

ANNEXE - TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire du marché s'engage à effectuer pour le compte de la personne publique (responsable du traitement) les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « le règlement européen sur la protection des données ») ainsi que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2018-493 du 19 juin 2018 relative à la protection des données personnelles et ses décrets d'application.

Description du traitement de données à caractère personnel

Le titulaire est autorisé à traiter pour le compte de la personne publique et pour la durée du présent marché public les données à caractère personnel nécessaires pour exécuter les prestations objet du présent marché.

Les données à caractère personnel sont traitées pour une durée de quatre fois un an.

La finalité du traitement est la traçabilité des données tout au long du processus, de la notification du marché ou de l'initiation du bon de commande jusqu'à la réalisation des prestations.

Les types de données à caractère personnel traitées sont les noms, prénoms et adresses.

La personne publique met à la disposition du titulaire : les informations nécessaires à la réalisation des prestations.

Obligations du titulaire vis-à-vis de la personne publique

Le titulaire s'engage à :

- Traiter les données uniquement pour la seule finalité qui fait l'objet du présent marché.
- Garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché.
- 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.
- 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.

Information des personnes concernées

Il appartient au titulaire d'informer les 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 la personne publique avant la collecte de données.

Le titulaire doit répondre, au nom et pour le compte de la personne publique et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits notamment le droit d'accès, de rectification, d'effacement et d'opposition, le droit à la limitation du traitement, le droit à la portabilité des données, 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 à la personne publique toute violation de données à caractère personnel dans les meilleurs délais et si possible dans les 48 heures après en avoir pris connaissance et selon des moyens déterminés conjointement avec la personne publique.

Après accord écrit de la personne publique, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte de la personne publique, les violations de données à caractère personnel dans les meilleurs délais et si possible dans les 72 heures 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.

La notification 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.

Après accord de la personne publique, le titulaire communique, au nom et pour le compte de l'acheteur, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

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 l'acheteur 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 aide la personne publique :

- pour la réalisation d'analyses d'impact relative à la protection des données
- pour la réalisation de la consultation préalable de l'autorité de contrôle.

Mesures de sécurité :

Le titulaire met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, et 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 ;
- Un outil garantissant la confidentialité dans la transmission des documents sensibles.

Sort des données

Au terme de l'exécution du présent marché, le titulaire doit détruire toutes les données à caractère personnel et sauf disposition contraire résultant du droit communautaire ou du droit d'un État de l'UE. Les Parties conviennent d'ores et déjà que le titulaire conservera les données personnelles pour une durée minimale de 5 ans à compter de la fin du marché et ce conformément aux exigences légales en vigueur relatives aux contrôles fiscaux et sociaux.

Délégué à la protection des données

Le titulaire communique à la personne publique 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 tient par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte de la personne publique responsable de traitement comprenant :

- Les catégories de traitements effectués pour le compte de la personne publique;
- 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 §1, 2^e alinéa du règlement, 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.

Documentation

Le titulaire met à la disposition de l'acheteur 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 l'acheteur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.