CLAUSES CONTRACTUELLES DE SOUS-TRAITANCE DE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL - ARTICLE 28 - (Formant DATA PROCESSING AGREEMENT ou “DPA”)

Conformément au règlement 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 (RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 abrogeant la directive 95/46/CE - Règlement général sur la protection des données), les parties sont convenues de ce qui suit.

1. OBJET

Dans le cadre de l'exécution des Services, le Fournisseur aura accès ou sera fourni par le Client, ses sociétés affiliées, ses filiales et sa société holding, avec certaines Données à caractère personnel que le Fournisseur devra traiter pour le compte du Client, comme spécifié dans la Clause 4. Afin de s'assurer que toutes les Données à caractère personnel sont à tout moment traitées conformément aux lois sur la protection des données, les Parties ont convenu d'exécuter le présent Accord sur le traitement des données, y compris ses annexes (le "DPA").

Le présent DPA fait partie de l'accord et en reprend les termes. Dans la mesure où les conditions contenues dans le présent DPA sont contraires ou incompatibles avec les conditions relatives au même objet contenues dans l'accord, les conditions contenues dans le présent DPA prévalent. Sauf modification ci-dessous, les termes de l'accord restent pleinement en vigueur.

2. DÉFINITIONS

Les termes en majuscules utilisés mais non définis dans le présent DPA ont la signification qui leur est donnée dans l'accord. Les termes suivants ont la signification suivante lorsqu'ils sont utilisés dans le présent DPA :

Lois sur la protection des données désigne le règlement général sur la protection des données (UE 2016/679) (GDPR), la directive sur la vie privée et les communications électroniques (2002/58/CE) et toute autre loi applicable, y compris toute loi nationale de mise en œuvre, toute exigence réglementaire, toute orientation et tout code de pratique applicables au traitement ou aux données personnelles (tels que modifiés ou remplacés de temps à autre) dans les différents pays concernés par les Services.

Données à caractère personnel, processus ou traitement, personnes concernées, contrôleur des données (ou contrôleur) et sous-traitant des données (ou sous-traitant) ont la signification donnée à ces termes en vertu des lois sur la protection des données.

3. OBLIGATIONS

Les parties se conforment aux exigences des lois sur la protection des données en ce qui concerne la fourniture des services et d'autres aspects liés au présent DPA et ne font rien ou ne permettent rien en connaissance de cause qui pourrait entraîner une violation des lois sur la protection des données.

Sans préjudice de la clause ci-dessus, le fournisseur s'engage, en ce qui concerne le traitement des données à caractère personnel :

- Traiter les données à caractère personnel uniquement aux fins et dans le respect des conditions énoncées dans l'Accord et dans le présent DPA, ainsi que sur la base des instructions et directives écrites reçues du Client, et se conformer rapidement à toutes les instructions et directives reçues du Client de temps à autre ;
- informer immédiatement le Client si, de l'avis raisonnable du Fournisseur, toute instruction ou directive du Client enfreint les lois sur la protection des données ;
- ne pas traiter les données à caractère personnel ou permettre leur traitement ou leur accès, en tout ou en partie, autrement que pour la fourniture des services et uniquement dans la mesure raisonnablement nécessaire à l'exécution du présent DPA ;
- Traiter les données à caractère personnel conformément à la durée, à la finalité, au type et aux catégories de personnes concernées spécifiés à l'annexe 1 du présent document (détails du traitement des données) ;
- ne pas copier, exporter ou extraire des données à caractère personnel de quelque manière que ce soit, sauf si cela est nécessaire à l'exécution des services et au respect intégral de cette obligation par ses représentants et ses sous-traitants éventuels, tels que définis dans le cadre du présent DPA ;
- compte tenu de l'état de la technique, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du risque, dont la probabilité et la gravité varient, pour les droits et libertés des personnes physiques, la société et ses filiales mettent en œuvre, en ce qui concerne les données à caractère personnel des clients, les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté à ce risque, y compris, le cas échéant, les mesures visées à l'article 32, paragraphe 1, du RGPD.
- assurer le plein respect de toutes les mesures techniques et organisationnelles complémentaires exigées du client ;
- préserver la confidentialité des données à caractère personnel et ne pas les divulguer, en tout ou en partie, à toute personne ou entité, à l'exception de ses employés :
    - sur la base du besoin d'en connaître et uniquement dans la mesure où cela est nécessaire à l'exécution des services ;

- qui sont dûment habilités à cet effet en raison de leur fonction et de leur qualification et qui sont liés par des obligations équivalentes à celles énoncées dans la présente clause ;
- qui ont reçu une formation appropriée sur les lois relatives à la protection des données concernant le traitement des données à caractère personnel ;
- qui sont informés du caractère confidentiel des données à caractère personnel ; et
- qui sont soumis à un devoir de confidentialité .

- notifier par écrit au Client, dans les meilleurs délais après en avoir pris connaissance, tout accès, perte et/ou destruction, accidentel, illégal ou non autorisé, réel ou suspecté, de données à caractère personnel ("violation de données à caractère personnel"), cette notification devant inclure tous les détails pertinents de la violation, y compris (i) le moment et la nature de l'incident, (ii) le système affecté, le nombre de personnes concernées, les catégories de données à caractère personnel concernées, (iii) les conséquences probables de la violation de données à caractère personnel, (iv) le nom et les coordonnées du responsable de la protection des données ou d'un autre point de contact au sein du Fournisseur où de plus amples informations peuvent être obtenues et (v) les mesures prises ou proposées pour remédier à la violation de données à caractère personnel, y compris les mesures visant à atténuer les effets négatifs éventuels de la violation de données à caractère personnel. Le Fournisseur doit raisonnablement coopérer avec le Client et l'aider dans le cadre de toute enquête concernant la violation de données à caractère personnel, y compris en ce qui concerne les obligations de notification du Client en vertu des lois sur la protection des données. Le Fournisseur doit également aider le Client à se conformer à son obligation de documenter toute violation de données à caractère personnel en effectuant une analyse des causes profondes dès qu'il a connaissance d'une telle violation de données à caractère personnel et en partageant les résultats de cette analyse avec le Client ;
- traiter rapidement et correctement toutes les demandes du client relatives au traitement des données à caractère personnel ;
- aider raisonnablement le client à réaliser toute évaluation de l'impact sur la vie privée requise à la demande du client, dans chaque cas uniquement en relation avec le traitement des données à caractère personnel par le fournisseur et en tenant compte de la nature du traitement et des informations dont il dispose ;
- mettre en œuvre les principes de respect de la vie privée dès la conception et par défaut en ce qui concerne les outils et les applications que l'entreprise utilise pour fournir les services ;
- mettre en œuvre et maintenir un registre complet et actualisé des activités de traitement des données personnelles conformément aux lois sur la protection des données. le Fournisseur fournira au Client une copie de ce registre à la demande du Client ;
  aider raisonnablement le Client dans les meilleurs délais pour tout exercice des droits des personnes concernées et coopérer avec le Client et l'aider à remplir ses obligations en tant que responsable du traitement des données en ce qui concerne les demandes des personnes concernées à tout moment ; l'assistance est limitée à 1 (un) jour-homme, au-delà de cette durée, le Fournisseur facturera le Client sur la base des honoraires convenus.
- dans la mesure où le droit applicable le permet, notifier au client, dans les meilleurs délais, la réception de toute demande émanant d'un bureau gouvernemental ou d'un autre organe administratif, d'une autorité chargée de l'application de la loi ou d'une ordonnance d'un tribunal, l'invitant à divulguer des données à caractère personnel, en précisant le fondement de la demande, l'étendue de la divulgation et les personnes à qui les données à caractère personnel doivent être divulguées ;
- le Fournisseur doit sélectionner un tel sous-traitant avec la diligence requise et vérifier si le sous-traitant est en mesure de respecter les obligations qui lui incombent en vertu des lois sur la protection des données en ce qui concerne le traitement des données à caractère personnel. En outre, le Fournisseur doit :
  - faire en sorte que les sous-traitants secondaires concluent avec le fournisseur des accords écrits dont les conditions ne sont pas moins contraignantes que celles énoncées dans le présent DPA ; et
  - rester entièrement responsable vis-à-vis du client de l'exécution des obligations du soustraitant en vertu des lois sur la protection des données ou de tout acte ou omission de tout soustraitant.
- En cas de modification prévue concernant l'ajout ou le remplacement de sous-traitants, le fournisseur en informe le client à l'avance, donnant ainsi au client la possibilité de s'opposer, pour des motifs raisonnables, à un tel traitement de données à caractère personnel.
- mettre à disposition, sur demande raisonnable du client, toutes les informations nécessaires pour démontrer qu'il respecte les obligations qui lui incombent en vertu du présent DPA et des lois sur la protection des données, et permettre les audits, y compris les inspections, effectués par le client ou par un autre auditeur mandaté par le client, qui aura pris un engagement de confidentialité couvrant l'audit à tout moment, et contribuer à ces audits. Le Fournisseur accordera au Client tous les droits d'accès et toutes les informations nécessaires à la réalisation de ces audits ; toutefois, les droits d'information et d'audit ne s'appliquent que dans la mesure où l'audit réalisé en vertu de l'article 16 de l'Accord ne satisfait pas aux exigences pertinentes de la législation sur la protection des données (y compris, le cas échéant, l'article 28, paragraphe 3, point h), du GDPR) ;

4. SOUS-TRAITANTS

- Le Client autorise le Fournisseur à nommer de nouveaux Sous-traitants pour l'aider à s'acquitter de ses obligations au titre du Contrat. Avant de donner à un sous-traitant l'accès aux données à caractère personnel, le Fournisseur doit : (i) notifier le Client par courrier électronique ; et (ii) s'assurer que ce Sous-Traitant a conclu un accord écrit avec le Fournisseur exigeant que le Sous-Traitant respecte des conditions au moins aussi protectrices que celles prévues dans le présent Accord, y compris des conditions suffisantes pour répondre aux exigences de l'article 28(3) du GDPR. Entre le Client et le Fournisseur, le Fournisseur reste entièrement responsable de tous les actes ou omissions de tout Sous-Traitant tiers qu'il a désigné en vertu du présent Accord. Si le Client a un motif raisonnable de s'opposer à l'utilisation d'un Sous-Traitant, il en informera le Fournisseur. Si le Client s'oppose à un Sous-Traitant, le Fournisseur

mettra à disposition une modification des Services ou de l'utilisation des Services concernés afin d'éviter le Traitement des Données à caractère personnel par le Sous-Traitant ayant fait l'objet d'une objection. Toute modification de ce type sera soumise à l'accord préalable du Client, cet accord ne devant pas être refusé ou retardé de manière déraisonnable. Si le Fournisseur n'est pas en mesure d'apporter ce changement dans un délai raisonnable, qui ne dépassera pas trente (30) jours, le Client peut résilier les Services qui ne peuvent être fournis par le Fournisseur sans l'utilisation du Sous-Traitant récusé, en fournissant une notification écrite. Cette résiliation s'effectuera sans pénalité pour le Client, et si le Client a payé d'avance ces Services, il recevra un remboursement de tous les frais payés d'avance pour la période suivant la date effective de résiliation en ce qui concerne ces Services résiliés.

- La liste détaillée des sous-traitants du fournisseur fournissant des services de traitement de données est disponible sur le lien suivant : https://www.aragoconsulting.eu/wp-content/uploads/2015/12/ARAGO-Consulting-Affiliates-and-sub-processors.pdf. Elle peut être mise à jour si nécessaire conformément à la notification requise définie à l'article 5.

5. UTILISATION DES CLAUSES CONTRACTUELLES TYPES DE L'UE POUR LES TRANSFERTS INTERNATIONAUX

- Afin d'éviter que chacun des Clients affiliés, en tant qu'exportateurs de données, ne doive conclure des accords bilatéraux distincts avec le Fournisseur, en tant qu'importateur de données, le présent Accord, que le Client conclut en son nom propre et au nom des Clients affiliés, est réputé constituer un accord entre chacun des Clients affiliés (chacun de ces Clients affiliés étant un exportateur de données) et le Fournisseur, en tant qu'importateur de données, selon les termes du présent Accord.
- Les parties conviennent que chaque transfert de données à caractère personnel d'un ou plusieurs affiliés du client, en tant qu'exportateurs de données, vers le fournisseur en tant qu'importateur de données, dans chaque cas où un tel transfert serait interdit par les lois sur la protection des données en l'absence des clauses contractuelles types, sera soumis aux conditions des clauses contractuelles types.
- Le présent accord s'applique également aux transferts de données à caractère personnel effectués par des sociétés affiliées à des clients non européens (en tant qu'exportateurs de données) si et dans la mesure où les clauses contractuelles types sont suffisantes pour satisfaire aux exigences locales en la matière.
- Pour éviter toute ambiguïté, un transfert de données à caractère personnel est réputé se produire si le fournisseur accède aux données à caractère personnel d'un affilié du client par quelque moyen que ce soit, y compris, mais sans s'y limiter, par des moyens électroniques, même si l'emplacement physique des données ne change pas et que le fournisseur n'obtient pas la possession de ces données à caractère personnel.
- Les Parties conviennent que le Client peut modifier la liste des exportateurs de données de temps à autre, notamment en ajoutant ou en supprimant l'un de ses affiliés, en informant le Fournisseur.
- le client sera habilité, pour et au nom des sociétés affiliées au client, à faire appliquer le présent accord. le client déploiera des efforts commercialement raisonnables pour s'assurer que toutes les réclamations que les sociétés affiliées au client peuvent avoir en vertu du présent accord contre le fournisseur sont cédées par les sociétés affiliées au client, et le client accepte que ces réclamations puissent être ainsi cédées.

6. APPLICATION DES CLAUSES CONTRACTUELLES TYPES

- Le présent accord incorpore par référence les clauses contractuelles types.
- Les Clauses Contractuelles Types s'appliquent à toutes les Données Personnelles, en particulier les Données Personnelles relatives aux employés du Client, aux utilisateurs, aux clients, aux vendeurs ou à d'autres personnes en relation avec l'Accord, qui sont transférées ou auxquelles on accède à distance depuis l'extérieur de l'EEE, de la Suisse ou de tout pays dont les lois exigent des moyens adéquats pour un tel transfert ou accès international et les moyens adéquats requis peuvent être satisfaits par la conclusion des Clauses contractuelles types, soit directement, soit par transfert ultérieur vers tout pays ou destinataire, dans chaque cas, où un tel transfert ou accès serait interdit par les Lois sur la protection des données en l'absence des Clauses contractuelles types.
- Les clauses contractuelles types s'appliquent aux :
    - les clients affiliés énumérés à l'annexe 2, chacun en tant qu'exportateur de données ;
    - le fournisseur, en tant qu'importateur de données ; et
    - toute autre personne, y compris les sociétés affiliées au Fournisseur et les sous-traitants du Fournisseur qui ont accès aux données à caractère personnel dans le cadre de la fourniture de services au titre du Contrat, chacun en tant que sous-traitant ultérieur.
- Aux fins de la clause 5(a) des Clauses contractuelles types, les Services fournis en vertu du Contrat définissent les instructions de traitement de chaque exportateur de données respectif au Fournisseur en tant qu'importateur de données pour le Traitement des Données à caractère personnel. Le Client peut, à sa seule discrétion, fournir des instructions supplémentaires ou alternatives pour le Traitement des Données à caractère personnel sous son contrôle.
- Les parties conviennent que les copies des accords de sous-traitance qui doivent être envoyées par le fournisseur au client conformément à la clause 5(j) des clauses contractuelles types peuvent être expurgées de toutes les informations commercialement sensibles ou confidentielles.
- En ce qui concerne chaque transfert de données à caractère personnel d'un exportateur de données figurant à l'annexe 2 vers le fournisseur, en tant qu'importateur de données, et aux fins de la clause 9 (droit applicable) des clauses contractuelles types, tout litige ou toute réclamation découlant de son interprétation ou en rapport avec celle-ci sera régi par le droit national de l'exportateur de données concerné.
- Le Fournisseur doit, sur demande raisonnable, mettre à la disposition du Client une liste de tous les Sous-Traitants qui fournissent actuellement des Services dans le cadre du Contrat, et mettre à disposition pour inspection tous les

accords conclus avec ces Sous-Traitants, comme l'exige la clause 11(1) des Clauses Contractuelles Types. Le Client supportera ses propres coûts liés à cet audit et à cette inspection, à moins qu'une anomalie ne soit identifiée, auquel cas le coût de cet audit et de cette inspection sera supporté par le Fournisseur.

- Les clauses contractuelles types sont interprétées à la lumière des dispositions du présent accord. En cas de conflit ou d'incohérence entre le présent accord et les clauses contractuelles types, l'ordre de préséance suivant s'applique:
    - les clauses contractuelles types ;
    - le présent accord.
- Nonobstant ce qui précède, chaque partie prend rapidement, à la demande d'une autorité nationale de protection des données, toutes les mesures nécessaires, y compris la signature d'autres documents et/ou l'accomplissement d'autres formalités (sous forme d'autorisation, d'enregistrement ou autre), qui peuvent être nécessaires pour donner effet au présent accord et/ou se conformer aux lois applicables.

7. CLAUSES CONTRACTUELLES TYPES

Dans le but spécifique de fournir les Services, le Client autorise le Prestataire à transférer, si cela est strictement nécessaire à la fourniture des Services, les Données Personnelles du Client vers l'Inde, le Maroc et la Colombie où sont situées les Sociétés Affiliées du Prestataire fournissant des Services au Client. À cette fin, les Parties conviennent que les Clauses contractuelles types de l'UE pour le transfert de données à caractère personnel vers des pays tiers du 4 juin 2021 (" **CCU de l'UE** ") s'appliqueront à ce transfert de Données à caractère personnel du Client comme suit :

- Les affiliés du prestataire de services décrits à l'annexe 4 se conformeront aux obligations de l'"importateur de données" dans le CCN de l'UE et le client se conformera aux obligations de l'"exportateur de données",
- Lorsque le client agit en tant que responsable du traitement des données et les sociétés affiliées du prestataire de services en tant que sous-traitant, le module deux du CCN de l'UE s'applique. Lorsque le client agit en tant que responsable du traitement des données et les sociétés affiliées du prestataire de services en tant que sous-traitant, le module trois du CCN de l'UE s'applique,
- à la clause 7, la clause d'amarrage optionnelle s'applique,
- à la clause 9, l'option 1 "AUTORISATION PRÉALABLE SPÉCIFIQUE" s'applique et la demande d'autorisation spécifique est soumise au moins soixante (60) jours avant l'engagement du sous-traitant de rang 2,
- aux clauses 17 et 18, les parties conviennent que le droit applicable et le for des litiges pour le CCN de l'UE seront le droit français et les tribunaux français,
- les annexes de la CSC de l'UE seront réputées complétées par les informations figurant à l'appendice 4,
- si et dans la mesure où le CCN de l'UE est en contradiction avec une disposition du présent DPA, le CCN de l'UE prévaudra dans la mesure de cette contradiction.

8. RESTITUTION ET DESTRUCTION DES DONNÉES À CARACTÈRE PERSONNEL

Sauf dans la mesure où la loi applicable l'interdit, la société et le sous-traitant autorisé (le cas échéant) doivent, à la demande écrite du client et à tout moment, restituer rapidement au client toutes les données à caractère personnel ainsi que les copies autorisées (le cas échéant) des données à caractère personnel, y compris les extraits ou autres reproductions (le cas échéant), que ce soit sous forme écrite, électronique ou dans un autre format ou support lisible et exploitable ;

sauf dans la mesure où le droit applicable l'interdit, à l'expiration des périodes de conservation définies par le Client pour chaque catégorie de Données Personnelles ou à la résiliation ou à l'expiration de l'Accord, le Fournisseur supprimera, enlèvera et détruira en toute sécurité toutes les Données Personnelles traitées pour le compte du Client ainsi que les copies autorisées (le cas échéant) des Données Personnelles, y compris les extraits, sauvegardes ou autres reproductions (le cas échéant), que ce soit sous forme écrite, électronique ou autre forme ou support, sauf s'il est nécessaire de conserver ces Données Personnelles strictement à des fins de conformité avec le droit applicable. le Fournisseur certifie par écrit au Client que les Données à caractère personnel ont été détruites en toute sécurité.

Nonobstant la résiliation ou l'expiration de l'accord, les obligations du présent DPA restent valables jusqu'à la restitution ou la destruction complète, l'effacement et le retrait des données à caractère personnel, comme indiqué dans la présente clause.

9. DELEGUÉ A LA PROTECTION DES DONNEES

Le sous-traitant communique au responsable du traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du RGPD.

Il peut être contacté à l'adresse suivante David SAADA - dpo@aragoconsulting.com

10. OBLIGATIONS DU CONTROLEUR A L'EGARD DU SOUS-TRAITANT

Le responsable du traitement s'engage à :

1. fournir au sous-traitant les données mentionnées à l'annexe 1 Particularités du traitement des données,
2. documenter, par écrit, toute instruction relative au traitement des données par le sous-traitant,
3. assurer, avant et pendant le traitement, le respect des obligations prévues par le règlement général sur la protection des données de la part du sous-traitant..,

Annexe 1 Description du traitement des données

OBJET DU TRAITEMENT

Traitement des données relatives à la gestion des voyages et des notes de frais

DUREE DU TRAITEMENT

Le traitement n'excède pas la durée de l'accord et les périodes de conservation définies par le client. En particulier, les données à caractère personnel des employés du client ne seront pas traitées à l'expiration d'une période de 6 mois suivant la fin du contrat de travail.

NATURE ET FINALITE DU TRAITEMENT

Assistance technique en matière de paramétrage, d'assistance et de chargement de données dans le cadre de SAP Concur.

TYPE DE DONNEES A CARACTERE PERSONNEL

Données d'identification, données relatives à la vie professionnelle et données d'enregistrement

Les catégories de données à caractère personnel concernées sont les suivantes :

Module Expense :

- Nom, prénom, carte d'identité, email, pays de résidence
- Immatriculation du véhicule personnel ou professionnel

Module Travel

- Détails du voyage (lieu, localisation, date de départ, date d'arrivée) -
- Adresse personnelle
- Carte de fidélité
- carte d'identité
- Préférences de voyage

CATEGORIES DE PERSONNES CONCERNEES

Les employés et les travailleurs temporaires du client.

SOUS-TRAITANTS AUTORISES :

Tous les sous-traitants secondaires visés à l'annexe 2

ANNEXE 2 - Sous-traitants

Name du sous-traitant	Identifiant national	Nature des activités de traitement des données	Localisation des activités de traitement des données	Mécanisme de transfert, le cas échéant
ARAGO Consulting LATAM Carrera 28D Nº 67B-30, Officinas 204 - 205, 170004 – Manizales, Caldas Colombia	NIT : 901010948-8	Services de support services pour SAP Concur	Colombia	via SAP cloud services
Arago Consulting Iberia LDA, Rua Engº Ferreira Dias, 924, Piso 1, 22/23, 4100-246 Porto Portugal	514 134 305	Services de support services pour SAP Concur	Portugal	via SAP cloud services
Arago Consulting SARL Route de Pré-Bois, 29 Case Postale 1215 Genève Suisse	Numéro federal: CH-660.0.142.014-3	Services de support services pour SAP Concur	Switzerland	via SAP cloud services
Company Consulting Minds LLP JAL 1304, UNICCA EMPORIS Apartments, Sorahunase, Varthur Main Road, Varthur Hobli, Bengaluru – 560087 Karnataka, India	CIN AAY-1095	Services de support services pour SAP Concur	India	via SAP cloud services
ARAGO CONSULTING ESPAÑA, S.L. Calle Puerto 14, 5-5, 29016, Malaga, España	ID : B19328145	Services de support services pour SAP Concur	Spain	via SAP cloud services
ACAFRICA Florida Center Park, Lot 9, N 28, Etage 4 - Sidi Maarouf, Casablanca Maroc	ID : 433937	Services de support services pour SAP Concur	Morroco	via SAP cloud services
ArCoDe GMBH Königsallee 92a Düsseldorf Germany	HRB115801	Services de support services pour SAP Concur	Germany	via SAP cloud services
Arago Consulting Belgium BV Leonardo Da Vincilaan 19A bus 8 1831 Diegem Belgium	BE0768.826.354	Services de support services pour SAP Concur	Belgium	via SAP cloud services

ANNEXE 3 - Mesures techniques et organisationnelles

Les mesures suivantes doivent être prises par le fournisseur (le "prestataire de services") afin d'assurer la conformité avec les lois sur la protection des données, et en particulier avec les articles 28 et 32 du GDPR.

Le Prestataire est conscient de la confidentialité ou de la criticité (en termes d'intégrité ou de disponibilité) d'une partie importante des informations du Client hébergées ou traitées dans le cadre du Contrat et des Services et s'assure qu'il a mis en place, et qu'il maintiendra pendant la durée du RGPD ou la destruction des Données à caractère personnel, la date la plus tardive étant retenue, toutes les mesures techniques et organisationnelles nécessaires ou appropriées, en tenant compte de la nature et du volume des Données à caractère personnel.

Le champ d'application de ces informations confidentielles ou critiques comprend, sans s'y limiter, les données à caractère personnel.

A ce titre, le Prestataire s'engage à appliquer, maintenir et mettre à jour à tout moment des pratiques de sécurité au moins égales à celles communément admises dans le domaine au regard des risques considérés pour le Client. Le Prestataire s'engage également à mettre en place une gouvernance de la sécurité de l'information conforme aux normes de la famille ISO27000, couvrant l'ensemble du périmètre humain, fonctionnel et technique du Contrat.

En particulier, le fournisseur de services s'engage à :

- protéger l'intégrité, la disponibilité, la résilience, la confidentialité et la sécurité de toutes les données à caractère personnel,
- protéger les données à caractère personnel contre la destruction accidentelle ou illicite, les dommages, la perte, l'altération, la divulgation ou l'accès non autorisé ,
- pseudonymiser et crypter les données à caractère personnel, le cas échéant, et
- fournir un niveau de sécurité approprié au risque représenté par le traitement et à la nature des données à caractère personnel à protéger, comme l'exigent les lois sur la protection des données ;
- se conformer aux politiques, procédures et normes de sécurité de l'information que le client porte à son attention, en étant conscient que ces exigences sont susceptibles d'évoluer au fil du temps, en particulier à la lumière des changements dans la réglementation, les menaces et les risques, le contexte commercial et technique du client ;
- notifier sans délai au Client toute difficulté dans l'application de ces Politiques, Procédures et Normes, afin que le Prestataire de services et le Client définissent ensemble un moyen acceptable de traiter cette difficulté ;
- informer, conseiller et avertir sans délai le Client lorsque le Prestataire identifie un risque pour le Client en matière de sécurité de l'information, et a fortiori un incident mettant en cause la confidentialité, l'intégrité ou la disponibilité des données et du processus d'information du Client.

Ces engagements s'appliquent à tous les besoins du client en matière de sécurité de l'information, qu'il s'agisse de données personnelles ou non.

Le prestataire de services permet au Client de réaliser un audit de sécurité efficace mis en œuvre sur son périmètre et s'engage à soutenir la bonne réalisation de cet audit sans contrepartie financière. Cet audit peut donner lieu à la présentation de preuves documentaires ou à des vérifications techniques ou sur site. Il a lieu au maximum une fois par an à la demande du Client et peut également être requis sans limitation d'occurrence en cas d'événement susceptible de faire naître un doute sérieux sur l'adéquation entre la sécurité mise en œuvre et les risques perçus.

Contrôles

L'ACCES AUX DONNEES DU CLIENT ET LEUR GESTION

- Accès du personnel du fournisseur à l'environnement du client au moyen d'un compte nominatif et dédié afin de garantir la traçabilité.
- Le personnel du fournisseur n'a pas accès aux données non cryptées du client, à moins que le client ne l'ait autorisé. Si un tel accès est accordé, il est interdit au Personnel du Fournisseur de stocker des Données Client non cryptées sur des bureaux locaux, des ordinateurs portables, des appareils mobiles, des lecteurs partagés, des supports amovibles tels que des clés USB, ou sur des systèmes publics qui ne sont pas soumis au contrôle administratif ou aux processus de surveillance de la conformité du Fournisseur.
- Le fournisseur n'utilise les données du client que dans la mesure où cela est nécessaire pour fournir des services au client, comme le prévoit l'accord/le contrat.

CHIFFREMENT ET SEPARATION LOGIQUE DES DONNEES DU CLIENT

Dans l'environnement de stockage de production, le service crypte toujours les données du client lorsqu'elles sont au repos à l'aide d'un protocole de cryptage de pointe tel que AES 256 bits.

Le Service crypte le trafic à l'aide d'un protocole de cryptage de pointe tel que Transport Layer Security ("TLS") 1.2, lorsqu'il communique sur des réseaux non fiables tels que l'internet public.

INFRASTRUCTURE GENERALE GESTION DE LA SECURITE

L'accès aux systèmes et à l'infrastructure qui soutiennent le service est limité au personnel du fournisseur qui a besoin d'un tel accès dans le cadre de ses responsabilités professionnelles.

Des identifiants uniques sont attribués au personnel du fournisseur qui doit avoir accès aux serveurs du fournisseur qui supportent le service.

La politique en matière de mots de passe pour le service dans l'environnement de production est conforme aux exigences du client en matière de mots de passe (ou équivalent).

Les droits d'accès des membres du personnel du fournisseur qui ont quitté l'entreprise sont désactivés sans délai. Les privilèges d'accès des personnes transférées à des postes nécessitant des privilèges réduits sont ajustés en conséquence.

Tous les accès des utilisateurs aux systèmes et à l'infrastructure qui soutiennent le service sont examinés régulièrement, au moins deux fois par an.

Les tentatives d'accès aux systèmes et à l'infrastructure qui soutiennent le service sont enregistrées, surveillées et font l'objet d'alertes en cas d'activités suspectes.

GESTION DES RISQUES

Le processus de gestion des risques du fournisseur est fiable et repose sur un modèle bien connu.

Le fournisseur effectue tout au long de l'année différents types d'évaluation des risques, notamment des auto-évaluations et des tests, des analyses automatisées et des examens manuels.

Les modifications apportées aux contrôles et aux stratégies d'atténuation des menaces sont évaluées et classées par ordre de priorité en vue de leur mise en œuvre, sur la base d'un ajustement des risques.

Les menaces sont surveillées par différents moyens, notamment les services de renseignement sur les menaces, les notifications des fournisseurs et les sources publiques fiables.

ANALYSE DE LA VULNERABILITE ET TEST DE PENETRATION

Chaque poste de travail ou infrastructure informatique fait l'objet d'une gestion régulière des correctifs.

ACCES A DISTANCE ET RESEAU SANS FIL

Les bureaux des fournisseurs, y compris les réseaux LAN et Wi-Fi dans ces bureaux, sont considérés comme des réseaux non fiables.

ENREGISTREMENT DES EVENEMENTS SYSTEME, SURVEILLANCE ET ALERTE

Les outils et services de surveillance sont utilisés pour surveiller les systèmes, notamment le réseau, les événements de serveur, les événements de sécurité de l'API du fournisseur de cloud, les événements de disponibilité et l'utilisation des ressources.

Tous les terminaux du fournisseur sont dotés d'outils de protection des terminaux qui surveillent et alertent en cas d'activités suspectes et de logiciels malveillants potentiels.

Tous les réseaux privés en nuage s'appuient sur des outils avancés de détection des menaces pour surveiller et alerter les activités suspectes et les logiciels malveillants potentiels.

ADMINISTRATION DES SYSTEMES ET GESTION DES CORRECTIFS

Le Fournisseur doit créer, mettre en œuvre et maintenir des procédures d'administration de système pour les systèmes qui accèdent aux Données du Client, qui respectent ou dépassent les normes de l'industrie. Ces procédures comprennent, sans s'y limiter, le durcissement du système, l'application de correctifs au système et à l'appareil (système d'exploitation et applications) et l'installation correcte de logiciels de détection des menaces ainsi que la mise à jour quotidienne des signatures de ces logiciels.

L'équipe de sécurité des fournisseurs examine chaque semaine les annonces de vulnérabilités et évalue leur impact sur le fournisseur sur la base de critères de risque définis par le fournisseur, notamment l'applicabilité et la gravité.

Les mises à jour de sécurité applicables classées comme "élevées" ou "critiques" sont traitées dans les 30 jours suivant la publication du correctif et celles classées comme "moyennes" sont traitées dans les 90 jours suivant la publication du correctif.

La solution du fournisseur doit prendre en charge toutes les mises à jour de sécurité qui s'appliquent aux systèmes sur lesquels sa solution est installée.

FORMATION ET PERSONNEL DE SECURITE

Tous les membres du personnel du fournisseur reconnaissent qu'il leur incombe de signaler les incidents ou problèmes de sécurité réels ou présumés, les vols, les violations, les pertes et les divulgations non autorisées des données du client ou l'accès à celles-ci.

L'ensemble du personnel du fournisseur est tenu de suivre régulièrement et de manière satisfaisante une formation à la sécurité.

Le Fournisseur veillera à ce que ses sous-traitants, vendeurs et autres tiers (le cas échéant) qui ont un accès direct aux données du Client dans le cadre des services adhèrent à des normes de sécurité des données conformes aux exigences du Client.

SECURITE PHYSIQUE

Lorsqu'ils sont concernés, tous les contrôles de sécurité physique sont gérés par le fournisseur ou son fournisseur de services en nuage. Le fournisseur examine chaque année les meilleures pratiques afin de garantir des contrôles de sécurité physique appropriés, y compris :

- Gestion des visiteurs, y compris le suivi et la surveillance de l'accès physique.
- Les points d'accès physiques aux emplacements des serveurs sont gérés par des dispositifs de contrôle d'accès électroniques.
- Procédures de surveillance et de réponse aux alarmes.

NOTIFICATION D'UNE VIOLATION DE LA SECURITE

La "violation de la sécurité" est (a) l'accès non autorisé ou la divulgation des données du client, ou (b) l'accès non autorisé aux systèmes du service qui transmettent ou analysent les données du client.

- Le fournisseur notifie par écrit au client, dans les soixante-douze (72) heures, la confirmation d'une violation de la sécurité.
- Cette notification décrira la violation de la sécurité et l'état d'avancement de l'enquête menée par le prestataire.
- Le fournisseur prendra les mesures appropriées pour contenir la violation de la sécurité, enquêter sur celle-ci et en atténuer les effets.

ANNEXE 4

LISTE DES PARTIES soumises aux clauses contractuelles types

Exportateur(s) de données :

1. Nom : *Le client tel que décrit dans le DPA*

   Adresse : *Voir le DPA*

   Nom, fonction et coordonnées de la personne de contact : *Voir le DPA*

   Activités en rapport avec les données transférées en vertu des présentes clauses : *exécution des services conformément à l'accord.*

   Signature et date : *Voir le DPA*

   Rôle : *Contrôleur ou responsable du traitement des données tel que décrit dans l'article 18 du RGPD*

Importateur(s) de données :

1. Nom : *ARAGO Consulting LATAM*

   Adresse : *Carrera 28D Nº 67B-30, Officinas 204 - 205, 170004 - Manizales, Caldas - Colombie*

   Nom, fonction et coordonnées de la personne de contact : *M. Mikael TUITEL Directeur général*

   Activités en rapport avec les données transférées en vertu des présentes clauses : *L'importateur de données est une société spécialisée dans les services Cloud SAP SuccessFactors et Concur, qui fournit des services de mise en œuvre de solutions et de maintenance d'applications.*

   Rôle (contrôleur/traitement) : *Responsable ou sous-traitant du traitement des données, conformément à l'article 18 du RGPD.*

   Signature et date : *Voir le DPA*

2. Nom : *Société Consulting Minds LLP*

   Adresse : *JAL 1304, UNICCA EMPORIS, Varthur Hobli, Bangalore - 560087, Karnataka, Inde*

   Nom, fonction et coordonnées de la personne de contact : *M. Pradeep VUDDANDI Directeur général*

   Activités en rapport avec les données transférées en vertu des présentes clauses : *L'importateur de données est une société spécialisée dans les services Cloud SAP SuccessFactors et Concur, qui fournit des services de mise en œuvre de solutions et de maintenance d'applications.*

   Rôle (contrôleur/traitement) : *Responsable ou sous-traitant du traitement des données, conformément à l'article 18 du RGPD.*

   Signature et date : *Voir le DPA*

3. Nom : *ARAGO Consulting Africa (ACAfrica)*

   Adresse : *Casablanca Nearshore - 1100, Bld Al Quods, Shore 1, - 20270, Casablanca, Maroc*

   Nom, fonction et coordonnées de la personne de contact : *M. Bouchta Toumani Directeur général*

   Activités en rapport avec les données transférées en vertu des présentes clauses : *L'importateur de données est une société spécialisée dans les services Cloud SAP SuccessFactors et Concur, qui fournit des services de mise en œuvre de solutions et de maintenance d'applications.*

   Rôle (contrôleur/traitement) : *Responsable ou sous-traitant du traitement des données, conformément à l'article 18 du RGPD.*

   Signature et date : *Voir le DPA*

B. DESCRIPTION DU TRANSFERT

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

Employés et contractants externes

Catégories de données à caractère personnel transférées

Données d'identification, données relatives à la vie professionnelle et données de connexion

Responsable du traitement Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui prennent pleinement en considération la nature des données et les risques encourus, comme par exemple une limitation stricte de la finalité, des restrictions d'accès (y compris un accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre d'accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires.

Aucune donnée sensible n'est transférée

La fréquence du transfert (par exemple, si les données sont transférées de manière ponctuelle ou continue).

À la demande du client

Nature du traitement

Collecte, enregistrement, structuration, organisation, stockage, extraction, consultation, utilisation, diffusion ou autre mise à disposition et effacement ou destruction et en particulier : incident, demande de service, problème, changement, actions d'amélioration ou travaux de projet.

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

Assistance technique en matière de paramétrage, d'assistance et de chargement de données dans le cadre de SAP Concur

la durée de conservation des données à caractère personnel ou, si cela n'est pas possible, les critères utilisés pour déterminer cette durée

Non conservation sauf sur demande expresse du client. Dans ce cas précis, les données à caractère personnel seront conservées pendant la durée de l'activité de la demande.

Pour les transferts aux (sous-)traitants, préciser également l'objet, la nature et la durée du traitement.

N/A

C. AUTORITÉ DE SURVEILLANCE COMPÉTENTE

L'autorité de contrôle compétente est la Commission nationale de l'informatique et des libertés (*CNIL).*

D. Mesures techniques

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

Tous les détails figurent dans la politique de sécurité et de confidentialité d'ARAGO.