

Contrat de sous-traitance

(article 28 du RGPD)

Le présent Contrat de sous-traitance est conclu entre :

MYSOLUTION FRANCE, dont le siège social est situé 52 boulevard de Sébastopol, 75003 Paris, France, immatriculée au registre du commerce et des sociétés de Paris sous le numéro 514 565 712, ci-après « Mysolution » ou le « Sous-traitant » ;
et

le Client, tel qu'identifié dans le Contrat, ci-après le « Responsable du traitement ».

Le présent Contrat de sous-traitance fait partie intégrante du Contrat et est conclu par la signature de celui-ci.

1. GÉNÉRALITÉS

- 1.1 Les dispositions du Contrat s'appliquent intégralement au présent Contrat de sous-traitance. Le présent Contrat de sous-traitance fait partie intégrante du Contrat. Dans la mesure où le Contrat contient des dispositions relatives au traitement de données à caractère personnel, les dispositions du présent Contrat de sous-traitance prévalent.
- 1.2 En ce qui concerne le traitement de données à caractère personnel dans le cadre du Contrat, le Client est considéré comme le Responsable du traitement au sens de l'article 4, point 7), du Règlement général sur la protection des données (« RGPD ») et Mysolution comme le Sous-traitant au sens de l'article 4, point 8), du RGPD.
- 1.3 Les termes du RGPD tels que « traitement », « données à caractère personnel », « responsable du traitement » et « sous-traitant » ont le sens qui leur est donné dans le RGPD.

2. TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

- 2.1 Les catégories de personnes concernées et les types de données à caractère personnel traités par le Sous-traitant, ainsi que les finalités de ce traitement, sont précisés à l'**Annexe 1**.
- 2.2 Le Sous-traitant ne traite les données à caractère personnel portées à sa connaissance que sur la base d'instructions documentées du Responsable du traitement et uniquement dans le cadre de l'exécution du Contrat, sauf si le droit de l'Union ou le droit de l'État membre auquel le Sous-traitant est soumis l'oblige à procéder au traitement. Dans ce cas, le Sous-traitant informe 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.
- 2.3 Le Sous-traitant ne détermine ni les finalités ni les moyens essentiels du traitement des données à caractère personnel. Aucune disposition du présent Contrat de sous-traitance n'a pour objet de transférer au Sous-traitant, de quelque manière que ce soit, le contrôle des données à caractère personnel.
- 2.4 Il est interdit au Sous-traitant de traiter les données à caractère personnel :
 - 2.4.1 pour ses propres finalités ;
 - 2.4.2 à des fins autres que celles raisonnablement nécessaires dans le cadre de l'exécution du Contrat, ou allant au-delà de celles-ci ;
 - 2.4.3 en les communiquant à des tiers, dans la mesure où cela n'est pas autorisé par le Contrat et/ou le

présent Contrat de sous-traitance et/ou par une disposition de droit impératif en vertu de laquelle le Sous-traitant est tenu de communiquer des données à caractère personnel à des autorités (de contrôle ou d'enquête).

3. RESPECT DES DISPOSITIONS LÉGALES ET RÉGLEMENTAIRES

- 3.1 Les Parties se conforment aux dispositions du RGPD en vigueur à tout moment ainsi qu'aux futures dispositions législatives et réglementaires (européennes) en matière de traitement de données à caractère personnel. Si de futures dispositions législatives ou réglementaires nécessitent une adaptation du présent Contrat de sous-traitance, les Parties se concertent afin de convenir de nouvelles stipulations préservant autant que possible la portée du présent Contrat de sous-traitance.
- 3.2 Le Sous-traitant prête son concours au Responsable du traitement pour la réalisation d'une analyse d'impact relative à la protection des données (AIPD), dans la mesure où cela est possible compte tenu des informations dont il dispose et de la nature du traitement. Les coûts raisonnables que cette obligation de concours entraîne pour le Sous-traitant sont supportés par le Responsable du traitement.
- 3.3 Si et dans la mesure où le Responsable du traitement est tenu, en vertu de dispositions législatives ou réglementaires, de fournir à une autorité de contrôle des informations relatives au traitement de données à caractère personnel, le Sous-traitant lui prête, à première demande, tout le concours raisonnablement requis afin que ces informations soient disponibles et que l'autorité de contrôle puisse être dûment informée.

4. CONFIDENTIALITÉ

- 4.1 Le Sous-traitant est tenu de préserver la confidentialité des données à caractère personnel et veille à ce que les personnes autorisées à traiter ces données s'engagent à respecter la confidentialité.
- 4.2 Cette obligation de confidentialité subsiste après la fin du présent Contrat de sous-traitance, sauf pour les informations déjà rendues publiques autrement qu'à la suite d'un manquement à l'obligation de confidentialité susmentionnée.

5. MESURES DE SÉCURITÉ DU SOUS-TRAITANT

- 5.1 Le Sous-traitant prend les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, comprenant notamment les mesures mentionnées à l'**Annexe 2**.
- 5.2 Lorsqu'il détermine ces mesures, le Sous-traitant tient compte de l'état des connaissances, des coûts de mise en œuvre, ainsi que de la nature, de la portée, du contexte et des finalités du traitement et des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques.
- 5.3 Lors de l'évaluation du niveau de sécurité approprié, le Sous-traitant tient particulièrement compte des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération ou de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.
- 5.4 Le Sous-traitant prend des mesures pour garantir que toute personne physique agissant sous son autorité et ayant accès aux données à caractère personnel ne les traite que sur instruction du Responsable du traitement, à moins que le droit de l'Union ou le droit de l'État membre auquel le Sous-

traitant est soumis ne l'oblige à procéder au traitement.

6. CONTRÔLE PAR LE RESPONSABLE DU TRAITEMENT

- 6.1 Le Sous-traitant fournit au Responsable du traitement, à la demande de ce dernier, les informations nécessaires pour lui permettre d'apprécier le respect par le Sous-traitant des dispositions des articles 2, 4, 5, 7 et 10 du présent Contrat de sous-traitance.
- 6.2 Le Responsable du traitement a le droit de faire vérifier, par un expert indépendant tenu à une obligation de confidentialité, le respect par le Sous-traitant des obligations prévues aux articles 2, 4, 5, 7 et 10 du présent Contrat de sous-traitance. Le Sous-traitant coopère à cet audit et met à disposition, dans les meilleurs délais, toutes les informations raisonnablement pertinentes pour celui-ci. Les coûts des audits réalisés à la demande du Responsable du traitement sont supportés par ce dernier, sauf s'il apparaît que le Sous-traitant n'a pas suffisamment respecté ses obligations, auquel cas le Sous-traitant supporte ces coûts.
- 6.3 S'il ressort du rapport d'audit de l'expert indépendant que les mesures et dispositifs mis en place par le Sous-traitant ne sont pas suffisamment conformes aux exigences du présent Contrat de sous-traitance, le Sous-traitant prend sans délai les mesures nécessaires pour s'y conformer.

7. NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

- 7.1 Le Sous-traitant informe le Responsable du traitement sans délai dès qu'il constate qu'une violation de données à caractère personnel s'est produite. Cette information est fournie de manière à permettre au Responsable du traitement de satisfaire à

ses obligations au titre des articles 33 et 34 du RGPD.

- 7.2 Le Sous-traitant tient le Responsable du traitement pleinement informé de l'avancement des mesures correctives et de tout développement pertinent concernant la violation visée à l'article 7.1 et ses conséquences. Le Sous-traitant prend toutes les mesures que l'on peut raisonnablement attendre de lui afin de remédier aux conséquences préjudiciables de la violation visée à l'article 7.1 ou, le cas échéant, de les limiter autant que possible. 7.17.1
- 7.3 Il est interdit au Sous-traitant de communiquer avec la ou les personnes concernées et/ou la ou les autorités de contrôle au sujet d'une violation visée à l'article 7.1, autrement que sur instruction du Responsable du traitement ou avec son accord exprès. 7.1

8. SOUS-TRAITANTS ULTÉRIEURS

- 8.1 Le Responsable du traitement autorise par la présente le Sous-traitant, de manière générale et par écrit, à faire appel à d'autres sous-traitants pour une partie du traitement des données à caractère personnel pendant la durée du Contrat, comme indiqué à l'**Annexe 1**.
- 8.2 Le Sous-traitant informe le Responsable du traitement de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants ultérieurs, le Responsable du traitement disposant d'un délai de 30 jours pour s'opposer à ces changements.
- 8.3 Le Sous-traitant garantit que tous les sous-traitants ultérieurs qu'il fait intervenir dans l'exécution du Contrat respecteront les obligations énoncées dans le présent Contrat de sous-traitance, en particulier l'obligation de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées, de manière à assurer un niveau de protection

équivalent des données à caractère personnel.

9. DEMANDES DES PERSONNES CONCERNÉES

- 9.1 Le Responsable du traitement est soumis, en vertu du RGPD, à des obligations envers les personnes concernées, notamment en matière de fourniture d'informations et d'exercice des droits d'accès, de rectification et d'effacement des données à caractère personnel. Le Sous-traitant prête son concours, dans la mesure du possible, à l'exécution des obligations incombant au Responsable du traitement. Le Sous-traitant se réserve le droit de facturer au Responsable du traitement son tarif horaire habituel pour ce concours.
- 9.2 Si une personne concernée s'adresse directement au Sous-traitant pour l'exercice de ses droits au titre du RGPD, le Sous-traitant ne répond pas sur le fond mais en informe sans délai le Responsable du traitement.

10. TRANSFERTS INTERNATIONAUX

- 10.1 Le Sous-traitant veille à ce que tout traitement de données à caractère personnel effectué par lui ou pour son compte, y compris par les tiers qu'il fait intervenir, dans le cadre de l'exécution du Contrat, ait lieu au sein de l'Espace économique européen (EEE). Tout transfert en dehors de l'EEE est conforme au chapitre V du RGPD.
- 10.2 En conséquence, sans l'accord écrit préalable du Responsable du traitement, le Sous-traitant ne peut ni transférer des données à caractère personnel vers un pays ou une organisation situés en dehors de l'EEE, ni les y conserver, ni les rendre accessibles depuis un pays situé en dehors de l'EEE, sauf si le transfert est conforme au chapitre V du RGPD ou si le droit de l'Union ou le droit de l'État membre auquel le Sous-traitant est soumis l'oblige à procéder au

traitement. Dans ce cas, le Sous-traitant informe 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.

11. GARANTIE ET INDEMNISATION

- 11.1 Le Responsable du traitement garantit que le traitement des données est effectué conformément aux dispositions législatives et réglementaires applicables. Cela signifie en tout état de cause que le Responsable du traitement garantit qu'il est en droit de collecter ou de faire collecter les données et qu'il est habilité à traiter ou à faire traiter ces données.
- 11.2 Le Responsable du traitement garantit et indemnise le Sous-traitant contre les dommages et coûts résultant de toute réclamation de tiers, y compris expressément la ou les personnes concernées et les autorités de contrôle (telles que la Commission nationale de l'informatique et des libertés, la CNIL), en lien avec ou découlant d'un traitement illicite et/ou d'un autre manquement au RGPD et/ou au présent Contrat de sous-traitance imputable au Responsable du traitement.

12. RESPONSABILITÉ

- 12.1 Le Sous-traitant répond de la bonne exécution des obligations découlant du présent Contrat de sous-traitance. Le présent Contrat de sous-traitance fait partie intégrante du Contrat conclu entre le Responsable du traitement et le Sous-traitant ; la responsabilité totale du Sous-traitant est dès lors limitée conformément aux stipulations du Contrat et/ou des conditions générales.

13. DURÉE DU CONTRAT DE SOUS-TRAITANCE

- 13.1 Le présent Contrat de sous-traitance entre en vigueur au moment de l'entrée en vigueur du Contrat et est conclu pour la durée du Contrat.
- 13.2 Dès que le Contrat est résilié ou prend fin, pour quelque raison que ce soit, le présent Contrat de sous-traitance demeure en vigueur aussi longtemps que le Sous-traitant traite des données à caractère personnel, après quoi il prend fin de plein droit.
- 13.3 Le Responsable du traitement indique au Sous-traitant, avant la fin du Contrat ou dans les trente (30) jours suivant celle-ci, si les données à caractère personnel doivent être restituées ou effacées. À défaut d'indication dans ce délai, le Sous-traitant peut procéder à leur effacement conformément à l'alinéa suivant.

- 13.4 Le Sous-traitant est en droit d'effacer les données à caractère personnel trente (30) jours calendaires après la fin du Contrat.
- 13.5 Le Sous-traitant veille à ce que les données à caractère personnel soient effacées au plus tard trois (3) mois après la fin du Contrat.
- 13.6 Le Sous-traitant ne conserve une copie des données à caractère personnel que s'il y est tenu en vertu d'une disposition légale impérative.

14. DISPOSITION FINALE

- 14.1 Les modifications et compléments apportés au présent Contrat de sous-traitance ne sont valables que s'ils ont été convenus par écrit entre les Parties.
- 14.2 Le présent Contrat de sous-traitance est exclusivement régi par le droit français.

ANNEXE 1 APERÇU DES DONNÉES À CARACTÈRE PERSONNEL ET DES SOUS-TRAITANTS ULTÉRIEURS

I. Types de données à caractère personnel (à déterminer par le Responsable du traitement)

- Données d'identification d'une personne physique, numéro de sécurité sociale (numéro d'inscription au répertoire, NIR), nom, adresse et lieu de résidence
- Sexe, date de naissance, numéro de téléphone, adresse e-mail, nationalité, photo (d'identité)
- Profession et emploi, données relatives à l'expérience professionnelle et au parcours professionnel, CV
- Données relatives aux formations, cours et stages suivis et à suivre
- Données financières (numéro de compte bancaire)
- Comportement de navigation sur le site web (adresse IP)

II. Catégories de personnes concernées (à déterminer par le Responsable du traitement)

- Candidats / Postulants / Personnes évaluées
- Clients
- Contacts marketing
- Salariés
- Fournisseurs

III. Finalités du traitement des données à caractère personnel

- Finalités de recrutement
- Finalités de marketing
- Finalités de paiement
- Finalités administratives
- Finalités statistiques
- Sécurité, amélioration et développement du Service et de l'Application
- Évaluation et acceptation des clients (potentiels)
- Exécution de l'accord ou du contrat

IV. Sous-traitants ultérieurs

Nom : **Salesforce.org**

Adresse : Prins Bernhardplein 200 1097JB Amsterdam, Pays-Bas

Description du service : Services cloud (recrutement et sélection, gestion des relations, gestion des clients et des contrats)

Nom : **Microsoft BV**

Adresse : Evert van de Beekstraat 354 1118 CZ Amsterdam, Pays-Bas

Description du service : services cloud (gestion du personnel, gestion des temps, administration financière et gestion de la paie)

Nom : **Google Netherlands B.V.**

Adresse : Claude Debussylaan 34 1082 MD Amsterdam, Pays-Bas

Description du service : Services cloud, IA générative et modèles de langage

Nom : **Anthropic Ireland, Limited / Anthropic PBC**

Adresse (EEE) : 6e étage South Bank House, Barrow Street, Dublin 4, Dublin, Irlande

Adresse (États-Unis) : 548 Market Street, PMB 90375, San Francisco, Californie 94104, États-Unis

Description du service : systèmes d'IA, IA générative et modèles de langage

Nom : **Snowflake Computing Netherlands B.V.**

Adresse : Gustav Mahlerlaan 300 1022 AB Amsterdam, Pays-Bas

Description du service : Data lake, entrepôt de données, traitement des métadonnées et télémétrie

Nom : **Spotler Nederland BV**

Adresse : Boris Pasternaklaan 16 2719 DA Zoetermeer, Pays-Bas

Description du service : traitement des e-mails, gestion des clients et des contrats

Nom : **Textkernel BV**

Adresse : Nieuwendammerkade 26A-5 1022 AB Amsterdam, Pays-Bas

Description du service : Traitement des données de CV, recrutement et sélection

Nom : **NIXZ**

Adresse : Binckhorstlaan 36 - C0.28, 2516 BE Den Haag, Pays-Bas

Description du service : Extension pour créer et gérer un lien entre LinkedIn et les candidats.

Nom : Supabase Inc.

Adresse : Une société du Delaware dont les bureaux sont situés au 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513

Description du service : authentification et base de données Hirewithmaia pour le traitement des conversations, journaux et données d'utilisation

Nom : Veeam Software B.V.

Adresse (EEE) : Reykjavikstraat 1, 3543 KB, Utrecht, Pays-Bas

Adresse (États-Unis) : 3000 Carillon Point, Suite 600, Kirkland (Seattle), WA 98033, États-Unis

Description du service : logiciel de sauvegarde et services cloud de sauvegarde

V. Durée du traitement

Pendant la durée du Contrat de sous-traitance.

ANNEXE 2 SPÉCIFICATION DE LA SÉCURITÉ

Mesures de sécurité techniques et organisationnelles

A. Informations générales sur les mesures de sécurité prises :

- Une politique de sécurité de l'information a été élaborée, incluant les meilleures pratiques en matière de sécurité de l'information. Le programme de sécurité de l'information s'applique à l'ensemble de l'infrastructure informatique, avec des règles strictes relatives aux mots de passe, des pare-feux et une protection antivirus.
- Les activités de traitement sont documentées, les responsabilités sont clairement attribuées et des évaluations périodiques de la protection des données sont réalisées afin de garantir la conformité.
- Les systèmes sont régulièrement mis à jour et corrigés, avec une protection antivirus à jour et des analyses de vulnérabilités pour prévenir les abus.
- Les employés du Sous-traitant ont signé un contrat de travail comportant une clause de confidentialité. Des formations régulières sur les exigences du RGPD, les bonnes pratiques de protection des données et la sécurité de l'information sont dispensées à tous les collaborateurs, afin de favoriser une culture de conformité.
- Les données à caractère personnel ne sont traitées que lorsque cela est strictement nécessaire à la fourniture de services déterminés, sans collecte d'informations superflues ou non pertinentes.
- Les données à caractère personnel ne sont traitées que par des sous-traitants ultérieurs approuvés avec lesquels un contrat de sous-traitance a été conclu et qui offrent au moins le même niveau de protection des données à caractère personnel que Mysolution.
 - Google propose des directives concernant la conformité au RGPD : <https://cloud.google.com/privacy/gdpr>
 - Microsoft propose des directives concernant la conformité au RGPD : <https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure/GDPR>
 - Salesforce propose des directives concernant la conformité au RGPD : https://help.salesforce.com/articleView?id=data_protection_and_privacy.htm
 - Snowflake propose des directives concernant la conformité au RGPD : <https://www.snowflake.com/legal/>
- Les données à caractère personnel ne sont conservées que le temps nécessaire à la finalité déterminée.
- Si le Sous-traitant reçoit des données à caractère personnel sous forme de sauvegarde en vue de résoudre un incident logiciel ou d'effectuer une conversion de données, celles-ci sont stockées dans un segment de réseau cloisonné auquel seules les personnes directement concernées ont accès. Les données sont détruites dès qu'il n'est plus nécessaire de les conserver.
- Des plans documentés garantissent la continuité du service, avec des tests annuels visant à vérifier leur efficacité.

B. Mesures visant à garantir que seul le personnel autorisé a accès aux données à caractère personnel :

- Le Sous-traitant applique une structure d'autorisations et de droits fondée sur le rôle de l'utilisateur. Seuls les collaborateurs disposant du rôle approprié ont accès aux données à caractère personnel.
- L'accès au centre de données n'est accordé qu'au personnel autorisé.

C. Mesures visant à protéger les données à caractère personnel contre la perte ou l'altération, ainsi que contre le traitement, l'accès ou la divulgation non autorisés ou illicites :

- Les données sont stockées dans un centre de données européen certifié ISO 27001. Le centre de données est sécurisé 24 h/24, 7 j/7, à la fois électroniquement et physiquement.
- Les employés du Sous-traitant et de ses sous-traitants ultérieurs n'ont accès aux serveurs qu'à distance, avec authentification à deux facteurs obligatoire.
- Les journaux d'accès aux serveurs sont conservés et régulièrement contrôlés pour détecter les actions non autorisées.

- Un système de sauvegarde robuste garantit l'intégrité et la disponibilité des données, avec un plan de reprise après sinistre éprouvé.

D. Mesures de détection des vulnérabilités et de gestion des incidents :

- Une solution de détection et de réponse étendues (XDR), combinée à un centre opérationnel de sécurité (SOC) disponible 24 h/24 et 7 j/7, détecte les activités suspectes et bloque les accès non autorisés.
- Des tests d'intrusion sont réalisés périodiquement par des tiers externes sur les applications web hébergées. Les éventuelles vulnérabilités détectées sont corrigées dans l'application.
- Il existe un protocole établi pour répondre aux violations de données. La réponse aux incidents comprend des procédures documentées pour identifier, examiner et résoudre les failles de sécurité et les violations de données à caractère personnel.