MEAE_26042_CEAPD

ANNEXE AU CCAP
TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Dans le cadre du présent marché, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, notamment le RGPD et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Précisions terminologiques

Le responsable de traitement au sens du 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 (ci-après «règlement général sur la protection des données » ou RGPD) est la personne publique et le sous-traitant est le titulaire du présent marché.

Nature, durée, finalité et description du traitement de données à caractères personnel

Le titulaire est autorisé à traiter pour le compte de la personne publique, les données à caractère personnel nécessaires pour exécuter la prestation.

Les données à caractère personnel sont traitées pour toute la durée du marché. En cas de résiliation ou de prolongation, la durée de traitement est réduite ou prolongée d'autant.

La finalité du traitement recouvre :

- la collecte de données et leur consultation dans le cadre du suivi de la relation client.

La nature du traitement est :

- L'hébergement ;
- La collecte ;
- La modification des données à caractère personnel ;
- La structuration des données à caractère personnel.

Les types de données à caractère personnel traitées pourront être notamment :

- le nom ;
- le prénom ;
- la fonction ;
- les coordonnées professionnelles ;

Les catégories de personnes concernées sont :

- les agents du ministère de l'Europe et des Affaires étrangères ;

Mise en œuvre du traitement

Le titulaire du marché s'engage, notamment, à :

- traiter les données à caractère personnel que sur instruction du responsable de traitement (y compris les transferts de données personnelles hors UE vers un pays tiers ou organisation internationale) ;
- traiter les données uniquement pour la ou les seule(s) finalité(s) qui en font l'objet ;
- dans le cas où une instruction est donnée en violation du règlement général 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, à en informer immédiatement la personne publique ;
- dans le cas où il est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, à informer la personne publique de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;
- les données transférées vers un pays tiers doivent bénéficier d'un degré de protection équivalent à celui garanti par le RGPD au sein de l'Union européenne. Tout transfert de données à caractère personnel, au bénéfice de toute entité et notamment de pays tiers ou d'organisations internationales, qui ne serait pas strictement conforme à la réglementation française ou européenne est formellement prohibé. A défaut de pouvoir garantir le respect de ces exigences en cas de transfert de données à caractère personnel vers un pays tiers, le titulaire suspend tout transfert et se rapproche de la personne publique pour envisager, le cas échéant, l'adaptation des modalités d'exécution permettant le respect des exigences du RGPD.
  Si les modalités d'exécution ne peuvent être adaptées, la personne publique procède à la résiliation du marché pour motif d'intérêt général dans les conditions prévues par le CCAG de référence.
- garantir la confidentialité des données à caractère personnel traitées ;
- veiller à ce que les personnes autorisées à traiter les données à caractère personnel :
  - 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.

Sous-traitance des activités de traitement

Lorsque le titulaire (sous-traitant au sens RGPD), fait appel à un sous-traitant (au sens de la commande publique) pour mener des activités de traitement spécifiques, il informe préalablement et par écrit la personne publique (le responsable de traitement au sens du RGPD).

Cette information doit indiquer clairement la nature des 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 la personne publique

n'a pas émis d'objection pendant le délai de 21 jours à compter de la date de réception de la demande en application des dispositions de l'article R.2193-4 du Code de la commande publique.

Afin d'obtenir l'acceptation et l'agrément de la personne publique, le titulaire doit présenter son sous-traitant par le biais de l'acte spécial de sous-traitance, dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent (téléchargeable sur https://www.economie.gouv.fr/daj/formulaires-declaration-du-candidat).

Le sous-traitant est tenu de respecter les obligations du présent marché pour le compte et selon les instructions de la personne publique. 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 de la législation et de la règlementation en vigueur sur la protection des données.

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

Exercices des droits par les personnes concernées par le traitement sur leurs données personnelles

Il appartient au responsable du traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données. Le titulaire apporte l'aide nécessaire pour ce faire (collecte, rédaction…), il ne peut s'opposer à une demande d'accompagnement de la personne publique.

La formulation et le format de l'information doivent être convenus avec la personne publique avant la collecte de données.

La personne publique en qualité de responsable du traitement répond, avec l'aide du titulaire, dans les délais prévus par le règlement général sur la protection des données, aux demandes des personnes concernées en cas d'exercice de leurs droits.

Notification des violations de données à caractère personnel

Le titulaire notifie à la personne publique toute violation de données à caractère personnel dans un délai de 24 heures après en avoir pris connaissance et par courriel. Cette notification est accompagnée de toute documentation utile afin de permettre à la personne publique, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance.

La personne publique notifie à l'autorité de contrôle compétente, les violations de données à caractère personnel dans un délai maximum de 72 heures à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Avant transmission par le responsable de traitement, le titulaire rédige le courrier de notification qui contient au moins :

- 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 par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que la personne publique 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.

Avec l'aide du titulaire, notamment via la rédaction du courrier, la personne publique communique 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 :
- 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 par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que la personne publique 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.

Aide du titulaire dans le cadre du respect par la personne publique de ses obligations

Le titulaire aide la personne publique :
- à la réalisation d'analyses d'impact relative à la protection des données ;
- à la réalisation de la consultation préalable de l'autorité de contrôle.

Le titulaire met à la disposition de la personne publique la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre, le cas échéant, la réalisation d'audits, y compris des inspections, par la personne publique ou un auditeur mandaté par lui, et contribuer à ces audits.

Mesures de sécurité

Le titulaire met en œuvre les mesures de sécurité suivantes :
- 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.

Le titulaire doit pouvoir garantir, pendant toute la durée des prestations, que l'intégralité des données à caractère personnel qu'il traite dans le cadre de l'exécution du marché/de l'accord-cadre en qualité de sous-traitant RGPD sont traitées et plus généralement rendues accessibles exclusivement au sein :

- de l'Espace économique européen ;
- d'un État tiers bénéficiant d'une décision d'adéquation au sens de l'article 45 du RGPD ;
- ou, à défaut, que les transferts résultant de la réalisation des prestations sont encadrés par des garanties appropriées ou des règles d'entreprise contraignantes au sens des articles 46 et 47 du RGPD, le cas échéant complétées par des mesures supplémentaires visant à garantir qu'il ne pourra pas y être fait échec dans l'État tiers de destination, dans le strict respect de la jurisprudence.

La garantie du titulaire sur ce point doit non seulement couvrir l'hébergement des données, mais également toutes les opérations de traitement réalisées par le titulaire ou par les sous-traitants RGPD ultérieurs auxquels pourraient le cas échéant être confiées certaines opérations de traitement (notamment maintenance et assistance).
Le titulaire doit ainsi pouvoir garantir que les données traitées ne peuvent pas être rendues accessibles à des destinataires, y compris des autorités administratives ou judiciaires, situés hors de l'Espace économique européen sans que soit respecté le droit applicable, et en particulier le RGPD. Le titulaire détaille les moyens mis en place pour y répondre.

La présente clause est complétée par les clauses de sécurité et de confidentialité prévues dans le cahier des clauses administratives particulières (CCAP) et dans le cahier des clauses techniques particulières (CCTP) rattachés au marché.

Sort des données

Au terme de l'exécution du présent marché, la personne publique informe le titulaire de sa décision relative au sort des données. La personne publique peut demander au titulaire de :

- détruire toutes les données à caractère personnel ;
- renvoyer toutes les données à caractère personnel à la personne publique ou au tiers désigné par elle.

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

Délégué à la protection des données

Dès la notification du marché, la personne publique communique au titulaire le nom et les coordonnées de son délégué à la protection des données.

Registre des activités de traitement

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte de la personne publique comprenant :

1. le nom et les coordonnées de la personne publique pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
2. les catégories de traitements effectués pour le compte de la personne publique ;
3. 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 général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, 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.