

ANNEXE RGPD

Définitions

La notion de « sous-traitant » utilisée dans le présent document s'entend au regard de la loi Informatique et Liberté.

Pour rappel, le responsable de traitement est celui « qui détermine les finalités et les moyens d'un traitement » (article 4 du règlement européen n°2016/679 sur la protection des données).

Le sous-traitant est l'entité qui traite des données personnelles pour le compte, sur instruction et sous l'autorité d'un responsable de traitement.

Traitement de type 1

La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée sur le site de la Personne Publique et les données traitées et les traitements effectués sur ces données sont réalisés in situ par la Personne Publique, qui est Responsable de Traitement.

Exemple : un logiciel ou un matériel hébergé dans les datacenters de la Personne Publique, une prestation de service réalisée dans les locaux de la Personne Publique, etc.

Traitement de type 2

La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée dans les locaux du Titulaire du marché avec une assistance technique ou organisationnelle du Titulaire, mais les données traitées et les traitements effectués sur ces données sont réalisés par la Personne Publique qui est Responsable de Traitement. La plupart du temps, le Titulaire n'est pas en contact direct avec les personnes dont les données sont traitées.

Exemple : un logiciel en mode SaaS, une prestation d'analyse de biologie, etc.

Traitement de type 3

La prestation objet du marché (matériel, logiciel, prestation de services, etc.) est livrée dans les locaux de la Personne Publique ou ceux du Titulaire du marché, mais les données traitées et les traitements effectués sont réalisés par le Titulaire du marché, qui est Responsable du Traitement.

Exemple : une prestation de services de conciergerie livrée « clés en main » par le Titulaire.

Les précisions attendues par candidat sont :

- En partie II, pour les traitements de type 3, le descriptif exhaustif du traitement ;
- En partie IV/6 : pour les traitements de type 1 et 2, descriptif des mesures de sécurité

Ces précisions sont attendues à la remise des offres.

Remarque : un contrat de maintenance in-situ est de type 1, dans ce cas les dispositions des type 2 et 3 ne s'appliquent pas.

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de 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 applicable à compter du 25 mai 2018 (ci-après, « *le règlement européen sur la protection des données* »).

En particulier, les parties reconnaissent que la réglementation ci-dessus—ainsi que les lois françaises ou européennes priment sur toute autre réglementation extraterritoriale.

II. Description du traitement faisant l'objet de la sous-traitance

Traitement de type 1

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

- Intervention de maintenance sur site ou à distance ;
- Opérations techniques nécessaires au maintien en condition opérationnelle, notamment supervision, remontée d'alertes techniques, etc.

Traitement de type 2

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) :

- Exécution des prestations de services telles que définies dans le cadre du marché afférent ;
- Intervention de maintenance sur site ou à distance ;
- Opérations techniques nécessaires au maintien en condition opérationnelle, notamment supervision, remontée d'alertes techniques, etc. ;
- Sauvegardes de données, restaurations, etc. ;

Traitement de type 3

Le Titulaire doit décrire précisément :

- Les données traitées ;
- La nature des opérations réalisées sur ces données ;
- La ou les finalité(s) du traitement ;

III. Durée du contrat

Le présent document entre en vigueur dès la signature et jusqu'à la fin du ou des marchés afférents ci-après les « Contrats Principaux ».

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

- traiter les données **uniquement pour la ou les seule(s) finalité(s)** qui fait/font l'objet de la sous-traitance ;
- traiter les données **conformément aux instructions documentées** du responsable de traitement figurant dans les documents du marché. Si le sous-traitant 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 du

droit des Etats membres relative à la protection des données, il en **informe immédiatement** le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale présentant le niveau de sécurité requis, 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 ; dans le cas où il s'agirait de transférer des données vers un pays tiers ou à une organisation internationale présentant le niveau de sécurité requis au sens du RGPD, le sous-traitant doit obtenir un accord écrit de la part du Responsable de Traitement ;

- garantir la **confidentialité** des données à caractère personnel traitées dans le cadre du présent contrat ;
- veiller à ce que les **personnes autorisées à traiter les données à caractère personnel** en vertu du présent contrat :
 - o s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité
 - o 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**

Le RGPD l'emporte sur toute autre loi ou règlement d'origine extra-territoriale, et notamment le Cloud Act et le Patriot Act.

Le sous-traitant peut ajouter les annexes de son choix au présent document, étant entendu que ces annexes viennent en dernier dans l'ordre de préséance.

1. Sous-traitance

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « **le sous-traitant ultérieur** ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement le responsable de traitement 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 contrat de sous-traitance.

Cette information peut être effectuée, au choix du sous-traitant, par courrier ou par accès à un site Internet avec un compte client dédié. Le responsable de traitement dispose d'un délai de cinq jours ouvrables 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.

Si l'objection est faite pour des motifs légitimes du responsable de traitement, le sous-traitant devra proposer un autre sous-traitant ultérieur.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial 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 sous-traitant initial demeure pleinement responsable devant le responsable de traitement de l'exécution par l'autre sous-traitant de ses obligations.

Si le sous-traitant fait appel à un sous-traitant ultérieur originaire d'un pays tiers (hors UE¹ /EEE²), le sous-traitant s'engage à utiliser des mécanismes de transfert des données conformes aux dispositions des articles 44 et suivant du RGPD. Le sous-traitant s'engage en particulier à ce que des mesures techniques et organisationnelles soient mises en œuvre de telle manière que le traitement respecte les exigences du RGPD, assure la protection des droits des personnes concernées, maintienne un enregistrement des données transférées et documente des mesures de sécurité appropriées.

Lorsque le sous-traitant met en place des mesures de protection appropriées, notamment en utilisant des clauses contractuelles types conformément aux dispositions de la décision UE 2010/87 de la Commission ou des clauses types de protection des données qui figurent à l'article 46 du RGPD (« clauses types de protection »), le responsable de traitement donne mandat au sous-traitant pour convenir de ces clauses au nom et pour le compte du responsable de traitement. De plus, le responsable de traitement autorise expressément le sous-traitant à représenter le sous-traitant ultérieur lorsque qu'il convient de ces dispositions. Cela signifie que le sous-traitant

¹ Union Européenne

² Espace Economique Européen

est autorisé à agir au nom et pour le compte du responsable de traitement et du sous-traitant ultérieur. Le sous-traitant est également habilité à exercer les droits et pouvoirs du responsable de traitement découlant des dispositions standards relatives à la protection des données vis-à-vis du sous-traitant ultérieur.

2. Droit d'information des personnes concernées

Traitements de type 1 et 2

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

Traitements de type 3

Le Titulaire, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information sont de la seule responsabilité du Titulaire.

3. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement 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).

Traitements de type 1 et 2

Le Responsable du traitement est responsable de la prise en charge de l'exercice des droits des personnes. Le sous-traitant transmet toutes les données nécessaires dans un délai de 5 jours pour que le responsable du traitement puisse assurer cette conformité réglementaire.

Traitements de type 3

Le Titulaire doit répondre, 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, s'agissant des données faisant l'objet du présent contrat.

4. Notification des violations de données à caractère personnel

Traitements de type 1 et 2

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance et par les moyens suivants : mail, courrier papier. 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.

Traitements de type 3

Le Titulaire notifie à l'autorité de contrôle compétente (la CNIL) 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.

Dans tous les cas, 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 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.

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.

5. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données, dans la limite de la part du traitement dont il a la charge.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle, dans la limite de la part du traitement dont il a la charge.

6. Mesures de sécurité

Traitements de type 1 et 2

Le sous-traitant décrit les mesures de sécurité mise en place pour assurer la sécurité des traitements.

En particulier, le sous-traitant décrit :

- Des cas d'usages précis ;
- Des exemples de risques pris en compte et leur mode de traitement ;
- Les éventuels usages de procédés d'anonymisation ou de pseudonymisation ;
- Les moyens permettant de garantir la confidentialité, l'intégrité et la disponibilité des données ;
- Les moyens permettant de remettre en service rapidement le(s) traitement(s) après incident ;

En particulier, le sous-traitant fournit son appréciation des risques formalisée telle qu'exigée dans le RGPD.

7. Sort des données

Traitements de type 1

A l'issue du marché et au terme de la prestation de services relatifs au traitement de ces données, pour les seules données traitées par le sous-traitant (journaux des accès, compte-rendu d'intervention sur site ou à distance), le sous-traitant s'engage au choix des parties à :

- Détruire ces données ;
- ou
- Transmettre ces données au responsable de traitement et détruire toute copie en sa possession.

Traitements de type 2

A l'issue du marché et au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage au choix des parties à :

- détruire toutes les données à caractère personnel
- ou
- renvoyer toutes les données à caractère personnel au responsable de traitement
- ou
- renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

La suppression du caractère personnel des données (anonymisation) étant très complexe à réaliser, elle doit obtenir l'accord écrit du responsable de traitement.

Traitements de type 3

Le sort des données est de la seule responsabilité du Titulaire du marché.

8. Délégué à la protection des données

Le sous-traitant communique 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

Le délégué à la protection des données désigné par le sous-traitant est si possible francophone, ou au moins anglophone.

9. Registre des catégories d'activités de traitement

- Le sous-traitant déclare **tenir par écrit un registre** de toutes les catégories d'activités de traitement effectuées pour le compte du responsable de traitement comprenant :
 - 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;
 - les catégories de traitements effectués pour le compte du responsable 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 règlement européen 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, 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.

10. Documentation et audits

Le sous-traitant met à la disposition du responsable de traitement sur demande formelle (mail ou courrier papier) la **documentation nécessaire pour démontrer le respect de toutes ses obligations** et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

Le sous-traitant pourra conduire ces audits périodiques nécessaires destinés à faire valider par une entité tierce le bon respect de ses obligations au regard du RGPD. Les conclusions de cet audit seront communicables sur simple demande au responsable de traitement.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

- fournir au sous-traitant les données visées au paragraphe II des présentes clauses
- documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant
- superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.