

|  |
| --- |
| **Annexe n° 2 au Cahier des Clauses Particulières**  **ANNEXE SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL**  **(Conformément à l’article 28 du RGPD)** |

La présente annexe a pour objet de définir les conditions dans lesquelles le titulaire du marché public s’engage à effectuer pour le compte de l’acheteur les opérations de traitement de données à caractère personnel définies ci-après.

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

Description du traitement de données à caractères personnel :

Le titulaire est autorisé à traiter pour le compte de l’acheteur, pour la durée du présent marché public, les données à caractère personnel nécessaires pour fournir la ou les prestation(s) suivante(s) : prestations de fournitures de matériels d’affranchissement, de traitement du courrier, accessoires et prestations associées.

La nature des opérations réalisées sur les données est : la collecte, l’utilisation, le stockage, l’archivage et la destruction des données selon un processus formalisé et sécurisé.

La ou les finalité(s) du traitement sont : réaliser les opérations strictement nécessaires à l’exécution du présent marché public.

Les données à caractère personnel traitées sont les données de l’acheteur, des représentants des services bénéficiaires et des utilisateurs du marché, nécessaires à l’exécution des commandes, au pilotage et au suivi des prestations et des consommations.

Les catégories de personnes concernées sont toutes les personnes désignées par l’acheteur, les services bénéficiaires et les utilisateurs.

Pour l’exécution des prestations objets du présent marché public, l’acheteur met à la disposition du titulaire les informations strictement nécessaires pour l’exécution des prestations. Le titulaire communique la liste des informations requises aux services bénéficiaires et aux utilisateurs.

Obligations du titulaire vis-à-vis de l’acheteur (article 28.3 du RGPD) :

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

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet du présent marché public ;

2. traiter les données conformément aux instructions documentées de l’acheteur figurant dans les documents contractuels du présent marché public. Si le titulaire considère qu’une instruction constitue une violation du règlement général sur la protection des données ou de toute autre disposition du droit de l’Union ou du droit des États membres relative à la protection des données, il en informe immédiatement l’acheteur ;

3. Si le titulaire 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’État membre auquel il est soumis, il doit informer l’acheteur de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;

4. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché public ;

5. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché public :

- 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

6. 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 (articles 28.2 et 28.4 du RGPD) :

Lorsque le titulaire fait appel à un sous-traitant pour mener des activités de traitement spécifiques, il informe préalablement et par écrit l’acheteur 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 marché public.

Afin d'obtenir l'acceptation et l'agrément de l'acheteur, 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 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 public pour le compte et selon les instructions de l’acheteur. Il appartient au titulaire de s’assurer que le sous-traitant présente les mêmes garanties suffisantes quant à la mise en oeuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement général sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le titulaire demeure pleinement responsable devant l’acheteur de l’exécution par le sous-traitant de ses obligations.

Droit d’information et exercice des personnes concernées par le traitement (articles 13 à 15 du RGPD) :

Il appartient au titulaire de fournir l’information aux 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 l’acheteur avant la collecte de données.

Le titulaire doit répondre, au nom et pour le compte de l’acheteur et 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 (article 33 du RGPD) :

Le titulaire notifie à l’acheteur toute violation de données à caractère personnel dans un délai de trois heures après en avoir pris connaissance et par téléphone doublé d’un message électronique. Cette notification est accompagnée de toute documentation utile afin de permettre à l’acheteur, 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.

Après accord écrit de l’acheteur, le titulaire notifie à l’autorité de contrôle compétente, au nom et pour le compte de l’acheteur, les violations de données à caractère personnel dans un délai maximum de 24 heures 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 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.

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 écrit de l’acheteur, 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, 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 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.

Aide du titulaire dans le cadre du respect par l’acheteur de ses obligations :

Le titulaire aide l’acheteur :

 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.

Mesures de sécurité :

Le titulaire met en oeuvre toutes les mesures techniques et organisationnelles garantissant un niveau de sécurité adapté au risque, y compris :

 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 communique à l’acheteur qui les valide expressément, la liste des mesures techniques et organisationnelles qu’il prend.

Sort des données (article 28.3.g du RGPD) :

Au terme de l’exécution du présent marché public, le titulaire doit renvoyer toutes les données à caractère personnel à l’acheteur ou au tiers désigné par l’acheteur.

Le renvoi doit s’accompagner de la destruction de toutes les copies existantes dans les systèmes d’information du titulaire et de ses sous-traitants. Une fois détruites, le titulaire et ses sous-traitants doivent justifier par écrit de la destruction.

Délégué à la protection des données (articles 37 à 39 du RGPD) :

Le titulaire communique à l’acheteur dès la notification du marché public 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, ou, à défaut, l’identité et les coordonnées d’un point de contact dédié à ces questions.

Registre des activités de traitement (article 30 du RGPD) :

Le titulaire tient par écrit un registre de toutes les activités de traitement effectuées pour le compte de l’acheteur comprenant :

 le nom et les coordonnées de l’acheteur 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 de l’acheteur ;

 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 ;

 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.

Documentation (article 28.3.h du RGPD) :

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 auditeur mandaté par lui, et contribuer à ces audits.

Obligations de l’acheteur vis-à-vis du titulaire :

L’acheteur s’engage à :

 Fournir au titulaire les données visées dans la clause relative à la « Description du traitement de données à caractères personnel » ;

 Documenter par écrit toute instruction concernant le traitement des données par le titulaire ;

 Veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD et par la loi Informatique et Libertés de la part du titulaire ;

 Superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.