**12.8 Protection des données à caractère personnel**

La réglementation applicable au traitement de données à caractère personnel désigne le Règlement (UE) n° 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données personnelles et à la libre circulation de ces données (dénommé ci-après "RGPD"), et toute réglementation relative aux traitements de données personnelles applicable pendant la durée du marché, notamment la loi n° 78-17 du 6 janvier 1978 modifiée relative à l’informatique, aux fichiers et aux libertés, désignés ci-après « réglementation applicable ».

L’ensemble des termes suivants sont définis à l’article 4 du RGPD :

Constitue un « responsable du traitement » : « la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement. » ;

Constitue un « sous-traitant » : « la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. ».

Au sens du RGPD (article 28), lorsque le « sous-traitant » recrute un autre sous-traitant, ce dernier est un prestataire de second rang comme le sous-traitant au sens de la loi n° 75-1334 du 31 décembre 1975 modifiée relative à la sous-traitance.

Est « sous-traitant du sous-traitant » celui qui est recruté par le « sous-traitant » pour mener des activités de traitement de données à caractère personnel spécifiques pour le compte du « responsable du traitement ».

**A Traitement des données à caractère personnel lorsque chaque partie est qualifiée de « responsable de traitement »**

Au sens de la disposition ci-dessous, le traitement des données à caractère personnel ne fait pas partie de l’objet même du marché.

À des fins de gestion administrative du marché, chaque partie est amenée à traiter les données à caractère personnel de l’autre partie. Pour le traitement desdites données qu’elle effectue, chaque partie est qualifiée de « responsable de traitement » au sens de la réglementation applicable et s’engage à respecter cette dernière.

À cet égard, pour se conformer à l'article 14 du RGPD, chaque partie s’engage à fournir à l’autre partie la mention d’information pour que cette dernière la communique aux personnes concernées.

**B Option : Traitement des données à caractère personnel lorsque la personne publique est « responsable de traitement » et le titulaire est « sous-traitant »**

Les dispositions de l’annexe n°01 sont applicables lorsque la réalisation de l’objet du marché implique le traitement de données à caractère personnel.

**Annexe Traitement des données à caractère personnel lorsque la personne publique est "responsable de traitement" et le titulaire est "sous-traitant"**

**1. Objet**

Aux fins de la présente annexe, la personne publique est le « responsable de traitement » et le titulaire du marché est le « sous-traitant » au sens de la réglementation applicable.

Les présentes dispositions ont pour objet de définir les conditions dans lesquelles le titulaire s’engage à effectuer, pour le compte de la personne publique, les traitements de données à caractère personnel prévus au titre du marché et dans les conditions définies ci-après.

**2. Description des traitements de données à caractère personnel à réaliser pour l’exécution du marché**

Le titulaire est autorisé à traiter, pour le compte de la personne publique des données à caractère personnel pour fournir le ou les service(s) suivant(s) : *[indiquer l’objet du marché].*

a) La nature des opérations réalisées sur les données à caractère personnel est [XXXX]

b) La ou les finalité(s) du traitement sont [XXX]

c) Les catégories de données à caractère personnel traitées sont [XXX]

d) Les catégories de personnes concernées sont [XXX]

Pour l’exécution des prestations objets des présentes, la personne publique met à la disposition du titulaire les informations nécessaires suivantes : [XXX]

**3. Durée de l’engagement des parties**

Les présentes dispositions entrent en vigueur à compter de la notification du marché par la personne publique au titulaire pour toute la durée d’exécution du marché.

**4. Obligations de la personne publique**

En sa qualité de « responsable de traitement », la personne publique s’engage à respecter la réglementation applicable. Ainsi, le « responsable de traitement », s’engage notamment à ce que les données à caractère personnel soient :

traitées de manière licite (conformément aux exigences règlementaires en la matière), loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'étant pas considéré, comme incompatible avec les finalités initiales (limitation des finalités) ;

adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

exactes et si nécessaire, tenues à jour ;

conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ;

traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

La personne publique s’engage à ne traiter aucune donnée à caractère personnel afférente à une des catégories particulières de données à caractère personnel de l’article 9 du RGPD sauf exceptions prévues par les lois et règlementations en vigueur durant l’exécution du marché.

Le « responsable du traitement » est pleinement responsable du respect des obligations précitées et est en mesure de démontrer que celles-ci sont respectées.

**5. Obligations du titulaire vis-à-vis de la personne publique**

Le titulaire s'engage à :

a) Traiter les données à caractère personnel uniquement pour la ou les seule(s) finalité(s) qui fait/font l’objet du présent marché ;

b) Traiter les données à caractère personnel conformément aux instructions documentées de la personne publique dans le CCTP le cas échéant ;

c) Garantir la confidentialité des données à caractère personnel dans le cadre des présentes dispositions ;

d) Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu des présentes dispositions :

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.

e) Prendre en compte, s’agissant de ses outils, produits, applications ou services, les principes de protection des données à caractère personnel dès la conception et de protection des données par défaut ;

f) Mettre en œuvre les mesures de sécurité des données à caractère personnel nécessaires ;

   Les mesures de sécurité sont listées ci-dessous :

XXX

XXX

g) Ne pas procéder au transfert des données en dehors de l’Espace Économique Européen sans avoir obtenu l’autorisation préalable de la personne publique. Si le titulaire considère qu’une demande constitue une violation de la loi du n°78-17 du 6 janvier 1978 modifiée, il en informe, dans les meilleurs délais, la personne publique. 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’État membre auquel il est soumis, il doit informer dans les meilleurs délais, la personne publique de cette obligation avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

h) Ne pas recruter un « sous-traitant du sous-traitant » sans avoir obtenu l’autorisation préalable de la personne publique. En cas de recrutement d’un « sous-traitant du sous-traitant », afin d'obtenir l'acceptation et l'agrément de la personne publique, le titulaire doit présenter son sous-traitant (tant au sens du RGPD, qu’au sens de la loi n°75-1334 du 31 décembre 1975 relative à la sous-traitance) 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 du sous-traitant » est tenu de respecter les obligations du présent marché pour le compte de la personne publique. Il appartient au titulaire du marché de s’assurer que le « sous-traitant du sous-traitant » présente des 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 à caractère personnel. Si le « sous-traitant du sous-traitant » ne remplit pas ses obligations en matière de protection des données, le titulaire du marché demeure pleinement responsable vis-à-vis de la personne publique de l’exécution par le « sous-traitant du sous-traitant » de ses obligations.

**6. Notification des violations des données à caractère personnel**

Le titulaire notifie à la personne publique toute violation de données à caractère personnel confiées par la personne publique dès qu’il en a connaissance et dans un délai maximum de 72 heures.

Dans la mesure où le titulaire dispose des informations listées à l’article 33 du RGPD, cette notification inclut ces informations afin de permettre à la personne publique, si nécessaire, de notifier cette violation au délégué à la protection des données du ministère des armées.

Dans le cas 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.

Le délégué à la protection des données du CROUS RENNES BRETAGNE notifie les violations à la commission nationale de l’informatique et des liberté (CNIL) et/ou aux personnes concernées dans les cas prévus par la réglementation applicable.

**7. Analyse d’impact**

Le titulaire aide la personne publique pour la réalisation d’éventuelles analyses d’impact relatives à la protection des données à caractère personnel.

Le titulaire aide la personne publique en cas de consultation de la CNIL sur l’analyse d’impact réalisée. Cependant, celle-ci est présentée à la CNIL par le délégué à la protection des données du CROUS RENNES BRETAGNE.

**8. Devenir des données au terme de l’exécution du marché**

Au terme de l’exécution du présent marché, le titulaire s’engage à détruire toutes les données à caractère personnel sauf exigences légales contraires.

**9. Droit d’information des personnes concernées et exercice de leurs droits**

9.1 Droit d’information

Il appartient à la personne publique de fournir l’information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

9.2 Exercice des droits des personnes concernées

Le titulaire s’engage à adresser à la personne publique toute demande d’exercice de ses droits par une personne concernée, reçue directement par le titulaire, afin que la personne publique puisse s’acquitter de ses obligations en tant que « responsable de traitement ».

Les demandes d’exercice des droits des personnes concernées sont à adresser par le titulaire à la personne publique, par courrier électronique dans les meilleurs délais à l’adresse suivante : dpo@crous-rennes.fr.

**10. Documentation et audits**

Le titulaire met à la disposition de la personne publique la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d’audits y compris des inspections par la personne publique ou un autre auditeur qu’il a mandaté et contribuer à ces audits.

Pendant l’exécution du marché, la personne publique peut réaliser elle-même ou faire réaliser par un tiers non concurrent du titulaire, et préalablement validé par ce dernier, un audit (dans une limite maximale d’une fois par an).

La personne publique aura accès aux seules zones et moyens informatiques concernés par le traitement objet du marché, dans le respect des consignes de sécurité prévues pour chaque site.

La personne publique doit notifier par écrit au titulaire la date de réalisation de l’audit avec un préavis d’au moins vingt jours ouvrés.

La personne publique s’engage à ne pas perturber l’activité normale du titulaire et à réaliser l’audit sous deux jours ouvrés.

Le rapport d’audit sera transmis au titulaire.

**11. Registre des activités de traitement**

Le titulaire déclare tenir par écrit un registre de toutes les catégories d’activités de traitement effectuées pour le compte de la personne publique comprenant :

Le nom et les coordonnées de la personne publique pour le compte duquel il agit et le cas échéant, du délégué à la protection des données ;

Les catégories de traitements effectués pour le compte de la personne publique ;

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.

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 RGPD, les documents attestant de l'existence de garanties appropriées.

**12. Délégué à la protection des données à caractère personnel**

Nom et coordonnées du délégué à la protection des données à caractère personnel du « sous-traitant » (ou, à défaut, l’identité et les coordonnées d’un point de contact dédié à ces questions) : [XXX]

Nom et coordonnées du point de contact du « responsable de traitement » dédié à ces questions :

[**dpo@crous-rennes.fr**](mailto:dpo@crous-rennes.fr)

Fait à Le

Pour le Titulaire,

Le Directeur Général,