

ANNEXE n°1 au Cahier des Clauses Administratives Particulières Le RGPD – Traitement des données à caractère personnel et à la libre circulation de ces données
--

▪ **A 1.1 Précisions terminologiques**

Pour l'application du présent article, 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 l'ensemble des bénéficiaires du marché et le sous-traitant est le titulaire du marché public.

Le présent article a pour objet de définir les conditions dans lesquelles le titulaire du marché public s'engage à effectuer pour le compte des bénéficiaires du marché 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 RGPD et la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ainsi que les dispositions du code de la santé publique (articles L. 1110-4 et suivants dudit code).

▪ **A 1.2 Description du traitement de données à caractère personnel**

Le titulaire est autorisé à traiter pour le compte des bénéficiaires du marché, pour la durée du présent marché public, les données à caractère personnel nécessaires pour fournir les prestations suivantes) :

- Acquisition d'échographes à ultrasons ultra-portables ;
- Prestations de formation ;
- Prestations de maintenance ;
- Prestations de fabrication additive.

Pour permettre les prestations objet du présent marché, la nature des opérations réalisées sur les données est :

- Stockage des coordonnées des établissements bénéficiaires ;

Les finalités du traitement sont :

- Réalisation d'attestations de formation ;
- Rédaction de compte-rendu de maintenance ;
- Livraison des fournitures et prestations commandées ;
- Suivi contractuel du marché ;

Les catégories de personnes concernées sont :

- Les personnes qui suivent le marché ;
- Les techniciens du SSA formés à la maintenance
- Les intervenants de la société pour la bonne conduite du marché.

Pour l'exécution des prestations objets du présent marché public, les bénéficiaires du marché mettent à la disposition du titulaire les informations/types de données à caractère personnelles traitées nécessaires suivantes :

- Les données à caractère personnel concernant les agents avec la liste des noms, prénoms, fonctions, e-mails et n° de téléphone des agents du SSA

▪ **A 1.3 Obligations du titulaire vis-à-vis de l'établissement** (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 des bénéficiaires du marché figurant dans l'annexe technique du présent marché public.
Si le titulaire considère qu'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 États membres relative à la protection des données, il en informe immédiatement les bénéficiaires du marché ;
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 en informer les bénéficiaires du marché de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information.
Il devra notamment respecter les dispositions du chapitre V du règlement RGPD et la décision d'exécution (UE) 2021/914 de la Commission européenne du 4 juin 2021 relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers ;
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.

▪ **A 1.4 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 les bénéficiaires du marché 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 des bénéficiaires du marché, 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 <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>).

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte de l'acheteur.

Il appartient au titulaire du marché 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.

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

▪ **A 1.5 Droit d'information et exercice des personnes concernées par le traitement** (articles 13 à 15 du RGPD)

Il appartient au Service de santé des armées de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

À ce titre, le titulaire devra répondre à toute requête de l'administration concernant les données personnelles stockées ou traitées dans les systèmes dont il a l'exploitation ou l'administration.

La formulation, le format et le délai de réponse, de et à ces requêtes doivent être convenus avec les bénéficiaires avant la collecte des données personnelles concernées.

Le titulaire doit répondre, au nom et pour le compte des bénéficiaires 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.

Le titulaire doit aider les bénéficiaires à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

La formulation et le format de l'information doivent être convenus avec les bénéficiaires avant la collecte des données.

▪ **A 1.6 Notification des violations de données à caractère personnel** (article 33 du RGPD)

Le titulaire notifie aux bénéficiaires toute violation de données à caractère personnel dans un délai de 72 heures après en avoir pris connaissance et par courriel.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'établissement, 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 des bénéficiaires, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte des bénéficiaires, 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.

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'établissement 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'établissement, le titulaire communique, au nom et pour le compte de l'établissement, 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'établissement 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.

▪ **A 1.7 Aide du titulaire dans le cadre du respect par l'établissement de ses obligations**

Le titulaire aide l'établissement :

- 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.

▪ **A 1.8 Mesures de sécurité des données**

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 met en œuvre les mesures de sécurité prévues par :

- Politique de sécurité des systèmes d'information de l'État ;
- Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) ;
- Politique générale des systèmes d'information des armées (PSSI-A) ;
- Politique de sécurité des systèmes d'information du SSA (PSSI-SSA).

▪ **A 1.9 Sort des données** (article 28.3.g du RGPD)

Au terme de l'exécution du présent marché public, le titulaire doit détruire toutes les données à caractère personnel, la durée de conservation des données doit être limitée au strict minimum.

Dans le cadre d'une éventuelle sous-traitance, celui-ci s'engage à renvoyer toutes les données à caractère personnel au titulaire.

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.

Pour rappel, les données doivent être conservées par le titulaire pour une durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées.

▪ **A 1.10 Délégué à la protection des données** (articles 37 à 39 du RGPD)

Le titulaire communique à l'établissement 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.

Le directeur des affaires juridiques du ministère des armées exerce les fonctions de délégué à la protection des données.

Au sein du service de santé des armées, le pharmacien en chef André MARCEL assure les fonctions de correspondant auprès du Délégué à la protection des données (DPD).

▪ **A 1.11 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'établissement comprenant :

1. Le nom et les coordonnées de l'établissement 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 l'établissement ;
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 et listée ci-dessus.
5. Les mesures de sécurité techniques et organisationnelles citées au A.1.8.

▪ **A 1.12 Documentation** (article 28.3.h du RGPD)

Le titulaire met à la disposition de l'établissement 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'établissement ou un auditeur mandaté par lui, et contribuer à ces audits.

▪ **A 1.13 Obligations de l'établissement vis-à-vis du titulaire**

Les bénéficiaires s'engagent à :

- Fournir au titulaire les données visées dans la clause relative à la « description du traitement de données à caractère 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.