

CLAUSES CONTRACTUELLES TYPES POUR LES TRANSFERTS INTERNATIONAUX

SECTION I

Clause 1. **Objet et champ d'application**

- a) L'objectif de ces clauses contractuelles types est de garantir que les exigences du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1) (règlement général sur la protection des données) sont respectées pour le transfert de données à caractère personnel vers un pays tiers.
- b) Les parties :
 - i) la (les) personne(s) physique(s) ou morale(s), autorité(s) publique(s), service(s) ou organisme(s) (ci-après, "entité" ou "entités") qui transférera les données à caractère personnel, énumérées à l'annexe I.A (chacune étant ci-après dénommée "exportateur de données"), et
 - ii) la ou les entités d'un pays tiers qui recevront les données à caractère personnel de l'exportateur de données directement ou indirectement par l'intermédiaire d'une autre entité également partie au présent cahier des charges, dont la liste figure à l'annexe I.A (chacune étant ci-après dénommée "importateur de données"), ont accepté les présentes clauses contractuelles types (ci-après dénommées "cahier des charges").
- c) La présente spécification s'applique au transfert des données à caractère personnel spécifiées à l'annexe I.B.
- d) L'annexe au présent cahier des charges, qui contient les annexes auxquelles il est fait référence dans le présent cahier des charges, fait partie intégrante du cahier des charges.

Clause 2. **Effet et invariabilité des clauses**

- a) La présente spécification prévoit des garanties adéquates, y compris des droits opposables aux personnes concernées et des voies de recours effectives, conformément à l'article 46, paragraphe 1, et à l'article 46, paragraphe 2, point c), du règlement (UE) 2016/679 et, en ce qui concerne les transferts de données des responsables du traitement vers les sous-traitants ou des sous-traitants vers d'autres sous-traitants, conformément aux clauses contractuelles types visées à l'article 28, paragraphe 7, du règlement (UE) 2016/679, pour autant qu'elles ne soient pas modifiées, sauf aux fins de sélectionner le(s) module(s) approprié(s) ou d'ajouter ou de mettre à jour des informations dans l'annexe. Cela n'empêche pas les parties d'inclure les clauses contractuelles types contenues dans le présent cahier des charges dans un contrat plus large, ou d'ajouter toute clause ou garantie supplémentaire pour autant qu'elles ne contredisent pas directement ou indirectement le présent cahier des charges ou qu'elles ne portent pas atteinte aux droits ou libertés fondamentaux des personnes concernées.
- b) Cette spécification est sans préjudice des obligations auxquelles l'exportateur de données est soumis en vertu du règlement (UE) 2016/679.

Clause 3 - **Tiers bénéficiaires**

- a) Les parties intéressées peuvent, en tant que tiers bénéficiaires, invoquer la présente spécification à l'encontre de l'exportateur et/ou de l'importateur de données et exiger qu'ils s'y conforment, avec les exceptions suivantes.
 - I. Clauses 1, 2, 3, 6 et 7.
 - II. Clause 8 : [module un] clause 8.5(e) et clause 8.9(b) ; [module deux] clause 8.1(b) et clause 8.9(a), (c), (d) et (e) ; [module trois] clause 8.1(a), (c) et (d) et clause 8.9(a), (c), (d), (e), (f) et (g) ; [module quatre] clause 8.1(b) et clause 8.3(b).

- III. Article 9 : [module deux] article 9(a), (c), (d) et (e) ; [module trois] article 9(a), (c), (d) et (e).
- IV. Clause 12 : [module un] clause 12(a) et (d) ; [modules deux et trois] clause 12(a), (d) et (f).
- V. Article 13.

- VI. Clause 15.1 (c), (d) et (e).
- VII. Article 16(e).
- VIII. Article 18 : [modules un, deux et trois] article 18 a) et b) ; [module quatre] article 18.

b) Le point a) est sans préjudice des droits des personnes concernées en vertu du règlement (UE) 2016/679.

Clause 4 - **Interprétation**

- a) Lorsque des termes définis dans le règlement (UE) 2016/679 sont utilisés dans le présent cahier des charges, ils s'entendent au sens dudit règlement.
- b) Ces spécifications doivent être lues et interprétées conformément aux dispositions du règlement (UE) 2016/679.
- c) Les présentes conditions générales ne peuvent être interprétées d'une manière qui entre en conflit avec les droits et obligations énoncés dans le règlement (UE) 2016/679.

Clause 5 - **Hiérarchie**

En cas de contradiction entre les présentes conditions générales et les dispositions des accords connexes entre les parties en vigueur au moment où les présentes conditions générales ont été convenues ou sont entrées en vigueur, les présentes conditions générales prévaudront.

Clause 6 - **Description du (des) transfert(s)**

Les détails du ou des transferts et, en particulier, les catégories de données à caractère personnel transférées et les finalités pour lesquelles elles sont transférées sont précisés à l'annexe I.B.

Clause 7 (facultative). **Clause d'incorporation**

- a) Toute entité qui n'est pas partie à la présente spécification peut, avec le consentement de toutes les parties, y adhérer à tout moment, soit en tant qu'exportateur de données, soit en tant qu'importateur de données, en complétant l'appendice et en signant l'annexe I.A.
- b) Une fois l'appendice complété et l'annexe I.A signée, l'entité adhérente est considérée comme partie à ces spécifications et a les droits et obligations d'un exportateur ou d'un importateur de données, selon la catégorie dans laquelle elle est inscrite à l'annexe I.A.
- c) L'entité adhérente n'acquiert pas de droits et d'obligations en vertu des présentes conditions générales découlant de la période antérieure à l'adhésion.

SECTION II : OBLIGATIONS DES PARTIES

Clause 8 - **Garanties en matière de protection des données**

L'exportateur de données garantit qu'il a fait des efforts raisonnables pour déterminer que l'importateur de données peut, en appliquant des mesures techniques et organisationnelles appropriées, respecter les obligations qui lui incombent en vertu de la présente spécification.

8.1. Instructions

- a) L'importateur de données ne traite les données à caractère personnel que sur la base d'instructions documentées de l'exportateur de données. L'exportateur de données peut donner de telles instructions pendant toute la durée du contrat.

- b) L'importateur de données informe immédiatement l'exportateur de données s'il n'est pas en mesure de suivre ces instructions.

8.2. Limitation de l'objet

L'importateur de données ne traite les données à caractère personnel qu'aux fins spécifiques du transfert énoncés à l'annexe I.B, sauf s'il suit des instructions supplémentaires de l'exportateur de données.

8.3. Transparence

Sur demande, l'exportateur de données met gratuitement à la disposition de la personne concernée une copie de la présente spécification, y compris l'appendice complété par les parties. Dans la mesure nécessaire pour protéger les secrets d'affaires ou d'autres informations confidentielles, telles que les mesures décrites à l'annexe II et les données à caractère personnel, l'exportateur de données peut expurger le texte de l'addendum au présent cahier des charges avant d'en partager une copie, mais il doit fournir un résumé significatif si l'absence de résumé empêche la personne concernée de comprendre le contenu de l'addendum ou d'exercer ses droits. Sur demande, les parties communiquent à la personne concernée les raisons de l'expurgation, dans la mesure du possible sans divulguer les informations expurgées. La présente clause est sans préjudice des obligations de l'exportateur de données en vertu des articles 13 et 14 du règlement (UE) 2016/679.

8.4. Précision

Si l'importateur de données se rend compte que les données à caractère personnel qu'il a reçues sont inexactes ou périmées, il en informe l'exportateur de données dans les meilleurs délais. Dans ce cas, l'importateur de données coopère avec l'exportateur de données pour supprimer ou rectifier les données.

8.5. Durée du traitement et suppression ou restitution des données

Le traitement par l'importateur de données n'est effectué que pendant la période spécifiée à l'annexe I.B. Après la fourniture des services de traitement, l'importateur de données, à la demande de l'exportateur de données, soit supprime toutes les données à caractère personnel traitées pour le compte de l'exportateur de données et fournit à ce dernier la preuve qu'il l'a fait, soit renvoie à l'exportateur de données toutes les données à caractère personnel traitées pour son compte et supprime toutes les copies existantes. Jusqu'à ce que les données soient détruites ou renvoyées, l'importateur de données continue de veiller au respect de la présente spécification. Si la loi du pays applicable à l'importateur de données interdit la restitution ou la destruction des données à caractère personnel, l'importateur de données s'engage à continuer à garantir le respect de la présente spécification et à ne traiter les données que dans la mesure et pour la durée requises par la loi du pays. Ceci est sans préjudice de la clause 14 et en particulier de l'obligation de l'importateur de données en vertu de la clause 14 d'informer l'exportateur de données pendant toute la durée du contrat s'il a des raisons de croire qu'il est ou a été soumis à des réglementations ou pratiques qui ne sont pas conformes aux exigences de la clause 14(a).

8.6. Sécurité du traitement

- a) L'importateur de données et, pendant le transfert, l'exportateur de données mettent en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des données ; en particulier, la protection contre les failles de sécurité entraînant la destruction, la perte ou l'altération accidentelle ou illicite de données à caractère personnel, ou la divulgation ou l'accès non autorisés ("violation de données à caractère personnel"). Pour déterminer un niveau de sécurité approprié, les parties tiennent dûment compte de l'état de la technique, des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques que le traitement fait courir aux personnes concernées. Les parties envisagent en particulier le cryptage ou la pseudonymisation, notamment lors de la transmission, si la finalité du traitement peut être atteinte de cette manière. En cas de pseudonymisation, les informations supplémentaires nécessaires pour attribuer des données à caractère personnel à une personne concernée spécifique doivent, dans la mesure du possible, rester sous le contrôle exclusif de l'exportateur de données. Pour s'acquitter des obligations qui lui incombent en vertu du présent paragraphe, l'importateur de données met en œuvre au moins les mesures techniques et organisationnelles prévues à l'annexe II. L'importateur de données

L'importateur de données effectue des contrôles réguliers pour s'assurer que ces mesures continuent à fournir un niveau de sécurité adéquat.

- b) L'importateur de données n'accorde l'accès aux données à caractère personnel aux membres de son personnel que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Il s'assure que les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont soumises à une obligation de confidentialité de nature légale.
- c) En cas de violation de la sécurité des données à caractère personnel traitées par l'importateur de données en vertu de la présente spécification, l'importateur de données prend les mesures appropriées pour remédier à la violation et, en particulier, des mesures pour en atténuer les effets négatifs. L'importateur de données notifie également à l'exportateur de données, dans un délai raisonnable, toute violation de la sécurité dont il a eu connaissance. Cette notification comprend les coordonnées d'un point de contact auprès duquel des informations complémentaires peuvent être obtenues, une description de la nature de la violation (y compris, si possible, les catégories et le nombre approximatif de personnes concernées et de dossiers de données à caractère personnel affectés), les conséquences probables et les mesures prises ou proposées pour remédier à la violation de la sécurité, en particulier, le cas échéant, les mesures visant à en atténuer les effets négatifs éventuels. Lorsque et dans la mesure où toutes les informations ne peuvent pas être fournies en même temps, la notification initiale fournit les informations actuellement disponibles, et des informations supplémentaires sont fournies sans délai injustifié dès qu'elles sont disponibles.
- d) L'importateur de données coopère avec l'exportateur de données et l'aide à remplir ses obligations au titre du règlement (UE) 2016/679, notamment en ce qui concerne la notification à l'autorité de contrôle compétente et aux personnes concernées, en tenant compte de la nature du traitement et des informations dont dispose l'importateur de données.

8.7. Données sensibles

Dans la mesure où le transfert comprend des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, des données génétiques ou des données biométriques destinées à identifier une personne physique de manière unique, des données relatives à la santé ou des données relatives à la vie sexuelle ou à l'orientation sexuelle d'une personne physique, ou des données relatives à des condamnations pénales et à des infractions (ci-après dénommées "données sensibles"), l'importateur de données applique les restrictions spécifiques et/ou les garanties supplémentaires décrites à l'annexe I.B.

8.8. Transferts ultérieurs

L'importateur de données ne divulgue des données à caractère personnel à un tiers que sur instruction documentée de l'exportateur de données. En outre, les données ne peuvent être divulguées à des tiers situés en dehors de l'Union européenne (4) (dans le même pays que l'importateur de données ou dans un autre pays tiers ; ci-après dénommé "transfert ultérieur") que si le tiers est lié par le présent cahier des charges ou consent à l'être, avec le choix du module concerné, ou si :

- I. le transfert ultérieur est à destination d'un pays couvert par une décision d'adéquation en vertu de l'article 45 du règlement (UE) 2016/679 couvrant le transfert ultérieur ;
- II. le tiers offre par ailleurs des garanties adéquates, au sens de l'article 46 ou 47 du règlement (UE) 2016/679, pour le traitement en question ;
- III. si le transfert ultérieur est nécessaire à la constatation, à l'exercice ou à la défense de droits liés à des procédures administratives, réglementaires ou judiciaires spécifiques ; ou
- IV. si le transfert ultérieur est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique. La validité des transferts ultérieurs dépend du fait que l'importateur de données fournisse les autres garanties prévues dans le présent cahier des charges, et en particulier la limitation de la finalité.

8.9. Documentation et conformité

- a) L'importateur de données répond rapidement et de manière appropriée à toute question de l'exportateur de données concernant le traitement conformément à la présente spécification.
- b) Les parties doivent être en mesure de démontrer le respect de cette spécification. En particulier, l'importateur de données doit conserver une documentation suffisante sur les activités de traitement effectuées pour le compte de l'exportateur de données.
- c) L'importateur de données met à la disposition de l'exportateur de données toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans la présente spécification et, à la demande de l'exportateur de données, autorise et contribue à des audits des activités de traitement couvertes par la présente spécification, à des intervalles raisonnables ou s'il existe des indices de non-respect. Lorsqu'il décide de procéder à un examen ou à un audit, l'exportateur de données peut prendre en compte les certifications pertinentes détenues par l'importateur de données.
- d) L'exportateur de données peut choisir d'effectuer l'audit lui-même ou d'autoriser un auditeur indépendant. Les audits peuvent prendre la forme d'inspections des locaux ou des installations physiques de l'importateur de données et, le cas échéant, être effectués avec un préavis raisonnable.
- e) Les parties mettent les informations visées aux points b) et c), et notamment les résultats des audits, à la disposition de l'autorité de contrôle compétente qui en fait la demande.

Clause 9. Recours à des sous-agents

- a) L'importateur de données ne sous-traite aucune des activités de traitement effectuées pour le compte de l'exportateur de données en vertu des présentes clauses à un sous-traitant ultérieur sans l'autorisation écrite spécifique préalable de l'exportateur de données. L'importateur de données soumet la demande d'autorisation spécifique au moins trente (30) jours civils avant l'engagement du sous-traitant ultérieur, accompagnée des informations nécessaires à l'exportateur de données pour décider de l'autorisation. La liste des sous-traitants ultérieurs déjà autorisés par l'exportateur de données figure à l'annexe III. Les parties tiennent l'annexe III à jour.
- b) Lorsque l'importateur de données fait appel à un sous-traitant ultérieur pour effectuer des activités de traitement spécifiques (pour le compte de l'exportateur de données), il le fait au moyen d'un contrat écrit énonçant, en substance, les mêmes obligations en matière de protection des données que celles imposées à l'importateur de données en vertu de la présente spécification, en particulier en ce qui concerne les droits des personnes concernées en tant que bénéficiaires tiers (8). Les parties conviennent qu'en se conformant à la présente spécification, l'importateur de données se conforme également aux obligations qui lui incombent en vertu de la clause 8.8. L'importateur de données veille à ce que le sous-fournisseur respecte les obligations qui lui incombent en vertu de la présente spécification.
- c) L'importateur de données fournit à l'exportateur de données, sur demande, une copie du contrat conclu avec le sous-traitant ultérieur et de toute modification ultérieure de ce contrat. Dans la mesure où cela est nécessaire pour protéger des secrets commerciaux ou d'autres informations confidentielles, telles que des données à caractère personnel, l'importateur de données peut expurger le texte du contrat avant d'en communiquer une copie.
- d) L'importateur de données reste pleinement responsable vis-à-vis de l'exportateur de données de l'exécution des obligations imposées au sous-traitant ultérieur par son contrat avec l'importateur de données. L'importateur de données notifie à l'exportateur de données tout manquement du sous-traitant ultérieur aux obligations qui lui incombent en vertu de ce contrat.

- e) L'importateur de données convient avec le sous-traitant ultérieur d'une clause de tiers bénéficiaire en vertu de laquelle, au cas où l'importateur de données disparaîtrait de facto, cesserait d'exister en droit ou deviendrait insolvable, l'exportateur de données aurait le droit de résilier le contrat du sous-traitant ultérieur et d'ordonner au sous-traitant ultérieur d'effacer ou de restituer les données à caractère personnel.

Clause 10 - **Droits de la personne concernée**

- a) L'importateur de données notifie sans délai à l'exportateur de données les demandes reçues de la personne concernée. Il ne répond pas lui-même à une telle demande, sauf s'il a été autorisé à le faire par l'exportateur de données.
- b) L'importateur de données aide l'exportateur de données à remplir ses obligations lorsqu'il répond aux demandes d'exercice des droits conférés aux personnes concernées par le règlement (UE) 2016/679. À cet égard, les parties définissent à l'annexe II les mesures techniques et organisationnelles appropriées, en tenant compte de la nature du traitement, garantissant que le responsable du traitement sera assisté dans la mise en œuvre de la présente clause, ainsi que l'objectif et la portée de l'assistance requise.
- c) Pour s'acquitter des obligations qui lui incombent en vertu des points a) et b), l'importateur de données suit les instructions de l'exportateur de données.

Clause 11 - **Recours**

- a) L'importateur de données informe les personnes concernées, de manière transparente et dans un format facilement accessible, par notification individuelle ou sur son site web, du point de contact autorisé pour le traitement des réclamations. L'importateur de données traite rapidement les réclamations reçues des personnes concernées.

L'importateur de données accepte que les personnes concernées puissent également déposer une plainte auprès d'un organisme indépendant de règlement des litiges, sans frais pour la personne concernée. Il informe les personnes concernées, de la manière décrite au point a), de l'existence d'un tel mécanisme de recours et du fait qu'elles ne sont pas obligées de l'utiliser ou de suivre une séquence particulière pour obtenir réparation.

- b) En cas de différend entre une partie intéressée et une partie concernant l'application de ces clauses, cette partie met tout en œuvre pour résoudre la question à l'amiable en temps opportun. Les parties se tiennent mutuellement informées de ces différends et, le cas échéant, coopèrent pour les résoudre.
- c) Lorsque la personne concernée invoque un droit de tiers bénéficiaire en vertu de la clause 3, l'importateur de données accepte la décision de la personne concernée de
 - I. déposer une plainte auprès de l'autorité de contrôle de l'État membre de sa résidence habituelle ou de son lieu de travail, ou auprès de l'autorité de contrôle compétente conformément à la clause 13 ;
 - II. soumettre le litige aux tribunaux compétents au sens de l'article 18.
- d) Les parties conviennent que la personne concernée peut être représentée par un organisme, une organisation ou une association à but non lucratif dans les conditions prévues à l'article 80, paragraphe 1, du règlement (UE) 2016/679.
- e) L'importateur de données doit se conformer à une décision contraignante en vertu du droit de l'UE ou de l'État membre applicable.
- f) L'importateur de données convient que le choix effectué par la personne concernée ne porte pas atteinte à ses droits substantiels et procéduraux de demander réparation conformément au droit applicable.

Clause 12. **Responsabilité**

- a) Chaque partie est responsable envers l'autre (les autres) de tout dommage qu'elle cause à l'autre (aux autres) en cas de violation de ces clauses.
- b) L'importateur de données est responsable envers la personne concernée, et la personne concernée a le droit d'être indemnisée, pour tout dommage matériel ou moral causé par l'importateur de données ou son sous-agent à la personne concernée en raison d'une violation des droits des tiers bénéficiaires en vertu des présentes clauses.
- c) Nonobstant le point b), l'exportateur de données est responsable envers la personne concernée, et la personne concernée a droit à une indemnisation, pour tout dommage matériel ou moral que l'exportateur de données ou l'importateur de données (ou son sous-traitant ultérieur) cause à la personne concernée en portant atteinte aux droits des tiers bénéficiaires en vertu des présentes clauses. Ceci est sans préjudice de la responsabilité de l'exportateur de données et, lorsque l'exportateur de données est un sous-traitant agissant pour le compte d'un responsable du traitement, de la responsabilité du responsable du traitement en vertu du règlement (UE) 2016/679 ou du règlement (UE) 2018/1725, selon le cas.
- d) Les parties conviennent que si l'exportateur de données est tenu responsable, en vertu du point c), des dommages causés par l'importateur de données (ou son sous-agent), il est en droit de réclamer à l'importateur de données la partie de l'indemnisation correspondant à la responsabilité de l'importateur de données pour les dommages.
- e) Lorsque plusieurs parties sont responsables de tout dommage causé à la personne concernée du fait d'une violation des présentes clauses, toutes les parties responsables sont conjointement et solidairement responsables et la personne concernée a le droit d'intenter une action contre l'une quelconque de ces parties.
- f) Les parties conviennent que, si une partie est tenue pour responsable en vertu du paragraphe (e), elle est en droit de réclamer à l'autre (aux autres) partie(s) la partie de l'indemnisation correspondant à sa responsabilité dans le dommage.
- g) L'importateur de données ne peut pas invoquer le comportement d'un sous-fournisseur pour se soustraire à sa propre responsabilité.

Article 13 - **Contrôle**

- a) Lorsque l'exportateur de données est établi dans un État membre de l'UE :] L'autorité de contrôle chargée de veiller au respect par l'exportateur de données du règlement (UE) 2016/679 en ce qui concerne le transfert de données, tel que visé à l'annexe I.C., agit en tant qu'autorité de contrôle compétente.

Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du règlement (UE) 2016/679 conformément à son article 3, paragraphe 2, et a désigné un représentant conformément à l'article 27, paragraphe 1, du règlement (UE) 2016/679 :]. L'autorité de contrôle de l'État membre dans lequel le représentant est établi au sens de l'article 27, paragraphe 1, du règlement (UE) 2016/679, telle que visée à l'annexe I.C, agit en tant qu'autorité de contrôle compétente.

Lorsque l'exportateur de données n'est pas établi dans un État membre de l'UE, mais relève du champ d'application territorial du règlement (UE) 2016/679 conformément à son article 3, paragraphe 2, sans toutefois devoir désigner un représentant conformément à l'article 27, paragraphe 2, du règlement (UE) 2016/679 :]. L'autorité de contrôle compétente est l'autorité de contrôle de l'un des États membres dans lequel se trouvent les personnes concernées dont les données à caractère personnel sont transférées conformément aux présentes clauses dans le cadre de l'offre de biens ou de services qui leur est faite, ou dont le comportement est suivi, comme indiqué à l'annexe I.C.

- b) L'importateur de données accepte de se soumettre à la juridiction de l'autorité de contrôle compétente et de coopérer avec elle dans le cadre de toute procédure visant à assurer le respect de ces clauses. En particulier, l'importateur de données s'engage à répondre aux enquêtes, à se soumettre aux audits et à respecter les mesures prises par l'autorité de contrôle, y compris les mesures correctives et compensatoires. Il fournit à l'autorité de contrôle une confirmation écrite que les mesures nécessaires ont été prises.

SECTION III : DROIT LOCAL ET OBLIGATIONS EN CAS D'ACCÈS PAR LES AUTORITÉS PUBLIQUES

Clause 14. Droit local et pratique affectant l'application des clauses

- a) Les parties affirment qu'elles n'ont aucune raison de croire que le droit et les pratiques du pays tiers de destination applicables au traitement des données à caractère personnel par l'importateur de données, en particulier les exigences relatives à la communication des données à caractère personnel ou les mesures d'autorisation d'accès par les autorités publiques, empêchent l'importateur de données de remplir les obligations qui lui incombent en vertu de la présente spécification. Cette affirmation repose sur la prémisse que le présent cahier des charges n'est pas exclu par la loi et la pratique qui respectent essentiellement les droits et libertés fondamentaux et ne vont pas au-delà de ce qui est nécessaire et proportionné dans une société démocratique pour que l'importateur de données remplisse ses obligations.
préserver l'un des objectifs énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679.
- b) Les parties déclarent qu'en fournissant la garantie visée au point a), elles ont dûment tenu compte, en particulier, des aspects suivants :
- I. les circonstances particulières du transfert, telles que la longueur de la chaîne de traitement, le nombre d'acteurs impliqués et les canaux de transmission utilisés ; les transferts ultérieurs prévus ; le type de destinataire ; la finalité du traitement ; les catégories et le format des données à caractère personnel transférées ; le secteur économique dans lequel le transfert a lieu ; le lieu de stockage des données transférées ;
 - II. le droit et les pratiques du pays tiers de destination, en particulier ceux qui exigent la communication de données aux autorités publiques ou l'autorisation d'accès par ces autorités, qui sont pertinents au regard des circonstances particulières du transfert, ainsi que les limitations et garanties applicables (12) ;
 - III. les garanties contractuelles, techniques ou organisationnelles pertinentes fournies pour compléter les garanties prévues dans le présent cahier des charges, notamment les mesures mises en œuvre lors du transfert et du traitement des données à caractère personnel dans le pays de destination.
- c) L'importateur de données garantit que, lors de l'évaluation visée au point b), il s'est efforcé de fournir à l'exportateur de données les informations pertinentes et s'engage à continuer à coopérer avec l'exportateur de données afin d'assurer le respect de la présente spécification.
- d) Les parties conviennent de documenter l'évaluation visée au point b) et de la mettre à la disposition de l'autorité de surveillance compétente sur demande.
- e) L'importateur de données s'engage à notifier rapidement à l'exportateur de données si, après avoir été lié par le présent cahier des charges et pendant la durée du contrat, il a des raisons de croire qu'il est ou a été soumis à des réglementations ou pratiques non conformes aux exigences du point a), y compris à la suite d'un changement de réglementation dans le pays tiers ou d'une mesure (telle qu'une demande de communication) indiquant une application de cette réglementation dans la pratique qui n'est pas conforme aux exigences du point a).
- f) Si la notification visée au point e) est effectuée ou si l'exportateur de données a des raisons de croire que l'importateur de données n'est plus en mesure de remplir ses obligations au titre de la présente spécification, l'exportateur de données est tenu de le notifier à l'importateur de données conformément aux dispositions

de la présente spécification.

(c) Si l'exportateur de données n'est pas satisfait du caractère adéquat des garanties, il détermine rapidement les mesures appropriées (par exemple, des mesures techniques ou organisationnelles pour assurer la sécurité et la confidentialité) à prendre par l'exportateur de données et/ou l'importateur de données pour remédier à la situation [Module trois : le cas échéant, après consultation du responsable du traitement]. L'exportateur de données suspend le transfert des données s'il considère qu'il n'existe pas de garanties adéquates ou si [Module trois : le responsable du traitement ou] l'autorité de contrôle compétente l'ordonne. Dans ce cas, l'exportateur de données a le droit de résilier le contrat en ce qui concerne le traitement des données à caractère personnel dans le cadre du présent cahier des charges. Si le contrat comporte plus de deux parties contractantes, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en aient convenu autrement. En cas de résiliation du contrat en vertu de la présente clause, la clause 16, points d) et e), s'applique.

Clause 15. **Obligations de l'importateur de données en cas d'accès par les autorités publiques**

15.1. **Notification**

- a) L'importateur de données s'engage à notifier rapidement à l'exportateur de données et, si possible, à la personne concernée (si nécessaire, avec l'aide de l'exportateur de données) si :
 - I. reçoit une demande juridiquement contraignante de communication de données à caractère personnel transférées conformément à la présente spécification de la part d'une autorité publique (en particulier une autorité judiciaire) en vertu du droit du pays de destination ; cette notification contient des informations sur les données à caractère personnel demandées, l'autorité requérante, la base juridique de la demande et la réponse apportée ; ou
 - II. sait que les autorités publiques ont eu un accès direct aux données à caractère personnel transférées conformément au présent cahier des charges en vertu de la législation du pays de destination ; cette notification comprendra toutes les informations dont dispose l'importateur de données.
- b) Si le droit du pays de destination interdit à l'importateur de données de notifier l'exportateur de données et/ou la personne concernée, l'importateur de données s'engage à faire de son mieux pour obtenir une dérogation à l'interdiction afin de communiquer toutes les informations disponibles dans les meilleurs délais. L'importateur de données s'engage à documenter ses actions à cette fin afin de pouvoir justifier sa diligence si l'exportateur de données le lui demande.
- c) Dans la mesure où le droit du pays de destination le permet, l'importateur de données s'engage à fournir à l'exportateur de données, à intervalles réguliers pendant la durée du contrat, autant d'informations pertinentes que possible sur les demandes reçues (en particulier, le nombre de demandes, le type de données demandées, l'autorité ou les autorités requérante(s), la contestation des demandes, l'issue de ces contestations, etc.
- d) L'importateur de données s'engage à conserver les informations visées aux points a) à c) pendant la durée du contrat et à les mettre à la disposition de l'autorité de contrôle compétente sur demande.
- e) Les points a) à c) sont sans préjudice de l'obligation de l'importateur de données, visée à la clause 14, point e), et à la clause 16, d'informer rapidement l'exportateur de données lorsqu'il n'est pas en mesure de se conformer à la présente spécification.

15.2. **Contrôles de légalité et minimisation des données**

- a) L'importateur de données s'engage à contrôler la légalité de la demande de communication et, en particulier, à vérifier si l'autorité publique requérante est dûment habilitée à le faire, et à contester la demande si, après une évaluation minutieuse, il conclut qu'il existe des motifs raisonnables de considérer que la demande est illégale en vertu du droit du pays de destination, y compris les obligations suivantes

applicables en vertu du droit international et des principes de courtoisie internationale. L'importateur de données doit, dans les mêmes conditions, épuiser toutes les autres voies de recours. Lorsqu'il conteste une demande, l'importateur de données demande des mesures provisoires pour suspendre les effets de la demande jusqu'à ce que l'autorité judiciaire compétente ait statué sur le fond. Il ne communique pas les données à caractère personnel demandées tant qu'il n'est pas tenu de le faire en vertu des règles de procédure applicables. Ces exigences sont sans préjudice des obligations de l'importateur de données au titre de la clause 14, point e).

- b) L'importateur de données s'engage à documenter ses évaluations juridiques et ses contestations des demandes de divulgation et à mettre cette documentation à la disposition de l'exportateur de données dans la mesure où le droit du pays de destination le permet. Il met également cette documentation à la disposition de l'autorité de contrôle compétente qui en fait la demande. [Module trois : L'exportateur de données met l'évaluation à la disposition du responsable du traitement.
- c) L'importateur de données s'engage à fournir le moins d'informations possible lorsqu'il répond à des demandes de communication, sur la base d'une interprétation raisonnable de la demande.

SECTION IV : DISPOSITIONS FINALES

Clause 16. Non-exécution des clauses et résiliation du contrat

- a) L'importateur de données informe rapidement l'exportateur de données s'il n'est pas en mesure de respecter la présente spécification pour quelque raison que ce soit.
- b) Si l'importateur de données ne respecte pas les obligations qui lui incombent en vertu de la présente spécification, l'exportateur de données suspend le transfert de données à caractère personnel à l'importateur de données jusqu'à ce que l'exécution soit à nouveau assurée ou que le contrat soit résilié. Cette disposition est sans préjudice de la clause 14, point f).
- c) L'exportateur de données a le droit de résilier le contrat en ce qui concerne le traitement des données à caractère personnel en vertu de la présente spécification lorsque :
 - I. l'exportateur de données a suspendu le transfert de données à caractère personnel à l'importateur de données conformément au point b) et le respect de cette spécification n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
 - II. l'importateur de données enfreint de manière substantielle ou persistante les présentes spécifications ;
ou
 - III. l'importateur de données ne se conforme pas à une décision contraignante d'un tribunal compétent ou d'une autorité de contrôle en ce qui concerne les obligations qui lui incombent en vertu du présent cahier des charges.

Dans ce cas, il informe l'autorité de contrôle compétente [module trois : et le responsable du traitement] de sa violation. Si le contrat comporte plus de deux parties contractantes, l'exportateur de données ne peut exercer ce droit de résiliation qu'à l'égard de la partie concernée, à moins que les parties n'en aient convenu autrement.

- d) Les données à caractère personnel qui ont été transférées avant la résiliation du contrat conformément au point c) sont, au choix de l'exportateur de données, renvoyées immédiatement à l'exportateur de données ou détruites dans leur intégralité. Il en va de même pour les copies des données]. [Module quatre : Les données à caractère personnel collectées par l'exportateur de données dans l'UE qui ont été transférées avant la résiliation du contrat conformément au point c) sont détruites immédiatement dans leur intégralité, ainsi que toute copie de ces données]. L'importateur de données fournit à l'exportateur de données la preuve de la destruction des données. Jusqu'à ce que les données soient détruites ou renvoyées, l'importateur de données continue de veiller au respect de la présente spécification. Si la loi du pays applicable à l'importateur de

données interdit la restitution ou la destruction des données à caractère personnel transférées, l'importateur de données s'engage à continuer à

garantir le respect du présent cahier des charges et ne traitera les données que dans la mesure et pour la durée requises par le droit national.

- e) Aucune des parties ne peut retirer son consentement à être liée par la présente spécification si : (i) la Commission européenne adopte une décision en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 réglementant le transfert de données à caractère personnel auquel la présente spécification s'applique ; ou (ii) le règlement (UE) 2016/679 devient partie intégrante du droit du pays vers lequel les données à caractère personnel sont transférées. Ceci est sans préjudice des autres responsabilités qui s'appliquent au traitement en question en vertu du règlement (UE) 2016/679.

Clause 17. Droit applicable

Ces clauses sont régies par le droit de l'un des États membres de l'UE, à condition que ce droit autorise les droits des tiers bénéficiaires. Les parties conviennent que le droit espagnol sera applicable.

Clause 18. Choix du for et de la juridiction

- a) Tout litige découlant du présent cahier des charges sera tranché judiciairement dans un État membre de l'Union européenne.
- b) Les parties conviennent que les tribunaux espagnols sont compétents.
- c) Les personnes concernées peuvent également tenter une action en justice contre l'exportateur de données et/ou l'importateur de données dans l'État membre dans lequel la personne concernée a sa résidence habituelle.
- d) Les parties acceptent de se soumettre à la juridiction de cet État membre.

Clause 19 - Garanties supplémentaires

L'importateur de données s'engage à mettre en œuvre les garanties supplémentaires spécifiées dans la **section 3 : Mesures de sécurité**.

ANNEXE

ANNEXE I

A. LISTE DES PIÈCES

Exportateur(s) de données :

Nom : **CTAIMA OUTSOURCING Y CONSULTING S.L.** - B43715812

Adresse : Salvador Espriu, 18, Tarragona 43007, Espagne

Nom, fonction et coordonnées : Lorenzo de Zavala, représentant légal, administracion@ctaima.com

Activités liées aux données transférées en vertu des présentes clauses :

L'importateur de données fournit les services à l'exportateur de données conformément à un accord entre les parties.

Les services consistent en l'examen, la validation et le téléchargement de la documentation sur les plateformes de coordination des entreprises.

Lorenzo de Zavala

4/12/2023

Fonction : contrôleur de données.

Importateur(s) de données :

Nom : **CTAIMA COLOMBIA S.A.S.** - 901717143-1

Adresse : Cra. 12 No. 89-33, Bogotá D.C. 110211, Colombie

Nom, fonction et coordonnées : Luis de los Santos, représentant légal, administracion@ctaima.com

Activités liées aux données transférées en vertu des présentes clauses :

L'importateur de données fournit des services d'examen, de validation et de téléchargement aux plateformes de coordination des entreprises applicables à l'exportateur de données, conformément à l'accord conclu entre les parties.

Luis de los Santos

4/12/2023

Fonction : Processeur.

B. DESCRIPTION DU TRANSFERT

Catégories de personnes dont les données à caractère personnel sont transférées

- Travailleurs du client/entrepreneur.

Catégories de données à caractère personnel transférées

- Données d'identification (nom et prénom), fonction, e-mail et numéro de téléphone des utilisateurs de l'application du client.
- Données d'identification (nom et prénom), fonction, e-mail et numéro de téléphone des contractants du client.
- Données d'identification (nom et prénom), fonction, e-mail et numéro de téléphone des clients de nos clients.

- Données d'identification (nom et prénom), données relatives au travail et à la prévention des risques professionnels (coordination de l'entreprise) des travailleurs de l'entrepreneur.

Activités de traitement.

Fréquence de transfert : continue.

Nature du traitement

La nature du traitement est de fournir les services au contrôleur conformément au contrat et à toute autre instruction donnée par le contrôleur.

Objet du transfert et du traitement ultérieur des données

Examen, validation et téléchargement de la documentation sur les plates-formes de coordination des entreprises. Il n'y a pas de post-traitement après la fin de l'accord.

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

L'importateur de données conserve les données à caractère personnel transférées jusqu'à leur suppression conformément aux directives de l'exportateur de données concernant leur destruction ou leur restitution.

Il n'y a pas de sous-traitance.

C. L'AUTORITÉ DE SURVEILLANCE COMPÉTENTE

Agence espagnole de protection des données. C/ Jorge Juan, 6. 28001 - Madrid. Tél. 900 293 183. www.aepd.es

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

1. Politiques de sécurité de l'information : mettre en œuvre des politiques de sécurité de l'information qui établissent des normes et des procédures pour protéger les données personnelles transférées. L'entreprise établit des politiques et des procédures pour protéger le transfert d'informations afin d'empêcher leur interception, leur copie, leur modification ou leur destruction non autorisées.
2. L'examen et la validation des documents se font exclusivement à distance avec les systèmes informatiques du responsable du traitement, et il est expressément interdit de télécharger des documents contenant des données à caractère personnel sur les propres systèmes informatiques du sous-traitant dans le pays où il est situé.
3. Cryptage des données : crypter toutes les informations sensibles pendant le transfert et le stockage afin d'empêcher tout accès non autorisé.
4. Contrôle d'accès : mettre en œuvre des systèmes de contrôle d'accès qui limitent l'accès aux données au seul personnel autorisé, en attribuant des rôles et des permissions. Les installations doivent être protégées par un contrôle physique des entrées afin de garantir l'accès au seul personnel autorisé. Toutes les visites seront supervisées et contrôlées.
5. Contrôle et enregistrement des accès : mettre en place un système de contrôle et d'enregistrement des accès afin d'enregistrer et de superviser toutes les activités liées aux données transférées. L'entreprise surveille ses systèmes d'information et de traitement hébergés dans le nuage à l'aide du service Microsoft Azure Monitor afin de détecter les activités non autorisées et de les enregistrer en tant qu'incidents de sécurité, en examinant le journal des opérations et des défaillances de ses systèmes afin d'identifier le problème.
6. L'entreprise gère et contrôle son réseau afin de le protéger contre tout accès non autorisé, de maintenir la sécurité de ses systèmes et des applications qui l'utilisent, y compris les informations en transit.
7. Mises à jour et correctifs de sécurité : maintenir tous les systèmes et applications à jour avec les derniers correctifs de sécurité afin d'atténuer les vulnérabilités. Les vulnérabilités identifiées dans les environnements critiques seront enregistrées et une personne responsable de la gestion et de la coordination de la correction des vulnérabilités sera désignée.
8. Protection contre les logiciels malveillants : mettre en œuvre des mesures de protection contre les logiciels malveillants, telles que des pare-feu, des antivirus et des anti-programmes malveillants, afin de prévenir les infections et les cyber-attaques. L'entreprise met en œuvre des contrôles pour la détection, la prévention et la récupération qui protègent les systèmes d'information, ainsi qu'une sensibilisation appropriée du personnel. L'entreprise établit ces politiques afin de maintenir la confidentialité, la disponibilité et l'intégrité des informations sur ses systèmes.
9. Sauvegarde et récupération des données : établir des procédures de sauvegarde régulières pour les données transférées et des systèmes de récupération en cas de défaillance ou d'incident de sécurité.
10. Formation et sensibilisation du personnel : former et sensibiliser régulièrement le personnel à la sécurité de l'information afin de garantir le respect des politiques et procédures établies.
11. Audits de sécurité : effectuer régulièrement des audits de sécurité afin d'évaluer l'efficacité des mesures mises en œuvre et de détecter d'éventuelles vulnérabilités.
12. Gestion des incidents de sécurité : établir un plan de gestion des incidents de sécurité qui prévoit la notification en temps utile de toute violation de la sécurité au délégué à la protection des données et aux autorités compétentes.
13. Évaluation des risques : procéder à des évaluations régulières des risques liés à la sécurité de l'information afin d'identifier et d'atténuer les menaces et les vulnérabilités potentielles.

Ces mesures techniques et organisationnelles contribueront à garantir la sécurité des données transférées en dehors de l'Union européenne, respectant ainsi les exigences en matière de protection des données énoncées dans le contrat de clauses contractuelles types.

ANNEXE III - LISTE DES SOUS-TRAITANTS SECONDAIRES

Il n'y a pas de sous-traitance.

CTAIMA COLOMBIA S.A.S.

*Nom : Luis de los Santos
Poste : Représentant légal*

**CTAIMA OUTSOURCING AND CONSULTING
S.L.**

*Nom : Lorenzo de Zavala
Poste : Représentant légal*