

Contrat de sous-traitance en matière de traitements de données à caractère personnel

ENTRE

[...]

Situé [..]

et représentée par [..]

(ci-après, « *le responsable de traitement* »)

d'une part,

ET

[...]

situé à [..]

et représenté par [..]

(ci-après, « *le sous-traitant* »)

d'autre part,

A ETE CONCLU LE CONTRAT SUIVANT

1. Objet du traitement

Suivant le contrat du [...] pour une durée de [...], le sous-traitant est en charge de la prestation suivante : [...].

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 général sur la protection des données »).

2. Description du traitement

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour l'exécution de la prestation citée en objet.

2.1. Catégories de personnes concernées	Les traitements de données à caractère personnel effectués pour les besoins de la prestation susvisée visent les personnes suivantes : [...]
2.2. Catégories de données traitées	Les données traitées pour les besoins de la prestation susvisée sont les suivantes : [...]
2.3. Nature des opérations	La nature des opérations réalisées sur les données est [...].
2.4. Finalité(s)	<p>OPTION 1. La finalité du traitement est [...].</p> <p>OPTION 2. Les finalités du traitement sont [...].</p>

3. Durée des clauses contractuelles

Les présentes clauses contractuelles entrent en vigueur à compter du [...], pour la durée du contrat objet du point 1^{er} ci-dessus.

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

Le sous-traitant s'engage aux obligations suivantes:

4.1. Respecter la limitation des finalités	Le sous-traitant s'engage à traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/ont l'objet de la sous-traitance.
4.2. Garantir la confidentialité des données	<p>Afin de garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat, le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :</p> <ul style="list-style-type: none"> • 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

4.3. Protection des données dès la conception et par défaut Le sous-traitant s'engage à 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.

4.4. Sous-traitance ultérieure 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 et par écrit 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.

Le responsable de traitement dispose d'un délai minimum de quinze jours 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.

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.

4.5. Droit d'information des personnes concernées **CHOISIR L'UNE DES DEUX OPTIONS :**

OPTION A. LES DONNEES SONT COLLECTEES PAR LE RESPONSABLE DU TRAITEMENT ET COMMUNIQUEES AU SOUS TRAITANT

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.

OPTION B. LES DONNEES SONT COLLECTEES PAR LE SOUS TRAITANT ET TRAITEES POUR LE COMPTE DU RESPONSABLE DU TRAITEMENT

Le sous-traitant, 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 doit être convenue avec le responsable de traitement avant la collecte de données.

4.6. 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).

Lorsque les personnes concernées exercent auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à [...] **INDIQUER UN CONTACT AU SEIN DU RESPONSABLE DU TRAITEMENT**

4.7. Notifications des fuites de données à caractère personnel**(1) L'obligation de notification au responsable du traitement**

Le sous-traitant notifie au responsable de traitement toute fuite de données à caractère personnel dans un **déla** maximum de vingt-quatre heures après en avoir pris connaissance, et par courriel à [...]

INDIQUER UN CONTACT AU SEIN DU RESPONSABLE DU TRAITEMENT

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.

(2) La possibilité de notification directe auprès de l'autorité de contrôle

Après accord préalable du responsable de traitement, le sous-traitant a la possibilité d'effectuer directement auprès de l'autorité de contrôle compétente (la CNPD), au nom et pour le compte du responsable de traitement, une violation de données à caractère personnel.

Cette notification aura lieu 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.

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.

4.8. Analyses d'impact

Le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.

Le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

4.9. Mesures de sécurité Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté au risque.

Les mesures suivantes ont été prises [...]

DECRIRE LES MESURES :

EXEMPLES

- 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 sous-traitant s'engage à mettre en œuvre les mesures de sécurité prévues par [code de conduite, certification].

4.10. Sort des données Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à, au choix du responsable du traitement,

- à détruire toutes les données à caractère personnel
- à renvoyer toutes les données à caractère personnel au responsable de traitement, ou un sous-traitant désigné par le responsable du traitement ; 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.

4.11. Délégués 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 Général sur la Protection des Données.

Le responsable du traitement pour toute question relative à la protection des données personnelles peut être contacté à l'adresse e-mail suivante : [...]

4.12. Documentation Le sous-traitant déclare documenter le traitement des données à caractère personnel nécessaires pour l'exécution de la prestation citée au point 1 des présentes clauses contractuelles conformément au Règlement Général sur la Protection des Données.

NB. Si le sous-traitant emploie au moins 250 salariés, ou si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel, ou porte sur des catégories particulières de données (p.ex . extrait de casier judiciaire), 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.

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations.

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

Le responsable de traitement s’engage à :

1. fournir au sous-traitant les données visées au POINT 2 des présentes clauses ;
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
3. 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 ;
4. superviser le traitement, y compris réaliser des inspections auprès du sous-traitant.

Fait à **Luxembourg**, le **.../.../...**

En deux exemplaires originaux, chaque partie reconnaissant avoir reçu le sien.

Pour le responsable du traitement	Pour le sous-traitant
Nom/Prénom et fonction [...]	Nom/Prénom et fonction [...]
Signature _____	Signature _____