

Accord sur le traitement des données

Comment obtenir un Accord contractuel : (1) remplissez les informations relatives au signataire ci-dessous ; (2) remplissez et signez la case de signature de la page 4 ; (3) envoyez l'Accord rempli et signé à SmartRecruiters de la manière suivante, soit : (i) si vous êtes un nouveau client, à votre contact commercial chez SmartRecruiters avec une copie à dpo@smartrecruiters.com, ou (ii) si vous êtes déjà un client existant, à dpo@smartrecruiters.com.

Le présent Accord sur le traitement des données (l'"**Accord**") est conclu entre _____ (ci-après le "**Client**"), domicilié à _____, et la société SmartRecruiters mentionnée dans le Contrat principal (ci-après "**SmartRecruiters**"). Le Client et SmartRecruiters sont ci-après dénommés individuellement une "**Partie**" et collectivement les "**Parties**".

Cet Accord a été pré-signé par la société SmartRecruiters citée ci-dessus. Toute modification manuscrite ou autre apportée à cet Accord sur le traitement des données sans l'approbation écrite préalable de SmartRecruiters n'aura aucune valeur contractuelle envers SmartRecruiters. S'il n'existe aucun Contrat principal entre les Parties, l'exécution de cet Accord n'aura aucune force ou effet entre SmartRecruiters et la personne ou l'entité qui contresigne cet Accord.

1. Définitions.

Les termes tels que "**Responsable du traitement des données**", "**Personne concernée**", "**Données à caractère personnel**", "**Traitement**" (y compris ses variantes) et "**Sous-traitant**" ont les significations données dans le RGPD.

"**Contrat principal**" désigne le contrat d'abonnement principal ou tout autre contrat d'abonnement entre le Client et SmartRecruiters régissant l'accès du Client au logiciel de SmartRecruiters.

"**Législation relative à la protection des données**" désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 abrogeant la directive 96/46/CE (règlement général sur la protection des données 2016/679 ("**RGPD**")), les lois nationales mettant en œuvre le RGPD et toute autre loi applicable en matière de protection des données.

2. Objet du présent Accord. Le présent Accord définit les droits et obligations du Client et de SmartRecruiters concernant le Traitement des Données à caractère personnel du Client dans le cadre du Contrat principal. Cet Accord s'applique à toutes les activités dans le cadre de et liées au Contrat principal. Dans les relations entre SmartRecruiters et le Client, SmartRecruiters est un Sous-traitant et le Client est un Responsable du traitement des données.

3. Traitement des Données - Obligations.

3.1. Exclusion des comptes personnels. Chaque individu a la faculté de créer un compte personnel dans le logiciel de SmartRecruiters. Avec ce compte personnel, l'individu est en mesure de coordonner différents profils et processus de candidature pour différentes entreprises. La collecte et le Traitement des Données à caractère personnel pour le compte personnel d'un individu ne sont pas effectués pour le Client mais uniquement pour l'individu par SmartRecruiters. Dès lors, la relation entre un individu avec un compte personnel et SmartRecruiters n'est pas régie par le présent Accord.

3.2. Garantie du Client. Le Client déclare et garantit, de manière continue pendant toute la durée du Contrat principal, que toutes les Données à caractère personnel fournies ou mises à disposition par le Client à SmartRecruiters en vue d'un Traitement dans le cadre du Contrat principal ont été collectées par le Client et transmises à SmartRecruiters conformément à la Législation en vigueur relative à la protection des données et que le Client a obtenu toutes les approbations, consentements, autorisations et licences nécessaires de la part de chaque Personne concernée requises en vertu de la Législation relative à la protection des données pour permettre à SmartRecruiters de Traiter les Données à caractère personnel conformément au Contrat principal et d'exercer ses droits et de remplir ses obligations en vertu du Contrat principal.

3.3. Assistance. SmartRecruiters assistera le Client de manière raisonnable dans les évaluations d'impact sur la protection des données, les consultations préalables avec les autorités de protection des données que le Client est tenu d'effectuer en vertu de la Législation relative à la protection des données, le traitement des demandes des Personnes concernées et toute autre obligation d'assistance requise par la loi applicable.

3.4. Personnel qualifié. SmartRecruiters n'engage que du personnel qui s'est engagé à respecter les obligations

en matière de confidentialité des données. SmartRecruiters formera régulièrement les employés à qui elle accorde l'accès aux Données à caractère personnel du Client au respect des lois sur la sécurité et la confidentialité.

3.5. Mesures techniques et organisationnelles. SmartRecruiters déclare avoir pris les mesures techniques et organisationnelles nécessaires conformément à l'article 32 RGPD pour assurer la sécurité et la protection des Données à caractère personnel contre les Traitements non autorisés ou illégaux ainsi que les pertes, destructions ou dommages accidentels, et s'engage à continuer à le faire pendant la durée du présent Accord. En particulier, SmartRecruiters a mis en œuvre les mesures techniques et organisationnelles décrites plus en détail dans l'**Annexe 2 des Clauses contractuelles types**. SmartRecruiters peut mettre en œuvre des mesures alternatives pour autant que le niveau de sécurité des mesures telles que spécifiées dans l'**Annexe 2** du présent Accord ne soit pas réduit. Afin de démontrer la conformité au présent Accord, le Client accepte que SmartRecruiters puisse fournir des attestations, rapports ou extraits à jour provenant d'organismes indépendants (par exemple des rapports/certificats ISO 27001) qui examinent et confirment que le Traitement des Données à caractère personnel du Client est conforme au présent Accord.

3.6. Violation des Données à caractère personnel. Pas plus tard que vingt-quatre heures après que SmartRecruiters ait un degré raisonnable de certitude sur la survenance d'une destruction accidentelle ou illégale, d'une perte ou d'une altération, d'une divulgation non autorisée ou d'un accès non autorisé à des Données à caractère personnel transmises, stockées ou traitées de toute autre manière par SmartRecruiters conformément au présent Accord (une "**Violation des Données à caractère personnel**"), SmartRecruiters notifiera le Client de la Violation des Données à caractère personnel, fournira les informations que le Client peut raisonnablement exiger afin de remplir ses obligations en vertu de la loi applicable en ce qui concerne la Violation des Données à caractère personnel, et prendra des mesures pour remédier à la Violation des Données à caractère personnel.

4. Clauses contractuelles types. "Clauses contractuelles types" désignent les Clauses contractuelles types contenues dans la Décision d'Exécution (UE) 2021/914 de la Commission Européenne du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil. Les Clauses contractuelles types et le Module 2 ci-après sont incorporées au présent Accord par référence. Les autres modules identifiés au sein des Clauses contractuelles type sont exclus du présent Accord et par conséquent, non-applicables aux présentes. Les Clauses contractuelles types sont identifiées aux Annexes 1, 2 et 3. Conformément à la Clause 18 des Clauses contractuelles types, les Parties conviennent que la juridiction compétente est celle de l'État membre où le Client est domicilié.

5. Sous-traitants ultérieurs.

5.1. Approbation de Sous-traitants ultérieurs. Conformément à la Clause 9, sous-section a) option 2 du Module 2 des Clauses contractuelles types, le Client donne par la présente son autorisation générale à SmartRecruiters de nommer tout sous-traitant ultérieur identifié par SmartRecruiters sur la liste suivante (la "**Liste des Sous-traitants ultérieurs**") pour traiter les Données à caractère personnel au nom de SmartRecruiters : <https://www.smartrecruiters.com/legal/subprocessors>. SmartRecruiters doit assurer que les Sous-traitants ultérieurs figurant sur cette Liste sont contractuellement tenus de protéger les Données à caractère personnel dans le respect des Législations relatives à la protection des données et conformément aux obligations imposées à SmartRecruiters dans le présent Accord. SmartRecruiters reste responsable des actes et omissions de chaque Sous-traitant ultérieur figurant sur la Liste des sous-traitants ultérieurs comme s'il s'agissait des actes et/ou omissions de SmartRecruiters. Le Client convient que SmartRecruiters puisse fournir une notification de tout changement à la Liste des sous-traitants ultérieurs en mettant à jour cette Liste sur le lien susmentionné. Toute mise à jour de ladite Liste devra être notifiée au Client dans un délai minimum de dix (10) jours avant que la modification n'opère et que SmartRecruiters ait recours à la nouvelle entité au titre de sous-traitant pour le compte du Client.

5.2. Objections concernant les Sous-traitants ultérieurs. Si le Client a un motif légitime lié à la protection des données pour s'opposer à l'ajout d'un Sous-traitant ultérieur à la Liste des sous-traitants ultérieurs, le Client peut s'y opposer en envoyant une objection et son justificatif à legal@smartrecruiters.com dans un délai maximum de trente (30) jours suite à l'ajout dudit Sous-traitant à la Liste.


Si les Parties ne parviennent pas à convenir mutuellement d'une résolution raisonnable à l'objection du Client dans les quatorze (14) jours ouvrables suivant la réception de ladite objection par SmartRecruiters, chaque Partie pourra résilier le Contrat principal en notifiant l'autre Partie par écrit.

6. Droits de vérification – Audit. Si le Client fait l'objet d'un audit ou d'une enquête de la part d'une autorité de contrôle en matière de protection des données, SmartRecruiters doit, lorsque cela est requis, répondre à toute demande d'information, et/ou accepter de soumettre ses locaux et ses opérations à des audits, y compris des inspections par le Client et/ou l'autorité de contrôle en matière de protection des données, dans chaque cas dans le but de prouver sa

conformité avec le présent Accord, à condition que : (v) le Client garantisse que toutes les informations obtenues ou générées dans le cadre d'une demande d'information, d'un audit ou d'une inspection sont strictement confidentielles (sauf en cas de divulgation à une autorité de contrôle en matière de protection des données ou si la loi applicable l'exige) ; (w) le Client fasse en sorte que toute demande d'information, tout audit ou toute inspection soit entrepris dans le cadre des heures normales de travail (à moins qu'un autre horaire ne soit imposé par une autorité de contrôle en matière de protection des données) avec une perturbation minimale de l'activité de SmartRecruiters, et en reconnaissant que cette demande d'information, cet audit ou cette inspection sera soumis à toutes les règles, procédures ou instructions raisonnables de SmartRecruiters dans le but de préserver la sécurité et la confidentialité ; (x) le Client fournisse à SmartRecruiters un préavis écrit d'au moins 15 jours concernant une demande d'information et/ou un audit ou une inspection (à moins que l'autorité de contrôle en matière de protection des données ne donne au Client un préavis inférieur à 15 jours, auquel cas le Client fournira à SmartRecruiters un préavis aussi long que cela est réalisable) ; (y) un maximum d'une demande d'information, d'un audit et/ou d'une inspection peut être faite par le Client sur une période de douze (12) mois, à moins qu'une demande d'information, un audit et/ou une inspection supplémentaire ne soit mandatée par écrit par une autorité de contrôle en matière de protection des données ; (z) le Client paiera les coûts raisonnables de SmartRecruiters pour toute assistance ou facilitation d'un audit ou d'une inspection ou de tout autre travail entrepris, à moins que ces coûts ne soient dus à une violation par SmartRecruiters de ses obligations en vertu du présent Accord. Si une requête d'audit n'est pas à la demande d'une autorité de contrôle en matière de protection des données, le Client convient que SmartRecruiters peut remplacer un audit requis par le Client par la fourniture des attestations, des rapports ou des extraits à jour provenant d'organismes indépendants (par exemple des rapports/certificats ISO 27001) qui vérifient et confirment que le traitement des Données à caractère personnel du Client est conforme aux mesures convenues dans les présentes.

- 7. Transfert international de données.** La présente section 7 prend effet lorsque SmartRecruiters ou ses Sous-traitants ultérieurs traitent les Données à caractère personnel du Client dans des pays situés en dehors de l'EEE ou de la Suisse ("**Transfert international**"). SmartRecruiters effectuera (et veillera à ce que ses Sous-traitants ultérieurs effectuent) un Transfert International uniquement : (i) dans le respect des termes des Clauses contractuelles types incorporées au présent Accord ; (ii) vers un pays ayant reçu une décision d'adéquation contraignante de la Commission européenne ou autrement en vertu des Législations relatives à la protection des données (collectivement, avec les Clauses contractuelles types, les "**Mécanismes de transfert international**"). Lorsque la présente section 7 est en vigueur, les termes du présent Accord seront interprétés en conjonction avec le Mécanisme de transfert international applicable. Aucune disposition du présent Accord ne doit être interprétée comme prévalant sur toute clause concurrente du Mécanisme de transfert international applicable.
- 8. Notifications.**
- 8.1.** Dans le cas où SmartRecruiters recevrait une demande, une assignation à comparaître ou une ordonnance d'un tribunal (y compris par le biais d'une obligation due à des dispositions légales ou à des injonctions officielles émanant d'autorités étatiques) exigeant que SmartRecruiters fournisse à une autorité toute Donnée à caractère personnel du Client traitée dans le cadre du présent Accord, SmartRecruiters tentera de rediriger l'autorité concernée pour qu'elle sollicite ces données directement auprès du Responsable du traitement des données, et en informera le Client sans délai excessif, à moins qu'il ne soit interdit à SmartRecruiters de le faire.
- 8.2.** Si les Données à caractère personnel du Client font l'objet d'une perquisition et d'une saisie, d'une ordonnance de saisie, d'une confiscation au cours d'une procédure de faillite ou d'insolvabilité, ou d'événements ou de mesures similaires par des tiers alors qu'elles sont sous le contrôle de SmartRecruiters, SmartRecruiters notifiera le Client d'une telle action sans délai excessif. SmartRecruiters doit, sans délai excessif, informer toutes les parties concernées dans un tel cas, que toute Donnée à caractère personnel affectée par cette action est la propriété exclusive et le domaine de responsabilité du Client, que les Données à caractère personnel sont à la disposition exclusive du Client, et que le Client est le Responsable du traitement des données.
- 9. California Consumer Privacy Act ("CCPA").** Si SmartRecruiters traite les Données à caractère personnel d'un résident de Californie au nom du Client, SmartRecruiters le fait en tant que prestataire de services en vertu du CCPA. SmartRecruiters s'engage à ne pas utiliser les Données à caractère personnel autrement qu'aux fins commerciales énoncées dans le Contrat principal. SmartRecruiters ne vendra pas les Données à caractère personnel du Client. SmartRecruiters déclare bien comprendre les restrictions de cet Accord et s'y conformer.

- 10. Divers.** Aucune modification du présent Accord ne sera valide et contraignante à moins d'être faite par écrit et seulement si cette modification indique expressément qu'elle s'applique aux dispositions du présent Accord. Ce qui précède s'applique également à toute renonciation ou modification de cette forme écrite obligatoire. En cas de divergence, le présent Accord prévaut sur les dispositions du Contrat principal. En cas de conflit, les dispositions des Clauses contractuelles types prévaudront sur celles du présent Accord. Cet Accord est régi par les lois du pays dans lequel le Client est établi.

Client	SmartRecruiters
Signature:	Signature: 
Nom du signataire :	Nom du signataire : Jerome Ternynck
Fonction:	Fonction: CEO
Date:	Date: 1 ^{er} août 2021

ANNEXE 1 AUX CLAUSES CONTRACTUELLES TYPES**MODULE 2 : transfert de responsable de traitement à sous-traitant**

Exportateur(s) de données : l'exportateur de données est (merci de bien vouloir lister brièvement les activités relatives au transfert des données)

- **Nom du Client :** le Client tel qu'identifié ci-avant et dans le Contrat principal.
- **Adresse du Client :** adresse telle qu'identifiée au sein du Contrat principal.
- **Activités en rapport avec les données transférées au titre des présentes clauses :** utilisation du logiciel SmartRecruiters aux fins d'attirer des candidats/talents.
- **Nom, fonction et coordonnées de la personne de contact :** tels qu'identifiés au sein du Contrat principal.
- **Rôle :** responsable du traitement.

Importateur de données : l'importateur de données est (merci de bien vouloir lister brièvement les activités relatives au transfert des données)

- **Importateur de données :** SmartRecruiters, Inc., un fournisseur de logiciel qui donne l'accès à ses clients à sa plateforme de recrutement en vue de l'acquisition de talents.
- **Adresse :** 225 Bush St, San Francisco, CA 94104.
- **Activités en rapport avec les données transférées au titre des présentes clauses :** fourniture de logiciel en vue de l'acquisition de talents tel qu'identifié au sein du Contrat principal entre l'Exportateur et l'Importateur de données.
- **Rôle :** sous-traitant.

Catégories de personnes concernées dont les données à caractère personnel sont transférées

- Les employés du Client utilisant le logiciel tel que décrit dans le Contrat principal.
- Les candidats utilisant le logiciel, tel que décrit dans le contrat principal, aux fins de postuler à des emplois.
- Les employés du Client qui ont postulé à des emplois en interne avec le Client.

Catégories de données à caractère personnel transférées

- Les données à caractère personnel (ex., nom, titre, historique de carrière, études, diplômes, intérêts personnels, photo, date de naissance, sexe, etc.)
- Les données organisationnelles du Client (ex., candidats internes ou les managers ou le personnel RH en charge des candidatures).
- Les données relatives aux procédures de candidature (ex., questions posées lors des entretiens, retour d'information, raison(s) de l'embauche, nombre de candidatures, numéro d'enregistrement de l'entreprise, candidatures internes ainsi que les remarques à l'attention ou provenant des candidats lors de l'utilisation des services d'emailing de l'application incluant les notifications).
- Les données en ligne (ex., adresse IP, identifiant de l'utilisateur, appareil mobile utilisé, système d'exploitation, fournisseur internet, date et heure de connexion et de déconnexion).
- Les données de communication (ex., adresse email, adresse privée et professionnelle, numéros de téléphone privés et professionnel, identifiant Skype, identifiants des réseaux sociaux, contenu des emails).
- Les données en ligne liées à l'utilisation de la Plateforme SmartRecruiters (e.g., identifiants des Cookies, empreintes digitales, adresses IP, historique des URL, etc.).
- Les données de connexion (ex., identifiant de l'utilisateur, mot de passe, date d'activation, date de création, nombre de connexions échouées, date de modification, type de statut, date de vérification et statut, information permettant de vérifier si et par qui les données ont été saisies dans la Plateforme SmartRecruiters ou si elles ont été modifiées ou supprimées).

Données sensibles transférées (le cas échéant) : si le traitement de données sensibles est nécessaire pour le compte d'un Client, ou si un candidat fournit volontairement des données à caractère personnel sensibles, alors, SmartRecruiters pourra procéder au traitement de données sensibles. Toutefois, les Applications SmartRecruiters ne sont pas conçues ou destinées à traiter des données sensibles.

Fréquence du transfert : en continu.

Finalité(s) du transfert et du traitement ultérieur des données :

- **Finalité(s) du transfert** : tel qu'identifié au sein du Contrat principal.
- **Traitement ultérieur des données** : collecte, enregistrement, organisation, structure, stockage, adaptation ou altération, récupération, consultation, utilisation, divulgation par transmission, dissémination ou mise à disposition d'une autre manière, alignement ou combinaison, restriction, effacement ou destruction.

Durée de conservation des données à caractère personnel : tel qu'indiqué dans le Contrat principal.

Pour les transferts à des sous-traitants ultérieurs:

- **Données concernées** : types de données à caractère personnel tels qu'identifiés ci-avant.
- **Nature du traitement** : collecte, enregistrement, organisation, structure, stockage, adaptation ou altération, récupération, consultation, utilisation, divulgation par transmission, dissémination ou mise à disposition d'une autre manière, alignement ou combinaison, restriction, effacement ou destruction.
- **Durée** : tel qu'indiqué dans le Contrat principal.

Autorité de Contrôle Compétente : l'Autorité de Contrôle Compétente est celle de l'État membre au sein duquel le responsable de traitement est établi.

ANNEXE 2 AUX CLAUSES CONTRACTUELLES TYPES

MESURES TECHNIQUES ET ORGANISATIONNELLES, Y COMPRIS LES MESURES TECHNIQUES ET ORGANISATIONNELLES VISANT À GARANTIR LA SÉCURITÉ DES DONNÉES

MODULE 2 : Transfert d'un responsable de traitement à un sous-traitant

1. Contrôle d'accès aux lieux et installations. Les mesures techniques et organisationnelles de vérification d'accès aux lieux et installations, particulièrement pour vérifier l'autorisation :

- Les paramètres de sécurité sont définis et utilisés pour protéger des espaces qui contiennent soit des informations sensibles ou critiques et des lieux de traitement des informations.
- La sécurité physique des bureaux, des salles et des installations est mise en place et appliquée.
- La protection physique contre les désastres naturels, les attaques malicieuses ou les accidents est mise en place et appliquée.
- L'équipement doit être protégé contre les coupures de courant et autres disruptions causées par des problèmes affectant les services en réseau.
- Pour les besoins de la conservation en lieu sûr ou de réutilisation des données, les équipements de stockage de média qui pourraient le cas échéant contenir des données à caractère personnel sont traitées comme s'ils contenaient de telles données.
- Du matériel mobile équipé des protections adéquates (cryptage).
- Une politique de rangement du bureau et de supports de stockage amovible et une politique de filtrage claire pour les centres de traitement des informations est adoptée.
- L'équipement est affecté à un site et protégé afin de réduire les risques provenant de menaces ou de catastrophes environnementales et les risques d'accès non autorisé.
- Il est garanti que seules des personnes autorisées peuvent accéder aux lieux et aux bâtiments de la société où les données du client sont stockées ou traitées.
- SmartRecruiters protège ses lieux et installations avec des systèmes d'alarme et un système de vidéosurveillance CCTV

2. Vérifications d'accès aux systèmes. Des mesures techniques (identifiant/mot de passe sécurisé) et organisationnelles (données de base de l'utilisateur) pour l'identification et l'authentification de l'utilisateur :

- Une politique de vérification d'accès est établie, documentée et révisée en fonction des exigences de l'entreprise et de la sécurité des informations.
- Il est fourni aux utilisateurs un accès au réseau et aux services en réseau qu'ils ont été autorisés à utiliser.
- L'allocation et l'utilisation de droits d'accès privilégiés est restreint et contrôlé.
- Un processus formel de provisionnement de l'accès de l'utilisateur est mis en place pour accorder ou révoquer des droits d'accès pour tous les types d'utilisateurs à tous les systèmes et services.
- L'allocation d'une authentification secrète à l'information est contrôlée au moyen d'un processus de gestion formel.
- Des mots de passe temporaires sont attribués aux utilisateurs d'une façon sécurisée. L'utilisation de messages électroniques ou de texte non protégé de tiers doit être évitée
- La politique concernant les mots de passe est connue et mise en œuvre par tous les employés de SmartRecruiters.
- Le système de gestion des mots de passe garantit des mots de passe de qualité.
- L'administrateur local et les mots de passes d'autres comptes privilégiés ne devront jamais apparaître décryptés sur le réseau.
- Il est mis un terme à des sessions inactives après une période définie d'inactivité.
- L'accès à l'information et aux fonctions d'application du système par les utilisateurs et les soutiens personnels sont restreints, conformément à la politique en place de vérification d'accès.
- L'accès au code source est protégé et restreint à un niveau proportionnel au niveau de risque.

3. Vérification d'accès aux données. Les exigences de définitions concernant la demande d'autorisation et des droits d'accès, et la surveillance des connexions et accès :

- Une politique de vérification d'accès aux données du Client est établie, documentée et révisée en fonction des exigences de l'entreprise et de la sécurité de l'information.
- SmartRecruiters met en œuvre une solution globale de cryptage pour les données en transit (y compris le réseau).
- Les stockages des bases de données sont cryptés.
- Les systèmes d'exploitation sont renforcés pour assurer les contrôles de sécurité requis.
- SmartRecruiters garantit que des procédures sont établies qui garantissent la rectitude, l'intégrité et la disponibilité des données de SmartRecruiters pendant toutes les étapes du traitement de données.

- Les média d'information sont détruites de façon sécurisée lorsqu'elles ne sont plus nécessaires, au moyen de procédures formelles.

4. Vérifications de communication de l'information. Mesures prises pour transporter, transférer et communiquer ou stocker les données sur le média d'information (manuel ou électronique) ou pour des vérifications subséquentes :

- L'accès aux systèmes qui conservent ou gèrent les données du Client est autorisé via des réseaux de connexions sécurisés.
- Les sites de connexion et les journaux d'informations sont protégés contre la falsification et l'accès non autorisé.
- Lorsque l'information est envoyée ou reçue, il est vérifié qu'elle n'est pas infectée par des virus et, si nécessaire, elle contient les détails de l'authentificateur et/ou de la vérification d'intégrité (signature électronique).

5. Vérifications de saisie. Mesures pour vérifier par la suite si les données ont été entrées, modifiées ou retirées (effacées), et par qui :

- Les événements liés à la sécurité de l'application sont notés au niveau de l'application.
- Les entrées du journal identifient l'individu dont l'action a été audité, l'individu affecté par l'action et le moment de l'action.
- La politique relative aux entrées prévoit que les entrées de registre ne doivent pas contenir d'informations sensibles.

6. Contrôle de qualité. Mesures (techniques/organisationnelles) de répartition des responsabilités entre SmartRecruiters (en qualité de sous-traitant) et le Client (en qualité de responsable de traitement des données) :

- La formulation sans ambiguïté de l'Accord sur le traitement des données entre SmartRecruiters et le Client avec des spécifications claires de SmartRecruiters et des obligations du Client.
- La sélection réfléchie de SmartRecruiters en tant que sous-traitant du Client.
- Le suivi de l'exécution de l'Accord de traitement des données à échéances régulières par SmartRecruiters et le Client.

7. Vérification des disponibilités. Mesures pour assurer la sécurité des données (physiques/logiques) :

- SmartRecruiters a mis au point un plan de reprise d'activité en cas de désastre qui contient toutes les procédures et informations de support requises pour la reprise de l'activité.
- Les procédures de SmartRecruiters sont établies qui garantissent la rectitude, l'intégrité et la disponibilité des données de SmartRecruiters à tous les stades du traitement de données.
- L'accès à des sauvegardes est restreint seulement au personnel autorisé.
- Les sauvegardes sont cryptées.
- Les fichiers téléchargés sur la plateforme sont scannés contre les virus.

8. Contrôle de ségrégation. Mesures à accomplir pour un traitement séparé (le stockage, la modification, la suppression, la transmission) des données pour différents motifs :

- Les environnements utilisés pour le test de développement et les besoins de la production sont physiquement séparés.
- L'utilisation de la production de données non-anonymes sur l'environnement de développement n'est pas autorisée.

Mesures Techniques et Organisationnelles de Sécurité du sous-traitant ultérieur

Les mesures techniques et organisationnelles du sous-traitant ultérieur visant à garantir la sécurité des données sont substantiellement similaires à celles identifiées ci-avant.

ANNEXE 3 AUX CLAUSES CONTRACTUELLES TYPES

MODULE 2 : Transfert d'un responsable de traitement à un sous-traitant

<https://www.smartrecruiters.com/legal/subprocessors>

Les sous-traitants ultérieurs de SmartRecruiters sont des fournisseurs de logiciels dont la situation est similaire et/ou sont des partenaires de mise en exécution d'activités de traitement similaires à celle de SmartRecruiters. Par conséquent, à l'exception des sous-traitants ultérieurs identifiés ci-après, les opérations de traitement des autres sous-traitants ultérieurs sont les mêmes que pour SmartRecruiters.

Sous-traitant ultérieur	Description du traitement ultérieur des données
Amazon Web Services Inc.	Stockage, suppression ou destruction.
SendGrid, Inc.	Collecte, enregistrement, organisation, structuration, stockage, adaptation ou altération, récupération, consultation, utilisation, divulgation par transmission, dissémination ou mise à disposition d'une autre manière, alignement ou combinaison, restriction, effacement ou destruction.
Textkernel BV	Collecte, enregistrement, organisation, structuration, stockage, adaptation ou altération, utilisation, divulgation par transmission, dissémination ou mise à disposition d'une autre manière, alignement ou combinaison.