

DERNIÈRE MISE À JOUR : 22 juin 2021

Avenant relatif au traitement des données

Le présent Avenant relatif au traitement des données (l'« **ATD** ») est un addendum au Contrat de licence d'utilisateur final de The Lincoln Electric Company (« **CLUF** ») et est applicable entre The Lincoln Electric Company (le « **Sous-traitant** » [Data Processor]) et l'Utilisateur autorisé conformément au CLUF (le « **Responsable du traitement des données** »), (chacun étant individuellement une « **Partie** » et ensemble les « **Parties** »).

ATTENDU QUE

Le CLUF régit le droit de l'Utilisateur autorisé d'utiliser l'Application sous licence et, le cas échéant, d'autres services en ligne fournis par The Lincoln Electric Company. Aux fins de satisfaire à ses obligations en vertu du CLUF, Lincoln Electric Company agira en tant que Sous-traitant [Data Processor] du traitement des données au nom de l'Utilisateur autorisé. Afin d'assurer le respect de la réglementation sur les Données personnelles, les Parties sont convenues de compléter le CLUF pour définir les conditions générales applicables au traitement des données à caractère personnel par le Sous-traitant [Data Processor] au traitement des données pour le compte du Responsable du traitement.

IL EST CONVENU QUE

1. DÉFINITIONS

1.1 Dans le présent ATD, les termes en majuscules auront les significations suivantes, à moins qu'ils ne soient définis dans le CLUF ou d'une autre façon requise compte tenu du contexte :

« Responsable du traitement des données »	désigne l'entité qui détermine les finalités et les moyens du Traitement des Données Personnelles ;
« Sous-traitant » [Data Processor]	désigne l'entité qui Traite des Données personnelles pour le compte du Responsable du traitement des données ;
« Personne concernée »	désigne une personne identifiée ou identifiable dont les Données personnelles sont traitées ;
« Instruction »	désigne les instructions communiquées par le Responsable du traitement des données au Sous-traitant [Data Processor] pour Traiter les Données personnelles dans le cadre de la prestation de services conformément au CLUF ;
« Données personnelles »	désigne toutes les informations relatives à une personne physique identifiée ou identifiable ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs facteurs propres à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale ;
« Violation de Données personnelles »	désigne une violation de la sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès accidentel ou illégal à des Données personnelles transmises, stockées ou Traitées de toute autre manière ;
« Traitement »/« Traitant »/« Traité »	désigne toute action effectuée sur les Données personnelles telle que la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion, transfert ou mise à disposition, l'alignement ou la combinaison, la restriction, la suppression ou la destruction ;
« Services de traitement »	désigne le Traitement des Données à caractère personnel par le Sous-traitant [Data Processor] dans le cadre du CLUF ;
« Catégories spéciales de données à caractère personnel »	désigne toute donnée à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance à un syndicat, à des associations ou à des fondations, la comparution, les condamnations pénales et les mesures de sûreté, les informations financières et

immobilières, les informations sur la localisation ou les informations de crédit et le Traitement de données génétiques, de données biométriques dans le but d'identifier de manière unique une personne physique, de données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou concernant des mineurs âgés de 14 ans ou moins ;

« Clauses contractuelles types »

désigne les clauses contractuelles types adoptées par la décision de la Commission européenne 2010/87 du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel à des sous-traitants établis dans des pays tiers, ou tout autre ensemble de clauses types convenues entre les parties. Lorsque le Responsable du traitement est établi dans une juridiction hors de l'Union européenne, les références aux États membres dans les dispositions de fond des clauses contractuelles types doivent être interprétées comme des références à la juridiction où le Responsable du traitement est établi ;

**« Sous-traitant »
[Subprocessor]**

désigne tout sous-traitant engagé par le Sous-traitant [Data Processor] (ou par tout autre Sous-traitant [Subprocessor] du Sous-traitant [Data Processor]) pour Traiter des Données personnelles pour le compte du Responsable du traitement des données conformément à ses Instructions et aux termes du contrat écrit de sous-traitance.

- 1.2 Les légendes et les en-têtes de section utilisés le sont uniquement à des fins de référence et de commodité, ne font pas partie du présent ATD et ne doivent pas être utilisés pour l'interpréter.

2. PORTÉE ET APPLICATION DE CET ATD

- 2.1 Cet ATD complète uniquement les stipulations du CLUF en ce qui concerne les Services de traitement fournis par le Sous-traitant au Responsable du traitement des données conformément au CLUF.

3. TRAITEMENT DES DONNÉES

- 3.1 Le Sous-traitant s'engage à traiter les données à caractère personnel conformément aux conditions générales énoncées dans le présent ATD, et en particulier à :

3.1.1 Traiter les Données personnelles uniquement pour le compte du Responsable du traitement des données et à tout moment conformément aux instructions du Responsable du traitement des données telles que définies dans le présent ATD, ainsi qu'à toutes les lois applicables en matière de protection des données ;

3.1.2 s'assurer que tout personnel chargé des Services de traitement s'est engagé à la confidentialité ou est soumis à une obligation légale adéquate de confidentialité ;

3.1.3 prendre des mesures techniques, physiques et organisationnelles pour assurer la sécurité et la confidentialité des Données personnelles et protéger de manière appropriée les Données personnelles traitées pour le compte du Responsable du traitement des données contre les abus et la perte, comme prévu à l'annexe 2 du présent ATD ;

3.1.4 informer rapidement le Responsable du traitement des données de : (a) toute demande juridiquement contraignante de divulgation des Données personnelles par une autorité gouvernementale, sauf interdiction contraire, telle qu'une interdiction en vertu du droit pénal pour préserver le secret d'une enquête policière ou de renseignement, (b) toute violation de Données personnelles affectant les Données personnelles traitées pour le compte du Responsable du traitement des données, (c) toute demande reçue directement des Personnes concernées (y compris les droits d'accès, de rectification, de suppression, d'objection, de restriction, de transfert de données et le droit ne pas faire l'objet d'une décision fondée uniquement sur un Traitement automatisé, y compris le profilage) ; le Sous-traitant (i) ne répondra pas directement à cette demande, sauf pour informer la Personne concernée qu'il agit pour le compte du Responsable du traitement des données, et pour communiquer à la Personne concernée les coordonnées du Responsable du traitement des données et, (ii) en tenant compte de la

nature du Traitement, assistera le Responsable du traitement par des mesures techniques, physiques et organisationnelles appropriées, dans la mesure du possible, pour l'exécution de l'obligation du Responsable du traitement de répondre aux demandes d'exercice des droits de la Personne concernée ;

- 3.1.5 fournir une coopération commercialement raisonnable au Responsable du traitement des données pour l'aider à se conformer à ses propres obligations légales liées à la sécurité des Données personnelles, telles que : notification d'une violation de Données personnelles à l'autorité de surveillance compétente, communication de cette violation de Données personnelles aux Personnes concernées et, le cas échéant, mise en œuvre d'analyses d'impact sur la protection des données et de consultations préalables avec les autorités de contrôle, en tenant compte de la nature du Traitement et des informations dont dispose le Sous-traitant ;
- 3.1.6 mettre à la disposition du Responsable du traitement des données toutes les informations nécessaires pour prouver le respect des obligations énoncées dans le présent ATD et permettre et contribuer aux audits, y compris les inspections, menés par le Responsable du traitement des données ou un autre auditeur mandaté par ledit Responsable comme indiqué à l'article 6 ; et,
- 3.1.7 que tous les Services de traitement exécutés par un Sous-traitant *[Subprocessor]* ultérieur seront exécutés conformément à l'article 7.

3.2 En ce qui concerne les Services de traitement, le Responsable du traitement des données sera responsable du respect de toutes les exigences qui lui sont applicables en vertu de la loi applicable concernant le Traitement de Données personnelles et les instructions qu'il transmet au Sous-traitant. En particulier, mais sans préjudice de la généralité de ce qui précède, le Responsable du traitement reconnaît et accepte qu'il sera seul responsable des éléments suivants : (i) l'exactitude, la qualité et la licéité des Données personnelles ; (ii) la conformité à toutes les exigences de transparence et de légalité nécessaires en vertu de la loi applicable pour la collecte et l'utilisation des Données personnelles, y compris l'obtention des consentements et autorisations nécessaires des Personnes concernées ou autrement ; (iii) le fait de s'assurer que le Responsable du traitement des données a le droit de transférer, ou de donner accès aux Données personnelles au Sous-traitant et que le Responsable du traitement a fourni toutes les notifications requises et obtenu tous les consentements et/ou autorisations requis en relation avec ce transfert ou accès et, plus généralement, pour le Traitement conformément aux termes du CLUF (y compris le présent ATD) ; et (iv) le fait de s'assurer que ses Instructions sont conformes aux lois applicables. À la demande du Sous-traitant, le Responsable du traitement des données fournira au Sous-traitant dans les trois (3) jours ouvrables une preuve écrite de ces notifications, consentements et autorisations. Le Responsable du traitement des données ne saisira dans les Services de traitement, ni ne fournira de quelque autre manière au Sous-traitant *[Data Processor]*, aucune catégorie spéciale de Données personnelles, à moins que le Responsable du traitement des données n'y consente séparément par écrit. Le Responsable du traitement des données informera le Sous-traitant, immédiatement et sans retard injustifié, s'il n'est pas en mesure de se conformer à ses responsabilités énoncées dans le présent ATD. L'Utilisateur autorisé est seul responsable de l'examen des Services de traitement, y compris la documentation et les fonctionnalités de sécurité disponibles, afin de déterminer s'ils satisfont aux exigences, aux besoins commerciaux et aux obligations légales de l'Utilisateur autorisé.

3.3 Le Responsable du traitement des données autorise le Sous-traitant à anonymiser les Données personnelles Traitées conformément au CLUF afin de dériver des données analytiques relatives à l'utilisation de l'Application sous licence et des produits et équipements de Lincoln. L'utilisation ultérieure des données statistiques en résultant par le Sous-traitant n'est pas soumise à l'autorisation préalable du Responsable du traitement des données.

4. TRANSFERTS INTERNATIONAUX DE DONNÉES

4.1 Le Responsable du traitement des données reconnaît et accepte par la présente que, pour fournir les Services de traitement en vertu du CLUF, le Sous-traitant peut transférer et conserver des Données personnelles aux États-Unis d'Amérique et dans tout autre pays dans lequel le Sous-traitant est situé, dans le but de fournir les Services de traitement. Par conséquent, dans le cadre de la prestation des Services de traitement, il peut être nécessaire de transférer des Données personnelles au Sous-traitant situé en dehors du pays d'établissement du Responsable du traitement des données. Si le Responsable du traitement des données est situé dans l'Espace économique européen ou en Suisse, les Parties s'engagent à appliquer les stipulations des clauses contractuelles

types pour le transfert de données personnelles par le Responsable du traitement (agissant en tant qu'exportateur de données conformément aux clauses contractuelles types) au Sous-traitant (agissant en tant qu'importateur de données conformément aux clauses contractuelles types).

- 4.2 Si le Responsable du traitement est situé en dehors de l'Espace économique européen et de la Suisse, les Parties s'engagent également à appliquer les stipulations des clauses contractuelles types pour le transfert de données personnelles par le Responsable du traitement des données (agissant en tant qu'exportateur de données conformément aux clauses contractuelles types) au Sous-traitant (agissant en tant qu'importateur de données conformément aux clauses contractuelles types), à condition que les clauses contractuelles types soient légalement requises et suffisantes pour répondre aux exigences des réglementations applicables en matière de protection des données pour le transfert de données personnelles par le Responsable du traitement des données au Sous-traitant conformément au CLUF.
- 4.3 Si les Parties appliquent les clauses contractuelles types conformément aux articles 4.1 ou 4.2 du présent ATD :
- 4.3.1 L'annexe 1 des clauses contractuelles types s'appliquera sur la base suivante : (a) Exportateur de données : le Responsable du traitement des données, (b) Importateur de données : le Sous-traitant, (c) Personnes concernées : le personnel du Responsable du traitement (Utilisateur autorisé), (d) Catégories de données : données relatives à l'utilisation de produits et d'équipements détenus, sous licence ou gérés par le Sous-traitant, telles que surveillées par l'Application sous licence conformément au CLUF, y compris les données d'enregistrement (c'est-à-dire les noms d'utilisateur et les mots de passe), (e) Catégories spéciales de Données personnelles : S.O., et (f) Opérations de traitement : collecte, copie, transfert, stockage, modification, suppression et autres opérations nécessaires aux Services de traitement conformément au CLUF.
- 4.3.2 La description des mesures de sécurité techniques, physiques et organisationnelles mises en œuvre par le Sous-traitant agissant en tant qu'importateur de données aux fins de l'annexe 2 des clauses contractuelles types doit être conforme à l'annexe 2 du présent ATD.
- 4.4 Si les clauses contractuelles types sont applicables entre les parties conformément à l'article 4.1 ou 4.2, leurs stipulations seront réputées incorporées par référence au présent ATD, à moins que les Parties ne signent les clauses contractuelles types en tant que document autonome conformément à l'article 4.5.
- 4.5 Dans la mesure requise par les réglementations applicables en matière de protection des données, les Parties concluront et signeront les clauses contractuelles types en tant que document séparé.

RÉSILIATION

- 5.1 Cet ATD entrera en vigueur à la date d'entrée en vigueur du CLUF.
- 5.2 Le présent ATD prendra fin automatiquement à la dernière des deux dates suivantes : la résiliation ou l'expiration (a) du CLUF ou (b) des obligations du Sous-traitant [Data Processor] au regard des Services de traitement, et cette résiliation ne nécessitera pas d'ordonnance ou de procédure judiciaire ou toute autre action du Sous-traitant [Data Processor], du Responsable du traitement ou de toute autre partie pour entrer en vigueur. Le cas échéant, à la résiliation du présent ATD, le Sous-traitant [Data Processor] doit restituer au Responsable du traitement ou supprimer, à la demande de ce dernier, toutes les Données personnelles du Responsable du traitement en sa possession ou sous son contrôle. À la demande du Responsable du traitement des données, le Sous-traitant [Data Processor] doit confirmer le respect de ces obligations par écrit et supprimer toutes les copies existantes, à moins que la loi applicable n'exige le stockage ou n'autorise autrement la conservation des Données personnelles.
- 5.3 Le Responsable du traitement des données aura le droit de résilier le présent ATD par notification écrite au Sous-traitant [Data Processor] si ce dernier commet une violation substantielle ou persistante du présent ATD qui, dans le cas d'une violation à laquelle il est possible de remédier, n'a pas été corrigée dans un délai de trente (30) jours ouvrables à compter de la date de réception par le Sous-traitant [Data Processor] d'une notification du Responsable du traitement identifiant la violation et exigeant qu'il y soit remédié.

5.4 Le Sous-traitant [*Data Processor*] aura le droit de résilier le présent ATD par notification écrite au Responsable du traitement des données si ce dernier commet une violation substantielle ou persistante du présent ATD qui, dans le cas d'une violation à laquelle il est possible de remédier, n'a pas été corrigée dans les trente (30) jours ouvrables à compter de la date de réception par le Responsable du traitement d'une notification du Sous-traitant [*Data Processor*] identifiant la violation et exigeant qu'il y soit remédié.

6. AUDITS ET DEMANDES D'INFORMATION

6.1. Dans la limite d'un (1) audit par an et sous réserve de la notification par le Responsable de traitement avec préavis de trente (30) jours, sauf en cas d'audit demandé par une autorité de contrôle, le Responsable de traitement peut, pendant les heures ouvrables régulières, sans interférer de manière déraisonnable avec les opérations commerciales du Sous-traitant [*Data Processor*], auditer personnellement le Sous-traitant [*Data Processor*] ou nommer un auditeur tiers soumis à des obligations de confidentialité pour effectuer cet audit.

6.2. Le Sous-traitant [*Data Processor*] doit coopérer dans le cas d'un audit en vertu du présent article 6 et fournir au Responsable du traitement toutes les informations nécessaires pour effectuer cet audit. Le Responsable du traitement fera son affaire des coûts et dépenses encourus par chaque partie en relation avec les audits en vertu du présent article 6.

7. DÉSIGNATION DE SOUS-TRAITANTS

7.1 Le Responsable du traitement autorise le Sous-traitant [*Data Processor*] à recourir aux services de Sous-traitants [*Subprocessors*] répertoriés sur la page accessible à l'adresse [<https://www.lincolnelectric.com/en/Legal-Information/Subprocessors>], uniquement dans la mesure nécessaire à l'exécution des Services en rapport avec le CLUF.

7.2 Le Responsable du traitement autorise le Sous-traitant [*Data Processor*] à recourir aux services de nouveaux Sous-traitants [*Subprocessors*], sous réserve d'une notification préalable au Responsable du traitement par le Sous-traitant [*Data Processor*] moyennant un préavis de quinze (15) jours avant le changement de Sous-traitant [*Subprocessor*]. Si le Responsable du traitement s'oppose au changement de Sous-traitant [*Subprocessor*] notifié, le Responsable du traitement peut, pendant toute la durée du préavis, résilier le présent ATD par écrit. Si le Responsable du traitement ne résilie pas dans le délai de préavis, cela formalise le consentement du Responsable du traitement au changement notifié de Sous-traitant [*Subprocessor*].

7.3 En tout état de cause, lorsque le Sous-traitant [*Data Processor*] a recours aux services d'un Sous-traitant [*Subprocessor*] ultérieur, ce dernier sera, par contrat, tenu de se conformer aux mêmes obligations que celles auxquelles le Sous-traitant [*Data Processor*] est lié en termes de traitement des Données personnelles en vertu du présent ATD.

8. STIPULATIONS DIVERSES

8.1 Les modifications ou ajouts à cet ATD doivent être faits par écrit pour entrer en vigueur. Nonobstant ce qui précède, le Sous-traitant [*Data Processor*] peut, à tout moment et sans préavis au Responsable du traitement des données, modifier les mesures techniques, physiques et organisationnelles énoncées à l'annexe 2, à condition que cette modification n'ait pas d'impact important sur la sécurité, la confidentialité ou l'intégrité des Données personnelles.

8.2 Les références dans le présent ATD à « par écrit » ou « écrit » incluent les communications par courrier électronique et les lettres recommandées.

8.3 Si une disposition de cet ATD est ou devient invalide, cela n'affectera pas la validité des stipulations restantes. En cas d'annulation d'une stipulation du présent ATD, les Parties s'efforceront, dans tous les cas, de bonne foi, de remplacer la stipulation annulée par une autre, exécutoire, valide et licite, ayant dans toute la mesure du possible un impact juridique égal ou équivalent à celui de la stipulation initiale.

8.4 Cet ATD est régi par la même loi applicable que le CLUF.

ANNEXE 1 - CONDITIONS SPÉCIFIQUES À LA JURIDICTION

Lorsque le Responsable du traitement est établi dans l'une des juridictions énumérées dans la présente annexe 1, les conditions suivantes s'appliquent à l'ATD, et ces conditions prévaudront en cas de conflit avec les autres stipulations de l'ATD. Tous les termes du CLUF qui ne sont pas spécifiquement modifiés par les termes spécifiques à la juridiction applicables dans cette Annexe restent inchangés, en vigueur et de plein effet.

Brésil :

Les Parties reconnaissent et conviennent que la modification suivante s'applique à l'ATD :

- a) Toutes les occurrences de « Catégories spéciales de Données personnelles » dans l'ATD seront remplacées par « Données personnelles sensibles ».

Mexique :

Les Parties reconnaissent et conviennent que les modification suivantes s'appliquent à l'ATD :

- a) Toutes les occurrences de « Catégories spéciales de Données personnelles » dans l'ATD seront remplacées par « Données personnelles sensibles » ;
- b) Pour l'application des clauses contractuelles types, toutes les références à des « transferts » de Données personnelles doivent être interprétées comme des remises de données personnelles conformément à la loi fédérale mexicaine sur la protection des données personnelles détenues par des parties privées (« *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* »).

Russie :

Outre les stipulations de l'ATD, les Parties s'engagent à ce qui suit :

- a) Le Sous-traitant [*Data Processor*] confirme par la présente qu'il est pleinement conscient que le but des activités de Traitement des Données personnelles conformément à l'ATD est uniquement de fournir les Services de traitement et qu'il ne traitera les Données personnelles qu'aux fins pour lesquelles elles sont communiquées, et le Responsable du traitement l'exige du Sous-traitant [*Data Processor*]. En outre, le Sous-traitant [*Data Processor*] confirmera par écrit, dans les plus brefs délais à la demande du Responsable du traitement, que cette règle est respectée.
- b) Avant de communiquer les Données personnelles provenant de ressortissants russes au Sous-traitant [*Data Processor*], le Responsable du traitement doit s'assurer que toutes ces Données personnelles ont été enregistrées, systématisées, accumulées, stockées, clarifiées (mises à jour, modifiées) et extraites à l'aide de bases de données situées sur le territoire de la Fédération de Russie lorsque ces Données personnelles ont été collectées de quelque manière que ce soit, y compris via Internet.
- c) Si le Responsable du traitement détecte un traitement illicite ou une inexactitude des Données personnelles, il doit immédiatement demander au Sous-traitant [*Data Processor*] de bloquer ces Données personnelles et de lancer une inspection. Les Données personnelles concernées seront bloquées pendant toute la période d'inspection. Si l'inspection confirme l'inexactitude des Données personnelles, le Responsable du traitement demandera les modifications à la Personne concernée (ou son représentant) ou à l'autorité de protection des données (le cas échéant) et les transmettra au Sous-traitant [*Data Processor*]. Les Données personnelles inexacts seront modifiées dans les plus brefs délais, et au plus tard dans les sept (7) jours ouvrables à compter du jour où les modifications ont été transmises au Sous-traitant [*Data Processor*]. Les Données Personnelles seront débloquées immédiatement après modification.
- d) S'il est détecté que les Données personnelles font l'objet d'un traitement illicite, le Responsable du traitement doit demander au Sous-traitant [*Data Processor*] de mettre fin à ce traitement illicite dans les trois (3) jours ouvrables à compter de la date de détection. S'il s'avère impossible d'éliminer les violations et de garantir la licéité du traitement des Données personnelles, le Responsable du traitement demandera au Sous-traitant de détruire les Données personnelles traitées illégalement dans les dix (10) jours ouvrables à compter de la date de détection. Le Responsable du traitement est également tenu d'informer la Personne concernée (ou son représentant) et, lorsque la loi l'exige, l'autorité de protection des données, de l'élimination des violations.
- e) Si une Personne concernée révoque son consentement au traitement des Données personnelles, le Responsable du traitement en informera immédiatement le Sous-traitant, et ce dernier devra arrêter le traitement et détruire les Données personnelles de cette Personne concernée dans les trente (30) jours à compter de la réception par le Responsable du traitement de la notification d'annulation.

- f) S'il est impossible de respecter les délais prévus aux clauses d) et e) ci-dessus, le Sous-traitant [*Data Processor*] bloquera les Données personnelles concernées à la demande du Responsable du traitement pendant au plus six (6) mois et détruira ces Données personnelles dans le même délai, sauf disposition contraire de la loi applicable.

Afrique du Sud :

Les Parties reconnaissent et conviennent que les modifications suivantes apportées à l'ATD s'appliqueront aux définitions fournies à l'article 1 de l'ATD :

- a) « Personne concernée » désigne une personne dont les Données personnelles sont traitées.
- b) « Données personnelles » désigne les informations à caractère personnel telles que définies dans POPIA, y compris toute information relative à un individu identifié ou identifiable.
- c) « POPIA » désigne la Loi sud-africaine sur la protection des informations à caractère personnel Loi 4 de 2013 et tout règlement, toute directive, décision, injonction ou ordonnance contraignante en vertu de POPIA.

États-Unis :

Outre les stipulations de l'ATD, les Parties s'engagent à ce qui suit :

- a) Chaque Partie reconnaît et accepte que la collecte et la divulgation des Données personnelles transmises aux Services de traitement (i) ne constituent pas, et il n'est dans l'intention d'aucune des Parties qu'elles constituent, une vente de Données personnelles, et (ii) si une contrepartie de valeur, monétaire ou autre, est fournie par l'Utilisateur autorisé au Sous-traitant [*Data Processor*], cette contrepartie de valeur, monétaire ou autre, est ainsi fournie pour l'utilisation des Services de traitement et non pour la communication des Données personnelles. Le Sous-traitant [*Data Processor*] ne doit pas conserver, utiliser, divulguer ou vendre des Données personnelles à d'autres fins que dans le but spécifique d'exécuter les Services de traitement, ou comme l'autorisent la loi ou le CLUF. Pour éviter tout doute, le Sous-traitant [*Data Processor*] des données ne doit pas vendre de Données personnelles ni autoriser ou permettre à un Sous-traitant [*Subprocessor*] de procéder de la sorte, sauf autorisation contraire du CLUF ou de la loi applicable.

Annexe 2 - Mesures de sécurité mises en œuvre par le Sous-traitant [Data Processor]**1. Contrôle d'accès physique aux locaux et aux installations**

Le Sous-traitant [Data Processor] mettra en œuvre des mesures techniques et organisationnelles pour contrôler l'accès aux locaux et aux installations, en particulier pour vérifier l'autorisation afin d'assurer la prévention des accès non autorisés.

Spécifiquement :

- Système de contrôle d'accès
- Lecteur d'identité, carte magnétique, carte à puce
- Remise de clés
- Verrouillage des portes
- Personnel de sécurité, gardiens
- Installations de surveillance
- Système d'alarme, moniteur vidéo/CCTV

2. Contrôle d'accès aux systèmes

Le Sous-traitant [Data Processor] mettra en œuvre des mesures techniques (sécurité des identifiants/mots de passe) et organisationnelles pour l'identification et l'authentification des utilisateurs afin d'empêcher l'accès non autorisé aux systèmes informatiques.

Spécifiquement :

- Procédures de mot de passe (y compris caractères spéciaux, longueur minimale, changement de mot de passe)
- Blocage automatique (par exemple, mot de passe ou délai d'attente)
- Cryptage des supports de données, y compris amovibles et portables.

3. Contrôle d'accès logique aux données

Le Sous-traitant [Data Processor] s'assurera que les activités des systèmes informatiques non couvertes par les droits d'accès attribués seront empêchées en utilisant une définition axée sur les exigences du régime d'autorisation et des droits d'accès, ainsi qu'en surveillant et en enregistrant les accès.

Spécifiquement :

- Droits d'accès basés sur les rôles (profils, rôles, transactions et objets)
- Utilisation d'une solution commerciale de gestion des comptes privilégiés pour faciliter l'authentification sécurisée des comptes administratifs auprès des systèmes à des fins de maintenance ou à d'autres fins administratives
- Rapports automatisés qui sont régulièrement examinés et suivis en cas d'activité anormale ou suspecte
- Accès, en utilisant un modèle de moindre privilège, pour autoriser uniquement l'accès aux systèmes et/ou aux données en fonction du besoin de savoir

4. Contrôle de la communication et de la protection des données

Le Sous-traitant [Data Processor] contrôlera la communication des Données personnelles en incorporant des mesures pour transporter, transmettre et communiquer ou stocker des données sur des supports de données (manuels ou électroniques) et pour vérification ultérieure via le transfert électronique, le transport de données et le contrôle des transmissions.

Spécifiquement :

- Cryptage/tunnelage
- Signature électronique
- Journalisation et surveillance continue des événements de sécurité et des alertes
- Sécurité du transport pour chiffrer les données en transit
- Cryptage des données au repos
- Rotation régulière des clés de chiffrement
- Restriction de l'accès aux clés de chiffrement à des personnes limitées
- Complexité du mot de passe activée, avec authentification à deux facteurs requise pour toutes les sessions d'accès à distance

5. Contrôle des saisies

Le Sous-traitant [*Data Processor*] conservera une documentation complète de la gestion et de la maintenance des données, y compris des mesures permettant de vérifier ultérieurement si des données ont été saisies, modifiées ou supprimées (effacées) et par qui :

Spécifiquement :

- Systèmes de journalisation et de rapport

6. Contrôle des tâches

Le Sous-traitant [Data Processor] traitera les Données personnelles conformément aux instructions du Responsable du traitement et acceptera des mesures (techniques/organisationnelles) pour séparer les responsabilités entre le Responsable du traitement et le Sous-traitant [*Data Processor*] : Spécifiquement :

- Libellé non ambigu du contrat
- Mise en service formelle (formulaire de demande)
- Critères de sélection du Sous-traitant [*Data Processor*]
- Suivi de l'exécution du contrat

7. Contrôle des disponibilités

Le Sous-traitant [*Data Processor*] veillera à ce que les données soient protégées contre la destruction ou la perte accidentelle ou malveillante, en prenant des mesures pour assurer la sécurité physique et logique des données.

Spécifiquement :

- Procédures de sauvegarde
- Mise en miroir des disques durs, par exemple la technologie RAID
- Alimentation sans interruption (UPS)
- Stockage à distance ou sur disque qui est répliqué vers d'autres centres de données
- Logiciels antivirus et/ou anti-programmes malveillants mis à jour régulièrement et systèmes de pare-feu compatibles avec les applications configurés avec des instructions de refus par défaut, autorisant uniquement le trafic explicitement autorisé à des fins commerciales
- Plan de continuité opérationnelle et de reprise après sinistre

8. Contrôle de la ségrégation

Le Sous-traitant [*Data Processor*] cherchera à faire en sorte que les données collectées à des fins différentes soient traitées séparément et ne soient pas mélangées avec d'autres données client, en mettant en œuvre des mesures spécifiques pour permettre un traitement séparé (stockage, modification, suppression, transmission) des données à des fins différentes :

Spécifiquement :

- Notion de « client interne » / limitation d'utilisation
- Séparation des fonctions (production/tests)