

CCAP - ANNEXE 2 - PROTECTION DES DONNEES A CARACTERE PERSONNEL

Chaque partie au marché est tenue au respect des règles relatives à la protection des données à caractère personnel auxquelles elle a accès pour les besoins de l'exécution des prestations.

Le titulaire s'engage à :

1. Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet du marché
2. Traiter les données conformément aux instructions documentées du responsable de traitement. 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 de la loi informatique et libertés ou de toute autre disposition du droit national, il en informe immédiatement le responsable de traitement. 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 le responsable du traitement 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 :
 - a. S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
 - b. 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

Sous-traitance de rang ultérieur

Le titulaire peut faire appel à un sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques.

Pour tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants, le titulaire informera préalablement et par écrit le responsable de traitement, en indiquant clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance.

Le responsable de traitement dispose d'un délai minimum de 45 jours à compter de la date de réception de cette information pour présenter ses objections. 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 des présentes clauses pour le compte et selon les instructions du responsable de traitement.

En conséquence il appartient au titulaire 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 et de la loi informatique et libertés.

Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte (directe ou indirecte, ou en cas de modification substantielle) des données.

Exercice des droits des personnes

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

Notification des violations de données à caractère personnel

Le titulaire notifie aux établissements concernés toute violation de données à caractère personnel dans un délai maximum de 36 heures après en avoir pris connaissance et par courrier électronique.

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.

Après accord du responsable de traitement, le titulaire notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Si le délai de 72 heures est dépassé, le titulaire devra expliquer les motifs du retard à l'autorité de contrôle compétente (la CNIL).

La notification contient au moins :

- (a) 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
- (b) 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
- (c) La description des conséquences probables de la violation de données à caractère personnel
- (d) 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

S'il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Aide du titulaire dans le cadre du respect par le responsable de traitement de ses obligations

Le titulaire assiste le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données concernant notamment les traitements de données « sensibles » ou présentant un risque particulier pour les droits des personnes concernées.

Le titulaire est également tenu de soutenir le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

Mesures de sécurité

Le titulaire s'engage à mettre en œuvre les mesures de sécurité conformes aux principes de base suivants :

- (a) Le chiffrement des données à caractère personnel selon la criticité des données, convenue avec le responsable de traitement
- (b) Les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement
- (c) 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
- (d) Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement

Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le titulaire s'engage à :

- Renvoyer toutes les données à caractère personnel au responsable de traitement
- Détruire toutes les copies existantes des données dans le système d'information du titulaire et des sous-traitants ultérieurs et justifier par écrit de cette destruction auprès du responsable de traitement dans un délai de 1 mois à compter de la fin du contrat support

Délégué à la protection des données

Le titulaire communiquera 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.

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 du responsable de traitement comprenant :

- (a) 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 ;
- (b) Les catégories de traitements effectués pour le compte du responsable du traitement ;
- (c) 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 ;
- (d) Une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - (i) La pseudonymisation et le chiffrement des données à caractère personnel ;
 - (ii) Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - (iii) 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 ;
 - (iv) Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Documentation et audit

Le titulaire s'engage à fournir au responsable de traitement toutes les informations nécessaires, afin de prouver sa conformité aux obligations prévues à l'article 28 du RGPD, et d'autoriser et faciliter les audits, y compris les inspections, aux frais du Responsable de Traitement. Toutefois, en cas de manquement à ses obligations prévues aux §1 à 6 + 4.1 du présent document, ces coûts incomberont au titulaire. L'audit sera mené par le Responsable du Traitement ou tout autre auditeurs tiers, choisi par le Responsable de Traitement, et expressément accepté par le titulaire.

Cet audit peut être réalisé une fois par année civile, sauf dans le cas avéré d'accès aux données personnelles non autorisé, ou raisonnablement suspecté.

Le Responsable de traitement s'engage à notifier par écrit avec un préavis minimum de 15 jour(s) au titulaire tout audit, en lui communiquant notamment l'objet de la mission, sa durée envisagée, et le nom du ou des expert(s) détaché(s).

Le titulaire mettra en place les moyens raisonnables pour permettre à l'auditeur de mener à bien son audit. Les opérations d'audit et les demandes d'information devront être effectuées pendant les heures normales d'ouverture du titulaire et ne devront pas perturber le bon fonctionnement des activités de ce dernier.

Au titre de cette assistance fournie au Responsable de traitement par le titulaire, ce dernier interviendra sans frais supplémentaire pour le Responsable de traitement dans la limite d'un jour/homme par an dans le cas d'un audit portant sur le registre des traitements. Toutefois, concernant un audit du système d'hébergement, le périmètre et la durée seront définis d'un commun accord (au cas par cas). Toute mobilisation complémentaire de ressource du titulaire pour cette assistance sera facturée au Responsable de traitement, sous réserve que l'audit ne conclue à aucun manquement du titulaire à ses obligations.

Un exemplaire du rapport d'audit sera remis gracieusement au titulaire. Les parties examineront de bonne foi le rapport d'audit dans le cadre du comité de pilotage, et identifieront, le cas échéant, les actions à engager par l'une ou l'autre des parties pour mettre en œuvre les décisions prises lors de ce comité.