NEOVIAQ

\ FIDUCIAIRE
\ HUMAN RESOURCES
\ ADVISORY
\ INTELLECTUAL PROPERTY
\ DATA PROTECTION

CONTRAT DE SOUS-TRAITANCE PORTANT SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

INFORMATIONS PRÉLIMINAIRES IMPORTANTES :

NEOVIAQ et le Client (« les Parties ») ont conclu un contrat de prestation de services principal définit à l'article 1 du Contrat de sous-traitance. Le Contrat de sous-traitance fait partie intégrante de l'Accord. Les Parties entendent compléter l'Accord par le présent Contrat de sous-traitance (« Contrat de sous-traitance ») et acceptent qu'en cas de divergence ou d'incohérence entre l'Accord et le Contrat de sous-traitance, ce dernier prime.

TABLE DES MATIERES

NEOVIAQ Advisory
CO.Results Consulting S.à r.l./GmbH
61, Gruuss-Strooss \ L-9991 Weiswampach
T. +352 97 80 81-1

Capital/Kapital 20.000€ \ TVA/MwSt. LU 31726468
RCS/HR Luxembourg B 239 653 \ Autor. Gouv. /Niederlass.gen. 10110140 / 0-1

BGL LU86 0030 2450 9712 0000 BIC BGLLLULL

advisory@neoviaq.lu

www.neoviaq.lu

1. DÉFINITIONS

1.1. **Accord** : l'Accord comprend la lettre de mission, les conditions générales de NEOVIAQ et le Contrat de sous-traitance.

1.2. **Client :** la personne physique ou morale faisant appel aux services de NEOVIAQ conformément à l'Accord.

1.3. **Données à caractère personnel** : l'ensemble des informations se rapportant à une personne physique identifiée ou identifiable, listées à l'annexe 1 du Contrat de sous-traitance.

1.4. **Données sensibles :** les données à caractère personnel qui révèlent : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé, données concernant l'orientation sexuelle, ou encore les données à caractère personnel relatives aux condamnations pénales et aux infractions.

1.5. **Fuite de données à caractère personnel** : désigne une violation de la sécurité ou toute autre action ou omission conduisant à la destruction, perte, altération, divulgation ou accès non autorisé ou illicite des Données personnelles du Client transmises, stockées ou traitées de toute autre manière par le Sous-traitant dans le cadre du présent Contrat de sous-traitance.

1.6. **Livrables** : tous les produits et/ou services devant être livrés par le Sous-traitant au Client dans le cadre de l'Accord.

1.7. **Mission** : la/les prestation(s) de services définie(s) dans la lettre de mission.

1.8. **Personne concernée** : personne physique identifiée ou identifiable à laquelle se rapportent les Données à caractère personnel.

1.9. **Responsable de traitement** : en ce qui concerne le Contrat de sous-traitance et l'Accord, le Client doit être considéré comme le responsable de traitement des Données à caractère personnel. En effet, l'article 4, 1, 7) du RGPD définit le responsable de traitement comme étant : « *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 (…)* ».

1.10. **RGPD** : 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.

1.11. **Sous-traitant** : en ce qui concerne le Contrat de sous-traitance et l'Accord, NEOVIAQ doit être considéré comme le sous-traitant des Données à caractère personnel. En effet, l'article 4, 1, 8) du RGPD définit le sous-traitant comme étant : *« 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 ».*

NEOVIAQ Advisory
CO.Results Consulting S.à r.l./GmbH
61, Gruuss-Strooss \ L-9991 Weiswampach
T. +352 97 80 81-1

Capital/Kapital 20.000€ \ TVA/MwSt. LU 31726468
RCS/HR Luxembourg B 239 653 \ Autor. Gouv. /Niederlass.gen. 10110140 / 0-1

BGL LU86 0030 2450 9712 0000 BIC BGLLLULL

advisory@neoviaq.lu

www.neoviaq.lu

2. OBJET DU CONTRAT DE SOUS-TRAITANCE

2.1. Afin de mener à bien sa Mission, NEOVIAQ agit en qualité de Sous-traitant des Données à caractère personnel que lui transmet le Client. Le Client, quant à lui, agit en qualité de Responsable de traitement des Données à caractère personnel.

2.2. En sa qualité de Responsable de traitement, le Client conserve le contrôle sur les Données à caractère personnel et détermine l'objet, la nature, la/les finalité(s), les moyens et la durée du traitement des Données à caractère personnel par le Sous-traitant dans le cadre de l'Accord et du Contrat de sous-traitance. En sa qualité de Sous-traitant, NEOVIAQ ne traite les Données à caractère personnel que sur instruction du Client.

2.3. Conformément à l'article 28, §3, du RGPD, les Parties entendent compléter l'Accord par le Contrat de sous-traitance afin, notamment, d'encadrer le traitement des Données à caractère personnel par le Sous-traitant et de définir les obligations et les responsabilités respectives des Parties.

2.4. Les Parties s'engagent à veiller au respect de l'ensemble des dispositions légales et réglementaires en matière de protection des données.

3. OBLIGATIONS DU SOUS-TRAITANT / NEOVIAQ

Traitement selon les instructions du Client :

3.1. Le Sous-traitant s'engage à ne traiter les Données à caractère personnel reçues du Client qu'aux fins de la fourniture des Livrables et de l'accomplissement de la Mission. Le Sous-traitant n'agit que sur instruction écrite du Client et s'engage à ne pas traiter les Données à caractère personnel pour ses finalités propres ou pour celles de tiers. Excepté pour les besoins normaux de la Mission et sauf application d'une disposition légale ou instruction expresse du Client, le Sous-traitant ne communique pas les Données à caractère personnel à des tiers.

3.2. Si une disposition légale ou règlementaire s'appliquant au Sous-traitant, contraint ce dernier à un traitement sortant du cadre fixé par le Contrat de sous-traitance ou l'Accord, le Sous-traitant le notifiera au Responsable de traitement, à moins que la disposition légale ou réglementaire pertinente empêche une telle notification pour des raisons d'intérêt général.

Durée du traitement :

3.3. La durée du traitement est limitée à la durée nécessaire à l'accomplissement de la Mission, et en tout état de cause, la durée du traitement ne peut excéder la durée du présent Contrat de sous-traitance, sauf application d'une disposition légale ou instruction expresse du Client exigeant une prolongation du traitement des Données à caractère personnel.

Recours à des sous-traitants :

3.4. Le Client consent par la signature du Contrat de sous-traitance à l'utilisation de sous-traitants par le Sous-traitant afin de mener à bien la Mission.

3.5. Le Sous-traitant s'engage à conclure avec l'ensemble de ses sous-traitants un contrat contenant des obligations similaires en matière de protection des données que celles énoncées dans le présent Contrat de sous-traitance.

3.6. Sur demande du Client, le Sous-traitant s'engage à fournir une liste complète de ses sous-traitants traitant des données à caractère personnel du Client.

Mesures techniques et organisationnelles de sécurité :

3.7. Le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles appropriées afin :

- De protéger les données à caractère personnel reçues du Responsable de traitement. Ces mesures assurent un niveau de sécurité approprié aux risques associés et à la nature des données à caractère personnel et tiennent compte de l'état de la technique, de la nature, du contexte et des finalités du traitement.
- D'assister le Client dans l'accomplissement de son obligation de répondre aux Personnes concernées qui exercent leurs droits, y compris notamment le droit à l'information et à l'accès aux Données personnelles, le droit de rectification et d'effacement, le droit de restriction, le droit à la portabilité des données et le droit de s'opposer au traitement.

3.8. Les mesures techniques et organisationnelles mises en place par le Sous-traitant sont décrites à l'annexe 2 du Contrat de sous-traitance.

Audit

3.9. Le Sous-traitant s'engage à permettre au Client et aux auditeurs mandatés par le Client d'inspecter et d'auditer les activités de traitement de Données à caractère personnel dont il est question dans le Contrat de sous-traitance.

3.10. Les audits dont il est question au point 3.9 ont lieu aux frais du Client et sous réserve du respect du droit de l'Union ou du droit des Etats membres.

3.11. Le Client ne fait appel qu'à des auditeurs mandatés disposant des compétences nécessaires pour mener à bien ce type d'audit et démontrant des garanties de confidentialité suffisantes. Si la personne choisie par le Client ne présente manifestement pas les compétences et les garanties nécessaires, le Sous-traitant se réserve le droit de le refuser.

3.12. Le Client est tenu de notifier sa volonté de procéder un audit de NEOVIAQ par l'envoi d'une lettre recommandée au moins deux (2) mois avant le début de l'audit. La notification doit impérativement contenir les coordonnées complètes de l'auditeur mandaté.

3.13. L'auditeur mandaté doit impérativement signer un accord de confidentialité en faveur de NEOVIAQ. Tout résultat ou information résultant de l'audit sont confidentielles et ne peuvent en aucun cas faire l'objet d'une divulgation à des tiers.

Obligations complémentaires

3.14. Le Sous-traitant s'engage également à :

- Ne traiter aucune Donnée à caractère personnel en dehors de l'Espace Économique Européen (ci-après également dénommé « EEE ») sans le consentement écrit préalable du Client, si un tel consentement devait être donné, le Sous-traitant veille à ce que des mesures de protection adéquates nécessaires soient prises ;
- Veiller à ce que son personnel et toute autre personne qu'il autorise à traiter les Données à caractère personnel soient liés par une obligation de confidentialité appropriée ;
- En cas de Fuite des Données à caractère personnel en informer le Client, immédiatement et en tout état de cause au plus tard 24 heures après que le Sous-traitant ait pris connaissance de la Fuite des Données à caractère personnel ;
- Tenir à jour un registre de Données à caractère personnel permettant de fournir au Client les informations nécessaires sur le traitement. Ce registre doit contenir au moins les informations suivantes :
  - Le cas échéant, les coordonnées du délégué à la protection des données du Sous-traitant (ci-après dénommé « DPO »), ainsi que celle du délégué à la protection des données du Responsable du traitement (si applicable) ;
  - Les catégories de traitements de Données à caractère personnel effectués pour le compte du Responsable de traitement ;
  - Une description générale des mesures de sécurité techniques et organisationnelles mises en place pour assurer la conformité avec le RGPD et les autres lois applicables en matière de protection des données ;
  - Les éventuels transferts de données à caractère personnel vers un pays en dehors de l'EEE, y compris l'identification de ces pays tiers et la documentation des garanties appropriées qui sont mises en place pour des situations spécifiques, sauf lorsque le transfert est basé sur une décision d'adéquation.

4. OBLIGATIONS DU RESPONSABLE DE TRAITEMENT / DU CLIENT

4.1. Le Client garantit que les instructions fournies au Sous-traitant sont licites et conformes aux dispositions légales et réglementaires en matière de protection des données, en particulier le

RGPD. Si le Sous-traitant venait à estimer que les instructions du Client portent atteinte aux dispositions légales et réglementaires en matière de protection des données, il serait alors tenu d'en informer le Client. Le Sous-traitant étant alors en droit de décider de ne pas exécuter et/ou de suspendre le traitement. Tout défaut éventuel de notification dans le chef du Sous-traitant n'altère en rien la responsabilité du Client à l'égard du Sous-traitant en raison de l'instruction illicite.

4.2. Si le Client agit lui-même en qualité de sous-traitant pour le compte d'un autre responsable de traitement, il garantit que ses instructions sont conformes aux instructions qui ont été fournies par le responsable de traitement initial.

4.3. Le Client garantit que toutes les Données à caractère personnel qui sont transmises aux Sous-traitants ont été obtenues de manière licite et peuvent être traitées en toute licéité par le Sous-traitant pendant toute la durée du Contrat de sous-traitance.

4.4. Le Client est responsable du caractère exact des Données à caractère personnel. Le Client s'engage à informer le Sous-traitant de tout changement et/ou mise à jour relatif aux Données à caractère personnel.

5. TRAITEMENT DE DONNÉES SENSIBLES

5.1. Le Responsable de traitement s'engage à ne fournir aucune Donnée sensible au Sous-traitant, sauf celles qui sont strictement nécessaires à l'accomplissement de la Mission. En effet, l'accomplissement de la Mission ne suppose, en principe, pas le traitement d'autres Données sensibles que celles indiquées à l'annexe 1 du Contrat de sous-traitance.

5.2. En cas de traitement de Données sensibles pour le compte du Responsable de traitement, le Sous-traitant indique, sur demande, les catégories de personnes susceptibles d'accéder aux Données sensibles et tient à jour une liste des personnes ayant accès à ces catégories de Données à caractère personnel.

6. DURÉE ET RÉSILIATION / RESTITUTION ET SUPPRESSION DES DONNÉES À CARACTÈRE PERSONNEL

6.1. Le Contrat de sous-traitance est conclu pour une période égale à la durée de l'Accord. Le Contrat de sous-traitance peut être résilié dans les mêmes conditions que l'Accord.

6.2. À la fin du Contrat de sous-traitance, le Sous-traitant, sur demande et aux frais du Responsable de traitement restituera toutes les Données à caractère personnel du Responsable de traitement.

6.3. À la fin du contrat de sous-traitance, le Sous-traitant s'engage, dans la mesure du possible, à supprimer les Données à caractère personnel, sauf dans les cas où le droit de l'Union ou le droit luxembourgeois exige la conservation des Données à caractère personnel.

7. CLAUSES DIVERSES

Responsabilité :

7.1. Les Parties conviennent que toute limitation éventuelle de la responsabilité du Sous-traitant telle qu'elle est énoncée dans l'Accord s'applique aux obligations du Sous-traitant en vertu du Contrat de sous-traitance.

Divisibilité :

7.2. Si une disposition du présent Contrat de sous-traitance est jugée illégale ou inapplicable, cette disposition sera modifiée par les Parties afin de la rendre légale ou exécutoire, tout en conservant autant que possible la signification initiale que les Parties ont voulues à l'égard de cette disposition.

Droit applicable et tribunaux compétents :

7.3. Le présent Contrat de sous-traitance est régi et interprété conformément au droit luxembourgeois (sans référence à ses règles de conflit de lois). Tout litige y afférent sera porté devant les Cours et tribunaux compétents du siège social du Sous-traitant. À tout moment, les Parties peuvent déjà saisir ces Cours et tribunaux ou d'autres juridictions compétentes de toute mesure provisoire (y compris les mesures conservatoires).

Confidentialité du Contrat de sous-traitance :

7.4. Le présent Contrat de sous-traitance est confidentiel et ne peut être transmis par les Parties à des tiers que moyennant l'accord de l'autre partie.

7.5. En cas de divulgation à une autorité de contrôle, une autorité judiciaire ou tout autre autorité publique compétente chaque partie se doit d'en informer l'autre partie avant la divulgation du Contrat de sous-traitance.

ANNEXE 1 - LISTING DES DONNÉES À CARACTÈRE PERSONNEL

Types de Missions	Catégories de données traitées
Conseils aux entreprises	- ***Données d'identification et de contact*** : Nom ; Prénom ; Âge ; Date de naissance ; Sexe ; Numéro de registre national ou d'affiliation à la sécurité sociale ; Copie de votre carte d'identité ; Adresse électronique ; Numéro de téléphone, de GSM ; Adresse du domicile ; Pays de résidence ; etc. - ***Données d'identification professionnelles*** : Votre entreprise ; Titre/Fonction ; Département ; Adresse électronique professionnelle ; etc. - Les données personnelles figurant sur ***les factures d'entrées et de sorties***. - ***Toutes autres données à caractère personnel*** nécessaires à l'accomplissement de notre mission et que vous nous communiquerez volontairement, par exemple celles relatives à vos employés.

ANNEXE 2 – LISTING DES MESURES TECHNIQUES ET ORGANISATIONNELLES DE SÉCURITÉ

Catégories	Description
Mesures organisationnelles	➢ Sensibilisation / formation des employés : Informer et sensibiliser les employés manipulant des données personnelles ; organisation de formation des employés (au moins 1 fois / an). ➢ Politique de gestion des données : Politique interne de gestion des données personnelles ; Charte d'utilisation des outils informatiques.
Contrôles d'accès logiques	➢ Gestion des accès / habilitations aux serveurs et logiciels : Définir les accès aux logiciels (« *need to know* ») ; Suppression des accès obsolètes ; Révision annuelle des autorisations d'accès/habilitations. ➢ Sécurisation de l'informatique mobile : Prévoir des moyens de chiffrement des équipements mobiles ; Faire des sauvegardes ou synchronisation régulières des données ; Exiger un code secret pour le déverrouillage des smartphones professionnels. ➢ Sécurisation des postes de travail : Prévoir une procédure de verrouillage automatique de session en cas d'inactivité ; Utiliser des antivirus régulièrement mis à jour. ➢ Installer des « pares-feu » (*firewall*). ➢ Sécuriser les accès distants des appareils informatiques nomades par VPN.

Sauvegarder et prévoir la continuité d'activité	➢ Effectuer des sauvegardes régulières. ➢ Stocker les supports de sauvegarde dans un endroit sécurisé.
Gestion de la sous-traitance	➢ Clause spécifique relative à la sécurisation des données dans les contrats des sous-traitants. ➢ Prévoir les conditions de restitution et de destruction des données. ➢ S'assurer de l'effectivité des garanties prévues (audits de sécurité, visites, etc.).

NEOVIAQ Advisory
CO.Results Consulting S.à r.l./GmbH
61, Gruuss-Strooss \ L-9991 Weiswampach
T. +352 97 80 81-1

Capital/Kapital 20.000€ \ TVA/MwSt. LU 31726468
RCS/HR Luxembourg B 239 653 \ Autor. Gouv. /Niederlass.gen. 10110140 / 0-1

BGL LU86 0030 2450 9712 0000 BIC BGLLLULL

advisory@neoviaq.lu

www.neoviaq.lu