

Accord de traitement des données

Version 2.1, en vigueur depuis le 5 octobre 2026

OutLine Digital Agency (entrepreneur individuel), Via Dalmazia 36, 76125 Trani (BT), Italie — TVA IT08978680729

Comment nous traitons, en tant que sous-traitant, les données personnelles de vos employés, de vos candidats et de vos autres collaborateurs que vous placez dans Omega People : ce que nous pouvons en faire, ce que nous ne pouvons pas en faire, et comment les transferts sont encadrés.

Références juridiques

Règlement (UE) 2016/679 (RGPD), art. 28 et chapitre V · Décision d'exécution (UE) 2021/914 de la Commission (clauses contractuelles types) · UK GDPR et International Data Transfer Addendum aux clauses contractuelles types de l'UE · Loi fédérale sur la protection des données (LPD), art. 9 et 16 · California Consumer Privacy Act (CCPA) et autres lois des États américains sur la protection de la vie privée, le cas échéant · Canada : LPRPDE ; Québec : Loi sur la protection des renseignements personnels dans le secteur privé, art. 17 et 18.3 ; Alberta et Colombie-Britannique : Personal Information Protection Acts · Australie : Privacy Act 1988, Australian Privacy Principles 8 et 11 et partie IIIC (violations de données à notifier) · Nouvelle-Zélande : Privacy Act 2020, art. 11 et principes 5 et 12 (information privacy principles)

Préambule

Le présent Accord complète les Conditions d'utilisation (<https://people.omegasuiteapp.com/legal/terms>) et régit le traitement des données personnelles que OutLine Digital Agency (**le Sous-traitant**) effectue pour le compte du client (**le Responsable du traitement**) dans le cadre de la fourniture d'Omega People.

Il constitue le contrat exigé par l'art. 28(3) du RGPD et, lorsque le Responsable du traitement y est soumis, par l'art. 28 du UK GDPR, l'art. 9 de la loi fédérale suisse sur la protection des données, l'article 18.3 de la Loi québécoise sur la protection des renseignements personnels dans le secteur privé et les lois des États américains sur la protection de la vie privée qui exigent un contrat écrit avec un fournisseur de services ou un sous-traitant. Il est conclu lorsque le Responsable du traitement l'accepte à l'ouverture de son premier espace de travail et reste en vigueur aussi longtemps que le Sous-traitant traite des données personnelles pour son compte.

Sous-traitant	OutLine Digital Agency (entrepreneur individuel), Via Dalmazia 36, 76125 Trani (BT), Italie — TVA IT08978680729
---------------	---

Responsable du traitement	Le client, tel qu'identifié dans le compte et dans les données de l'entreprise saisies dans l'application.
---------------------------	--

Contact pour la protection des données	amministrazione@outlinedigital.it
--	-----------------------------------

Les termes tels que « données personnelles », « traitement », « responsable du traitement », « sous-traitant » et « violation de données personnelles » ont le sens que leur donne le RGPD ; lorsqu'une autre loi s'applique, ils incluent les termes équivalents de cette loi (par exemple « business » et « service provider » au sens du CCPA).

Qui décide de quoi

Le Responsable du traitement est l'employeur. Il décide quelles données collecter sur ses employés, ses candidats et ses autres collaborateurs, à quelles fins, sur quelle base juridique et pour combien de temps, et c'est lui qui les en informe (par son propre avis de confidentialité destiné au personnel). Le Sous-traitant fournit l'outil et ne prend aucune de ces décisions. Cela signifie que le Sous-traitant ne peut pas supprimer des données à la demande d'une personne, et que le Responsable du traitement ne peut pas faire porter au Sous-traitant le choix d'avoir collecté des données qu'il n'aurait pas dû collecter.

1. Traitement sur instructions documentées

1. Le Sous-traitant ne traite les données personnelles **que sur instructions documentées du Responsable du traitement**. Constituent de telles instructions : le présent Accord, les Conditions d'utilisation, la documentation du service et les réglages que le Responsable du traitement configure dans l'application (utilisateurs, rôles et autorisations, modules qu'il active, règles de pointage et de localisation, pages publiques, intégrations, durées de conservation).
2. Le Sous-traitant ne traite pas les données à ses propres fins, ne les communique pas à des tiers, ne les utilise pas à des fins d'analyse commerciale ni pour entraîner des systèmes d'intelligence artificielle.
3. Si une obligation légale impose au Sous-traitant un traitement supplémentaire, il en informe le Responsable du traitement avant d'y procéder, sauf si la loi l'interdit pour des motifs importants d'intérêt public.
4. Le Sous-traitant informe immédiatement le Responsable du traitement si, selon lui, une instruction enfreint le droit de la protection des données.

2. Confidentialité des personnes autorisées

Le Sous-traitant veille à ce que les personnes autorisées à traiter les données — personnel et collaborateurs externes — soient tenues à une obligation de confidentialité qui survit à la fin de leur engagement, reçoivent des instructions et n'aient accès qu'aux données nécessaires à leur tâche.

Le personnel de l'assistance n'accède aux espaces de travail des clients qu'au moyen de l'**accès temporaire journalisé** décrit à la section 8.

3. Mesures de sécurité

Le Sous-traitant met en œuvre les mesures techniques et organisationnelles décrites à l'**Annexe B** et sur la page Mesures de sécurité (<https://people.omegasuiteapp.com/legal/security>), qui font partie du présent Accord.

Ces mesures peuvent être mises à jour au fil du temps à condition que le niveau de sécurité ne soit pas réduit. Les modifications importantes sont notifiées au Responsable du traitement avec le même préavis que pour les sous-traitants ultérieurs.

4. Sous-traitants ultérieurs

Le Responsable du traitement accorde au Sous-traitant une **autorisation générale** de recourir à d'autres sous-traitants, aux conditions suivantes.

1. La liste à jour est publiée sur la page Sous-traitants ultérieurs (<https://people.omegasuiteapp.com/legal/subprocessors>).
2. Chaque sous-traitant ultérieur est tenu par contrat à des obligations de protection des données équivalentes à celles du présent Accord ; le Sous-traitant répond de leur exécution comme de la sienne.
3. L'ajout ou le remplacement d'un sous-traitant ultérieur est notifié au Responsable du traitement au moins **30 jours** à l'avance, par e-mail et de manière visible dans l'application.
4. Dans ce délai, le Responsable du traitement peut s'y opposer pour des motifs raisonnables et documentés liés à la protection des données. En cas d'opposition, les parties recherchent de bonne foi une solution de rechange ; si aucune n'est praticable, le Responsable du traitement peut résilier sans pénalité avec effet à la date du changement.

Sous-traitant ultérieur	Activité	Pays
IONOS SE	Serveurs et stockage : héberge l'application, les bases de données des espaces de travail, les fichiers téléversés (documents du personnel, fiches de paie, justificatifs, pièces jointes) et les sauvegardes.	Allemagne
Aruba S.p.A.	Relaie les e-mails sortants du service : invitations aux employés et aux membres de l'équipe, réinitialisations de mot de passe, messages aux candidats, e-mails envoyés par les règles d'automatisation que le client configure, et e-mails relatifs à l'abonnement. Les messages contiennent le nom et l'adresse e-mail du destinataire ainsi que le contenu du message.	Italie
Stripe Payments Europe, Limited	Encaisse les paiements de l'abonnement et émet les reçus. Ne traite que les données de facturation de l'abonné (raison sociale, adresse, numéro de TVA, e-mail de facturation, données de carte — qui ne transitent jamais par nos serveurs). Il reçoit en outre le nom de l'espace de travail, l'adresse e-mail de connexion de son propriétaire et nos numéros de référence internes. Aucun accès aux données des espaces de travail.	Irlande

La version qui fait foi est celle tenue à jour sur [/legal/subprocessors](https://people.omegasuiteapp.com/legal/subprocessors) (<https://people.omegasuiteapp.com/legal/subprocessors>) : ce tableau en est une copie de courtoisie à la date de génération du présent document.

Les services que vous connectez ne sont pas nos sous-traitants ultérieurs

Si le Responsable du traitement connecte Omega People à d'autres services — un prestataire de signature électronique (Yousign) avec son propre compte et sa propre clé d'API, un fournisseur d'intelligence artificielle avec sa propre clé, ou des webhooks appelés par ses règles d'automatisation —, les données qui leur sont envoyées le sont sur instruction du Responsable du traitement et en vertu de son contrat avec ce fournisseur. Ces fournisseurs sont les sous-traitants du Responsable du traitement, et non des sous-traitants ultérieurs du Sous-traitant. Dans l'application, sous **Paramètres -> Confidentialité et conformité**, le Responsable du traitement trouve son registre des activités de traitement déjà rempli, la liste des services qu'il a connectés et les avis de confidentialité destinés à ses employés et à ses candidats.

5. Assistance pour les demandes des personnes concernées

L'application fournit au Responsable du traitement les outils pour répondre lui-même aux demandes de ses employés, de ses anciens employés et de ses candidats, sans attendre personne : recherche, export de l'ensemble des données détenues sur un employé, rectification, suppression et journal des modifications des données du personnel. Les employés disposant d'un accès à l'espace personnel peuvent consulter directement leurs présences, leurs congés, leurs horaires, leurs documents et leurs fiches de paie.

Si un employé, un candidat ou une autre personne concernée s'adresse directement au Sous-traitant, celui-ci **ne donne pas suite** à la demande et la transmet sans délai au Responsable du traitement, en indiquant à la personne que le responsable du traitement est son employeur (ou l'entreprise auprès de laquelle elle a postulé).

Lorsque les outils de l'application ne suffisent pas, le Sous-traitant fournit une assistance technique raisonnable, à ses propres frais si le besoin découle d'un dysfonctionnement.

6. Violations de données personnelles

1. Le Sous-traitant notifie au Responsable du traitement **dans les meilleurs délais et en tout état de cause dans les 48 heures** après en avoir pris connaissance toute violation de données personnelles touchant les données traitées pour son compte, et s'efforce de le faire dans les 24 heures. Une première notification est adressée même si toutes les informations ne sont pas encore disponibles ; les autres suivent par étapes, à mesure qu'elles sont connues.
2. La notification décrit la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements concernés, les conséquences probables et les mesures prises ou proposées, afin que le Responsable du traitement puisse évaluer s'il doit informer les autorités compétentes et les personnes concernées, et dans quel délai, selon la loi qui lui est applicable (par exemple 72 heures selon le RGPD et le UK GDPR, ou « dans les meilleurs délais » ou « dès que possible » selon la LPD suisse, la LPRPDE et les régimes australien et néo-zélandais).
3. Le Sous-traitant documente chaque violation et apporte au Responsable du traitement la coopération nécessaire pour remplir ses obligations envers les autorités et les personnes concernées.
4. La notification aux autorités et aux personnes concernées reste de la responsabilité du Responsable du traitement : le Sous-traitant n'y procède pas à sa place.

7. Analyses d'impact et consultation préalable

Compte tenu de la nature du traitement et des informations dont il dispose, le Sous-traitant aide le Responsable du traitement à réaliser les analyses d'impact relatives à la protection des données et toute consultation préalable d'une autorité, en fournissant la documentation technique sur l'architecture, les mesures de sécurité et les flux de données du service.

Quand une analyse d'impact est utile

Un logiciel RH traite des données concernant des personnes dont la subsistance dépend du Responsable du traitement, et plusieurs fonctionnalités d'Omega People méritent une attention particulière : le **pointage avec géolocalisation**, qui enregistre où se trouve un employé lorsqu'il pointe à l'entrée ou à la sortie ; les **données de santé** contenues dans les arrêts de travail, les dossiers de visites médicales et les déclarations d'accident ; les **entretiens d'évaluation et les dossiers disciplinaires** ; le **canal d'alerte** ; et toute utilisation des **fonctionnalités d'IA** sur les données des employés. Dans de nombreux pays, ces traitements relèvent aussi du droit du travail et des règles sur la surveillance au travail (information préalable du personnel, consultation des représentants du personnel ou d'une commission du personnel). L'application le signale sous **Paramètres -> Confidentialité et conformité**, mais l'analyse est réalisée par le Responsable du traitement.

8. Accès de l'assistance à l'espace de travail

- Il n'a lieu qu'à la demande du Responsable du traitement, ou pour une intervention technique nécessaire au maintien du service ou à la correction d'un dysfonctionnement.
- Il utilise un **accès temporaire dédié** créé dans l'espace de travail, qui expire automatiquement au bout de **15 minutes** : il n'utilise ni ne connaît les identifiants des utilisateurs du Responsable du traitement.
- Tant qu'il est actif, cet accès dispose des droits d'un administrateur de l'espace de travail : c'est ce qui permet de voir un problème tel que le Responsable du traitement le voit. La personne qui l'utilise est tenue à la confidentialité (section 2) et ne consulte que ce que la demande exige.
- Il est **consigné et visible par le Responsable du traitement** : chaque accès est enregistré avec son auteur, sa date, sa durée et son motif ; le titulaire du compte du Responsable du traitement reçoit un e-mail dès son ouverture, et ses propriétaires et administrateurs peuvent consulter le journal à tout moment dans Paramètres -> Accès du support. Pendant l'accès, les exports, les téléchargements de fichiers et les modifications de mots de passe, d'adresses de connexion et de clés d'API sont bloqués, et toute tentative figure dans le journal.

9. Audits et démonstration de la conformité

Le Sous-traitant met à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect du présent Accord et permet la réalisation d'audits, y compris d'inspections, par le Responsable du traitement ou par un auditeur qu'il mandate.

1. Les audits requièrent un préavis d'au moins 15 jours, ont lieu pendant les heures ouvrées et ne doivent compromettre ni la continuité du service ni la confidentialité des données des autres clients.
2. **Un audit par année civile** est autorisé, ainsi que des audits supplémentaires après une violation de données personnelles ou à la demande motivée d'une autorité de contrôle.
3. L'auditeur du Responsable du traitement ne doit pas être un concurrent du Sous-traitant et doit signer un engagement de confidentialité.
4. Le coût des audits supplémentaires demandés par le Responsable du traitement est à sa charge, sauf si l'audit révèle un manquement du Sous-traitant.

Le Sous-traitant tient un registre des traitements qu'il effectue pour le compte du Responsable du traitement (art. 30, paragraphe 2, du RGPD) et coopère, sur demande, avec les autorités de contrôle dans l'exécution de leurs missions.

10. Transferts internationaux

Le Sous-traitant traite les données au sein de l'Espace économique européen : l'infrastructure est hébergée par IONOS SE en Allemagne, et ses sous-traitants ultérieurs se trouvent dans l'Union européenne. **Il ne transfère pas les données vers des pays tiers**, si ce n'est pour les mettre à la disposition du Responsable du traitement et de ses utilisateurs, où qu'ils se trouvent.

1. **De l'UE vers le Responsable du traitement.** Lorsque le RGPD s'applique à la mise à disposition de données à un Responsable du traitement qui n'est pas couvert, pour ces données, par une décision d'adéquation de l'UE, les parties conviennent des clauses contractuelles types de l'UE (décision d'exécution (UE) 2021/914 de la Commission), **module 4** (sous-traitant à responsable du traitement), qui sont intégrées au présent Accord par renvoi. L'article 23 des Conditions d'utilisation détermine le droit applicable et les tribunaux compétents ; les détails du traitement sont ceux de l'Annexe A. Pour ces clauses : la clause d'adhésion (clause 7) ne s'applique pas ; les clauses 14 et 15 ne s'appliquent que si le Sous-traitant combine les données reçues du Responsable du traitement avec des données personnelles qu'il a collectées dans l'Union européenne, ce qu'il ne fait pas ; elles sont régies par le droit italien (clause 17) et les tribunaux italiens sont compétents (clause 18) ; les parties sont celles désignées dans le préambule et l'annexe I correspond à l'Annexe A du présent Accord. La mise à disposition de données à un Responsable du traitement situé au Royaume-Uni, en Suisse ou en Nouvelle-Zélande repose sur les décisions d'adéquation de la Commission européenne relatives à ces pays, tant qu'elles restent en vigueur ; il en va de même pour un Responsable du traitement situé au Canada dans la mesure où la LPRPDE s'applique aux données concernées, et pour un Responsable du traitement situé aux États-Unis dans la mesure où il est certifié, pour ces données, au titre du cadre de protection des données UE-États-Unis (EU-U.S. Data Privacy Framework). Dans tous les autres cas, le module 4 s'applique.
2. **Royaume-Uni.** Pour un Responsable du traitement soumis au UK GDPR, les transferts vers le Sous-traitant reposent sur les règlements d'adéquation du Royaume-Uni concernant l'Espace économique européen. S'ils cessaient de s'appliquer, les parties conviennent des clauses contractuelles types de l'UE (module 2) accompagnées de l'**International Data Transfer Addendum** britannique publié par l'Information Commissioner, intégrés par renvoi.
3. **Suisse.** Pour un Responsable du traitement soumis à la LPD suisse, les transferts vers le Sous-traitant reposent sur la reconnaissance, par le Conseil fédéral, du caractère adéquat de la protection dans les pays concernés. Si elle cessait de s'appliquer, les parties conviennent des clauses contractuelles types de l'UE avec les adaptations requises pour la Suisse : le PFPDT est l'autorité de contrôle compétente pour les transferts relevant du droit suisse, et la notion d'« État membre » inclut la Suisse pour l'exercice des droits des personnes concernées.
4. Si un transfert hors de l'EEE devenait un jour nécessaire pour un sous-traitant ultérieur, le Sous-traitant le notifie conformément à la section 4 et ne l'effectue qu'avec l'une des garanties du chapitre V du RGPD, en l'indiquant dans la liste des sous-traitants ultérieurs.

5. Les transferts résultant de services connectés par le Responsable du traitement (par exemple un fournisseur d'IA ou un prestataire de signature électronique établi hors de l'EEE) sont effectués sous sa responsabilité.
6. **Demandes des autorités.** Si un tribunal ou une autorité publique demande au Sous-traitant l'accès aux données du Responsable du traitement, le Sous-traitant vérifie la légalité de la demande, la conteste lorsqu'il existe des motifs raisonnables de le faire, ne communique que ce qui est strictement requis et, sauf interdiction légale, en informe préalablement le Responsable du traitement.

11. États-Unis : conditions applicables aux fournisseurs de services

Lorsque le Responsable du traitement est un « business » soumis au California Consumer Privacy Act (CCPA) ou un « controller » soumis à une autre loi d'un État américain sur la protection de la vie privée, le Sous-traitant agit en qualité de **fournisseur de services** (*service provider*, ou sous-traitant). Le Responsable du traitement ne lui communique les renseignements personnels que pour la finalité commerciale limitée et déterminée consistant à fournir le service décrit à l'Annexe A, et le Sous-traitant :

- ne vend ni ne partage les renseignements personnels, et ne les utilise pas à des fins de publicité comportementale intercontextuelle ou ciblée ;
- ne les conserve, ne les utilise ni ne les communique à aucune autre fin — y compris commerciale — que la fourniture du service prévue au contrat, ni en dehors de la relation d'affaires directe avec le Responsable du traitement ;
- ne les combine pas avec des renseignements personnels qu'il reçoit d'une autre source ou qu'il recueille dans ses propres relations avec la personne concernée, sauf dans la mesure où ces lois le permettent à un fournisseur de services ;
- respecte les obligations que ces lois imposent aux fournisseurs de services et aux sous-traitants, et assure aux renseignements personnels le niveau de protection qu'elles exigent, y compris les mesures de sécurité de l'Annexe B ;
- informe le Responsable du traitement **dans un délai de cinq jours ouvrés** s'il constate qu'il n'est plus en mesure de respecter ces obligations ;
- permet au Responsable du traitement de prendre des mesures raisonnables et appropriées pour s'assurer que les renseignements sont utilisés conformément aux obligations de ce dernier (sections 3 et 9) et, après notification, pour faire cesser et corriger toute utilisation non autorisée ;
- aide le Responsable du traitement à répondre aux demandes des personnes concernées (section 5) et impose à ses sous-traitants ultérieurs, par contrat écrit, les mêmes obligations (section 4) ;
- préserve la confidentialité des renseignements et les supprime ou les restitue à la fin du service (section 13).

Ni renseignements de santé protégés, ni identifiants biométriques. Le Sous-traitant n'est pas un « business associate » au sens de la loi HIPAA et n'a signé aucun accord à ce titre (*business associate agreement*) : le service ne doit pas servir à conserver les renseignements de santé protégés (*protected health information*) d'un régime d'assurance maladie ou d'un prestataire de soins. Les documents qu'un employeur tient en sa qualité d'employeur — un certificat d'arrêt de travail, une attestation d'aptitude — ne sont pas des renseignements de santé protégés ; il appartient au Responsable du traitement d'appliquer, au moyen des droits d'accès du service, les règles de confidentialité des dossiers médicaux des salariés (par exemple celles de l'ADA, de la FMLA et de la GINA). Le service ne recueille ni empreintes digitales, ni scans de la géométrie du visage ou de la main, ni empreintes vocales, ni autres identifiants biométriques — l'appareil photo ne sert qu'à lire un code QR et à photographier des documents —, et le Responsable du traitement ne doit pas en téléverser.

Incidents de sécurité. La section 6 couvre également la notification que les lois des États américains exigent d'une entreprise qui conserve des données pour le compte de leur propriétaire.

12. Canada, Australie et Nouvelle-Zélande

Pour un Responsable du traitement soumis à l'une des lois ci-dessous, le Sous-traitant ne traite les données que pour fournir le service, les protège au moyen des garanties décrites dans le présent Accord et assiste le Responsable du traitement comme décrit aux sections 5 à 9. En outre :

Canada (LPRPDE et lois sur la protection des renseignements personnels de l'Alberta et de la Colombie-Britannique)

Le Responsable du traitement demeure responsable des renseignements personnels qu'il confie au Sous-traitant aux fins de traitement. Le Sous-traitant ne les utilise qu'aux fins du service, leur assure une protection comparable à celle que le Responsable du traitement doit offrir, et informe celui-ci, conformément à la section 6, de toute atteinte aux mesures de sécurité, afin qu'il puisse évaluer s'il existe un risque réel de préjudice grave, la déclarer et tenir son registre des atteintes. **Les renseignements sont conservés et traités hors du Canada** — dans les pays indiqués dans la liste des sous-traitants ultérieurs (<https://people.omegasuiteapp.com/legal/subprocessors>) —, où ils sont soumis au droit de ces pays et peuvent être accessibles à leurs tribunaux et autorités en vertu de ce droit ; il incombe au Responsable du traitement d'en informer les personnes concernées et de nommer ces pays lorsque la loi l'exige (comme en Alberta).

Québec

Le présent Accord constitue le contrat écrit exigé par l'article 18.3 de la Loi sur la protection des renseignements personnels dans le secteur privé. Le Sous-traitant n'utilise les renseignements personnels que pour l'exécution du service ; applique les mesures de l'Annexe B pour en protéger le caractère confidentiel ; ne les conserve pas après l'expiration du contrat (section 13) ; avise **sans délai** le responsable de la protection des renseignements personnels du Responsable du traitement **de toute violation ou tentative de violation**, par toute personne, de l'une des obligations relatives à la confidentialité des renseignements ; et permet à ce responsable d'effectuer toute vérification relative à cette confidentialité (section 9). Avant de communiquer des renseignements à l'extérieur du Québec, le Responsable du traitement doit procéder à l'évaluation des facteurs relatifs à la vie privée prévue à l'article 17 de cette loi : le Sous-traitant lui fournit les informations nécessaires — lieu de conservation des données, identité des sous-traitants ultérieurs, mesures de sécurité et cadre juridique applicable dans l'Union européenne.

Australie

Le Responsable du traitement conserve le contrôle effectif des renseignements personnels : il décide qui peut y accéder et peut à tout moment y accéder, les modifier, les récupérer et les supprimer ; le Sous-traitant ne les traite que pour les conserver et les mettre à la disposition du Responsable du traitement et de ses utilisateurs, et impose les mêmes obligations à ses sous-traitants ultérieurs. Sur cette base, la fourniture des renseignements au Sous-traitant a vocation à constituer une *utilisation* (use) par le Responsable du traitement et non une *communication* (disclosure) au sens de l'Australian Privacy Principle 8 ; il appartient au Responsable du traitement d'apprécier si tel est le cas. Si le Sous-traitant a des motifs raisonnables de soupçonner un accès non autorisé aux renseignements, leur communication non autorisée ou leur perte, il en avise le Responsable du traitement conformément à la section 6, afin que celui-ci puisse achever son évaluation dans les 30 jours prévus par le régime de notification des violations de données (Notifiable Data Breaches scheme) ; les parties conviennent que toute notification à l'Office of the Australian Information Commissioner et aux personnes concernées est effectuée par le Responsable du traitement.

Le Sous-traitant détient les renseignements personnels en qualité de mandataire (agent) du Responsable du traitement, à des fins de conservation et de traitement, et ne les utilise ni ne les communique pour ses propres finalités : en vertu de l'article 11 du Privacy Act 2020, les renseignements sont réputés détenus par le Responsable du traitement, qui en demeure responsable, et leur envoi au Sous-traitant ne constitue pas une communication hors de Nouvelle-Zélande au sens du principe 12 (information privacy principle 12). Le Sous-traitant notifie les atteintes à la vie privée conformément à la section 6, afin que le Responsable du traitement puisse aviser le Privacy Commissioner et les personnes touchées dès que possible lorsqu'un préjudice grave est probable.

13. Ce qui se passe à la fin

1. Le Responsable du traitement peut exporter lui-même les données, dans des formats ouverts, pendant toute la durée de la relation.
2. À la fin du contrat, l'espace de travail reste accessible en lecture seule pendant **30 jours** afin de permettre l'export.
3. À l'issue de ce délai, le Sous-traitant **supprime** les données personnelles dans les meilleurs délais, et au plus tard dans les 30 jours qui suivent ; les copies figurant dans les sauvegardes cessent d'exister au fil de la rotation, au plus tard environ trois mois après la suppression. Les données ne sont conservées plus longtemps que si le droit de l'Union ou d'un État membre l'exige.
4. Sur demande, le Sous-traitant confirme la suppression par écrit.
5. La conservation légale des documents relatifs à l'emploi, à la paie, au temps de travail et à la santé et à la sécurité au travail est une obligation du Responsable du traitement en tant qu'employeur : le Responsable du traitement exporte ce qu'il doit conserver avant la clôture de la période d'export. Le Sous-traitant ne tient pas lieu d'archive du Responsable du traitement après la fin du contrat.

14. Ordre de priorité

En cas de conflit, les clauses contractuelles types (lorsqu'elles s'appliquent) prévalent sur le présent Accord, et le présent Accord prévaut sur les Conditions d'utilisation pour ce qui concerne les données personnelles. La responsabilité est régie par les Conditions d'utilisation.

Annexe A — Détails du traitement

Objet	Fourniture d'un service en ligne de gestion des ressources humaines : dossiers du personnel, temps et présences, horaires, congés et absences, documents et signature électronique, notes de frais, préparation de la paie, recrutement, formation, santé et sécurité au travail, entretiens d'évaluation, canal d'alerte, communication interne.
Durée	La durée du contrat de service, plus la période d'export de 30 jours.

Conservation pendant la durée du contrat	Les données sont conservées aussi longtemps que le Responsable du traitement les conserve dans l'espace de travail. Le Responsable du traitement décide des durées de conservation et supprime lui-même les enregistrements (par exemple ceux des anciens employés, des candidats non retenus, des signalements clos du canal d'alerte, pour lesquels un nettoyage automatique à l'issue d'une durée choisie par le Responsable du traitement peut être activé). Pendant la durée du contrat, le Sous-traitant ne supprime de sa propre initiative des données de l'espace de travail que dans les cas prévus par l'application et que le Responsable du traitement peut régler : les candidatures non retenues sont supprimées à l'issue de la durée fixée dans les paramètres de recrutement (12 mois par défaut), et les enregistrements d'appareils mobiles inutilisés depuis 180 jours sont retirés.
Nature et finalité	Collecte, enregistrement, organisation, structuration, conservation, extraction, consultation, transmission aux services configurés par le Responsable du traitement, effacement — dans le seul but de faire fonctionner l'application telle que le Responsable du traitement l'a configurée.
Fréquence	Continue, tant que le service est utilisé.

Catégories de personnes concernées — selon l'usage que le Responsable du traitement fait du service :

- employés, travailleurs, apprentis, stagiaires et autres membres du personnel du Responsable du traitement, y compris les **anciens membres du personnel** dont le Responsable du traitement conserve les dossiers ;
- **candidats à un emploi** qui postulent par la page carrières du Responsable du traitement ou que le Responsable du traitement saisit ;
- prestataires, travailleurs intérimaires et autres personnes que le Responsable du traitement gère dans l'espace de travail ;
- propriétaires, administrateurs et responsables du Responsable du traitement qui utilisent le service ;
- **personnes à contacter en cas d'urgence** indiquées par les employés, et membres de la famille lorsque le Responsable du traitement les enregistre (par exemple dans les justificatifs d'un congé pour raisons familiales) ;
- personnes qui envoient un signalement par le canal d'alerte (qui peuvent rester anonymes) et personnes mentionnées dans un signalement ;
- autres personnes mentionnées dans les documents, messages, notes de frais, déclarations d'accident et notes.

Catégories de données personnelles :

Catégorie	Exemples	Où elles apparaissent
Données d'identification et de contact	nom, date et lieu de naissance, genre, adresse du domicile, adresse e-mail, numéro de téléphone, personne à contacter en cas d'urgence	Fiches employé, espace personnel
Identifiants officiels	numéro d'assurance nationale, de sécurité sociale ou d'identification fiscale, numéro et date d'expiration de la pièce d'identité	Fiches employé, intégration
Données relatives à l'emploi	poste, service, site, responsable, type et dates du contrat, période d'essai, préavis, date et motif de fin de contrat, compétences, matériel attribué	Fiches employé, contrats, organigramme, matériel

Données de rémunération et données financières	salaire et éléments de rémunération, coordonnées bancaires, frais et remboursements, avantages, fiches de paie téléversées par le Responsable du traitement	Préparation de la paie, notes de frais, avantages, documents
Données de temps de travail	heures de pointage d'entrée et de sortie, feuilles de temps, horaires, disponibilités, heures supplémentaires, astreintes, heures par projet	Présences, planning des horaires, projets
Données de localisation	la position de l'appareil au moment du pointage d'entrée ou de sortie (coordonnées, précision, présence ou non dans la zone définie pour le site), uniquement si le Responsable du traitement active la localisation pour les pointages. Il n'y a aucun suivi continu.	Présences
Données de congés et d'absences	type, dates et motif des absences, soldes, justificatifs	Congés et absences
Données de performance et de développement	entretiens d'évaluation, auto-évaluations, objectifs, formations suivies et attestations, réponses aux sondages (anonymes lorsque le Responsable du traitement les définit ainsi)	Performance, formation, sondages
Données disciplinaires	griefs, réponse de l'employé, issue	Fiches employé
Données des candidats	nom, coordonnées, CV et message d'accompagnement, étape de la sélection, notes et évaluation	Recrutement, page carrières
Signalements du canal d'alerte	contenu du signalement et des messages de suivi, pièces jointes, noms des personnes concernées. L'auteur du signalement n'est pas identifié par le système : l'accès au suivi se fait au moyen d'un code affiché une seule fois, dont seule une empreinte est conservée.	Canal d'alerte
Documents et texte libre	contrats, documents signés, certificats, courriers, messages de la messagerie d'équipe, annonces et commentaires, fichiers de l'espace de stockage partagé	Documents, messagerie, annonces, stockage
Données d'utilisation et de sécurité	connexions, sessions, appareils enregistrés pour l'application mobile ou la borne, journal des modifications des données du personnel	Journaux d'activité et d'audit
Catégories particulières (art. 9 du RGPD) et données sensibles similaires	données de santé (arrêts de travail et motifs d'absence, visites de médecine du travail avec leur résultat et leurs restrictions, accidents du travail et lésions) ; données susceptibles de révéler l' appartenance syndicale (absences pour activité syndicale ou pour grève) ; toute autre donnée sensible — par exemple sur la religion, l'origine ethnique, le handicap ou les antécédents judiciaires — que le Responsable du traitement choisit d'enregistrer ou qui figure dans les documents qu'il téléverse	Congés et absences, santé et sécurité au travail, documents, préparation de la paie

Catégories particulières : le Responsable du traitement décide, et en répond

Un système RH contient par nature des catégories particulières de données. C'est le Responsable du traitement qui décide de les enregistrer ou non, sur quelle base juridique (par exemple les obligations de l'employeur en vertu du droit du travail, de la sécurité sociale et de la santé et de la sécurité au travail), qui peut les voir et pendant combien de temps ; il lui incombe de les limiter au minimum nécessaire : enregistrer qu'un employé est inapte ou absent, et non le diagnostic, chaque fois que la loi n'en exige pas davantage. Le Sous-traitant ne demande pas ces données, ne les lit pas et ne les utilise à aucune autre fin que leur conservation et leur affichage aux utilisateurs que le Responsable du traitement a autorisés.

Annexe B — Mesures de sécurité

Les mesures techniques et organisationnelles adoptées par le Sous-traitant sont décrites en détail sur la page Mesures de sécurité (<https://people.omegasuiteapp.com/legal/security>), qui fait partie du présent Accord. En résumé : une base de données distincte pour chaque espace de travail, chiffrement du trafic en transit, chiffrement au repos des identifiants des services connectés et de la clé d'API d'un fournisseur d'IA, mots de passe conservés uniquement sous forme de hachage, contrôle d'accès fondé sur les rôles et les autorisations, les signalements du canal d'alerte étant réservés aux référents désignés par le propriétaire du compte du Responsable du traitement et chaque accès étant journalisé, journal en ajout seul des modifications des données du personnel, accès de l'assistance temporaire et journalisé, sauvegardes quotidiennes des bases de données, journalisation des événements.

Le texte intégral à jour est toujours disponible à l'adresse <https://people.omegasuiteapp.com/legal/dpa?lang=fr>. Pour toute question : amministrazione@outlinedigital.it.