tous les cas où le titulaire du marché ou des personnes que celui-ci a employées contreviennent aux dispositions relatives à la protection des données ou aux instructions du CONSEIL D'ETAT.

Le titulaire du marché s'engage à informer sans délai, dès qu'il en a connaissance, le CONSEIL D'ETAT de toute faille de sécurité affectant la confidentialité, l'intégrité ou la sécurité des données, intervenue de manière volontaire ou accidentelle, notamment toute atteinte, perte, vol, accès non autorisé, divulgation, destruction, altération des Données (ci-après « violation des données »).

La notification des violations des données au CONSEIL D'ETAT par le titulaire du marché et leur gestion font partie intégrante des prestations issues de l'exécution du marché public et ne donnera pas lieu à facturation complémentaire.

Dans l'hypothèse où le CONSEIL D'ETAT et le titulaire du marché seraient tous deux soumis à une obligation de notification à une autorité de contrôle (notamment auprès de la CNIL concernant les

violations de données personnelles), une coordination sera assurée entre les Parties par le CONSEIL D'ETAT quant à la cohérence du contenu et aux délais des différentes notifications.

Dans l'hypothèse où une information des personnes concernées s'avèrerait nécessaire, cette communication s'effectuera selon un calendrier et un contenu déterminé par le CONSEIL D'ETAT (et le cas échéant en concertation avec l'autorité de contrôle compétente).

En accord avec le CONSEIL D'ETAT, le titulaire du marché doit prendre les mesures appropriées pour prévenir toute nouvelle violation des données.

9. Pouvoirs de contrôle du Conseil d'Etat

Le CONSEIL D'ETAT est autorisé à effectuer des visites de contrôle sur le lieu d'activité du titulaire du marché avant le début du traitement puis par intervalles réguliers afin de vérifier que les mesures techniques et organisationnelles mises en œuvre par le titulaire du marché, telles qu'imposées dans le Cahier des clauses techniques particulières sont effectivement mises en œuvre.

Le CONSEIL D'ETAT se réserve la possibilité de réaliser ces missions de contrôle lui-même ou de mandater un expert à cette fin, à sa charge.

Il est convenu que les visites de contrôle s'effectueront comme suit :

Le CONSEIL D'ETAT pourra diligenter une fois par an une mission de contrôle sur place, dans les locaux du titulaire du marché. Outre cette mission de contrôle annuelle, le Conseil d'Etat pourra diligenter toute mission de contrôle ad hoc en cas de violation de données chez le titulaire du marché affectant l'intégrité, la confidentialité ou la sécurité des données.

Le CONSEIL D'ETAT doit respecter les processus opérationnels du titulaire du marché et, dans la mesure du possible, prévenir 48 heures avant toute visite en précisant le périmètre du contrôle.

Le titulaire du marché s'engage à faire son maximum pour assister la personne mandatée par le CONSEIL D'ETAT lors des contrôles et à lui donner l'accès aux locaux ainsi qu'aux équipements pertinents.

Le titulaire du marché s'engage à fournir sur demande du CONSEIL D'ETAT les informations requises aux fins de permettre un contrôle effectif du CONSEIL D'ETAT des modalités de traitement des données et à rendre disponible la documentation s'y rapportant.

10. Sort des données et documentation utile

Au terme de l'exécution du marché public, le titulaire du marché doit restituer au CONSEIL D'ETAT toutes les données, collectées et produites dans le cadre de la fourniture des prestations, conformément à ses instructions. Cette restitution doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du titulaire du marché et ce, dans un délai de 2 mois après le terme du marché public.

La suppression sera consignée dans un procès-verbal avec indication de la date. Une copie de ce procès-verbal sera transmise au CONSEIL D'ETAT.

La documentation constituée aux fins de prouver la conformité du traitement des données avec les instructions du CONSEIL D'ETAT et les obligations résultant des présentes, doit :

- Soit être conservée au-delà du terme de la présente annexe, en respectant les durées de prescription légales ;
- Soit être remise au CONSEIL D'ETAT à la fin du marché public.

11. Délégué à la protection des données et registre des activités de traitement

Dans la mesure où le titulaire du marché aurait désigné un délégué à la protection des données, il s'engage à en communiquer le nom et les coordonnées au CONSEIL D'ETAT.

Par ailleurs, le titulaire du marché déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du CONSEIL D'ETAT, comprenant l'ensemble des informations requises en application de l'article 30 (2) du Règlement (UE) 2016/679.