Le présent document énonce la politique de confidentialité de « K » Line Logistics France (la « Société »). Il remplace toutes les politiques de confidentialité adoptées avant le 25 mai 2018.

Vous devez impérativement lire cette politique car elle vous offre des informations importantes concernant :

- les principes de confidentialité auxquels la Société doit se conformer ;
- la définition du terme « informations (ou données) à caractère personnel » et « informations (ou données) sensibles à caractère personnel » ;
- la manière dont nous recueillons, utilisons et (en dernière instance) supprimons les informations à caractère personnel et informations sensibles à caractère personnel conformément aux principes de confidentialité ;
- l'endroit où vous pouvez trouver des informations de confidentialité plus détaillées, p.ex. sur les informations à caractère personnel que nous recueillons et utilisons à votre sujet, la manière dont elles sont utilisées, stockées et transférées et à quelles fins, les démarches accomplies pour assurer la sécurité de ces informations et la durée pour laquelle elles sont conservées ;
- vos droits et obligations concernant la confidentialité ; et
- les conséquences du non-respect de la présente politique.

Le Responsable de la protection des données de la Société est Darren Smith.

Veuillez confirmer avoir lu et compris la présente politique en signant et retournant la copie ci-jointe au Responsable de la protection des données.

1 Introduction

1.1 La Société obtient, conserve et utilise des informations à caractère personnel (également dénommées « données ») concernant les postulants et les membres du personnel passés et actuels, notamment les employés, employés temporaires et intérimaires, stagiaires, travailleurs bénévoles et apprentis pour un certain nombre de motifs légaux spécifiques, comme indiqué dans les avis de confidentialité des données relatifs au recrutement et à l'emploi.

1.2 La présente politique décrit la manière dont nous respectons nos obligations de confidentialité et nous employons à protéger les informations à caractère personnel concernant notre main d'œuvre. Elle vise à s'assurer que les personnels comprennent et se conforment aux règles régissant la collecte, l'utilisation et la suppression des informations à caractère personnel auxquelles ces personnes pourraient avoir accès au cours de leurs activités.

1.3 Nous nous engageons à respecter nos obligations de confidentialité et à faire preuve de concision, clarté et transparence concernant la manière dont nous obtenons et utilisons les informations à caractère personnel au sujet de notre main d'œuvre et la manière dont nous supprimons ces informations lorsque leur conservation n'est plus nécessaire (et le moment où nous procédons à cette suppression).

1.4 Le Responsable de la confidentialité de la Société est chargé d'informer et de conseiller la Société et son personnel sur ses obligations de confidentialité ainsi que de contrôler le respect de ces obligations et des politiques de la Société. En cas de question ou de commentaire sur le contenu de cette politique ou pour toute demande de renseignement complémentaire, nous vous conseillons de contacter le Responsable de la confidentialité par e-mail (pcourgenouil@fr.klinelogistis.com), par téléphone (+33(0)148620636) ou par courrier.

2 Portée

2.1 La présente politique s'applique aux informations à caractère personnel des postulants et des membres du personnel passés et actuels, notamment les employés, employés temporaires et intérimaires, stagiaires, travailleurs bénévoles et apprentis.

2.2 Le personnel doit consulter l'avis de confidentialité des données de la Société et, le cas échéant, ses autres politiques pertinentes, notamment celles qui s'appliquent à Internet, aux e-mails et communications, au suivi, aux médias sociaux, à la sécurité des informations, à la conservation des données, aux dispositions bring your own device (BYOD, appareils personnels) et aux informations de casier judiciaire, qui contiennent des renseignements complémentaires concernant la confidentialité des informations à caractère personnel dans ce contexte.

2.3 Nous assurerons régulièrement la révision et la mise à jour de la présente politique, conformément à nos obligations de confidentialité. Elle ne fait pas partie du contrat de travail des employés et nous nous réservons le droit de la modifier, mettre à jour ou compléter de temps à autre. Nous diffuserons au personnel toute politique nouvelle ou modifiée lorsqu'elle sera adoptée.

3 Définitions

le terme « informations de casier judiciaire »	désigne les informations à caractère personnel liées aux condamnations pénales et aux délits, allégations, procédures et mesures de sécurité connexes ;
le terme « violation des données »	désigne une violation de sécurité entraînant la destruction, la perte ou la modification illégale ou accidentelle d'informations à caractère personnel ou leur divulgation ou consultation non autorisées ;
le terme « sujet de données »	désigne la personne sur laquelle portent les informations à caractère personnel ;
le terme « informations à caractère personnel »	(parfois dénommées « données à caractère personnel ») désigne les informations relatives à une personne qui peut être identifiée (directement ou indirectement) à partir de ces informations ;
le terme « informations de traitement »	désigne l'obtention, l'enregistrement, l'organisation, le stockage, la modification, la récupération, la divulgation et/ou la destruction des informations
le terme « pseudonymisé »	désigne le processus par lequel les informations à caractère personnel sont traitées de manière à ne pas pouvoir être utilisées pour identifier une personne sans avoir à utiliser d'informations complémentaires conservées dans un lieu séparé et soumises à des mesures techniques et organisationnelles conçues pour s'assurer que les informations à caractère personnel ne peuvent être reliées à un individu identifiable ;
le terme « informations sensibles à caractère personnel »	(parfois dénommées « catégories spéciales de données à caractère personnel » ou « données sensibles à caractère personnel ») désigne les informations à caractère personnel concernant la race, l'origine ethnique, les opinions politiques ou l'obédience religieuse ou philosophique d'une personne, l'adhésion (ou la non-adhésion) à un syndicat, les informations génétiques, les informations biométriques (lorsqu'elles sont utilisées pour identifier une personne) et les

informations concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne.

1 Principes de confidentialité

1.1 La Société respectera les principes de confidentialité suivants lors du traitement des informations à caractère personnel :

1.1.1 nous traiterons les informations à caractère personnel de manière légale, équitable et transparente ;

1.1.2 nous recueillerons les informations à caractère personnel à des fins spécifiques, explicites et légitimes uniquement et nous abstiendrons de les traiter d'une manière incompatible avec ces fins légitimes ;

1.1.3 nous traiterons uniquement les informations à caractère personnel adéquates, pertinentes et nécessaires aux fins concernées ;

1.1.4 nous conserverons des informations à caractère personnel exactes et à jour et accomplirons des démarches raisonnables pour nous assurer que les informations à caractère personnel inexactes sont supprimées ou rectifiées sans délai ;

1.1.5 nous nous abstiendrons de conserver les informations à caractère personnel sous une forme permettant d'identifier les sujets de données pour une période plus longue que nécessaire aux fins auxquelles les informations sont traitées ; et

1.1.6 nous mettrons en œuvre les mesures techniques et organisationnelles nécessaires pour nous assurer que les informations à caractère personnel sont en sécurité et protégées contre un traitement illégal ou interdit et contre la perte, la destruction ou les dommages accidentels.

2 Motif du traitement des informations à caractère personnel

2.1 S'agissant de toute activité de traitement, avant le commencement du traitement pour la première fois, puis de manière régulière au cours du traitement, nous nous engageons à :

2.1.1 revoir les objectifs de l'activité de traitement spécifique et sélectionner le motif (ou les motifs) légaux les plus adéquats pour ce traitement, c.-à-d. :

(a) le fait que le sujet de données ait consenti au traitement ;

(b) le fait que le traitement soit nécessaire pour exécuter un contrat auquel le sujet de données est partie ou en vue d'accomplir des démarches demandées par le sujet de données avant la conclusion d'un contrat ;

(c) le fait que le traitement soit nécessaire pour se conformer à une obligation légale à laquelle la Société est soumise ;

(d) le fait que le traitement soit nécessaire pour la protection des intérêts vitaux du sujet de données ou d'une autre personne physique ;

(e) le fait que le traitement soit nécessaire pour observer les intérêts légitimes de la Société ou d'un tiers, sauf si les droits et libertés fondamentales du sujet de données priment sur ces intérêts (voir la clause 5.2 ci-dessous).

2.1.2 sauf si le traitement se fonde sur le consentement, nous assurer que le traitement est nécessaire aux fins du motif légal concerné (c.-à-d. il n'existe pas d'autre manière raisonnable d'atteindre cet objectif) ;

2.1.3 documenter notre décision sur le motif légal qui doit s'appliquer afin de contribuer à démontrer notre conformité aux principes de confidentialité ;

2.1.4 inclure des informations sur les objectifs du traitement et le motif légal qui le sous-tend dans nos avis de confidentialité pertinents ;

2.1.5 si des informations sensibles à caractère personnel sont traitées, indiquer également une condition spéciale légale de traitement de ces informations (voir le paragraphe 6.2.2 ci-dessous) et la documenter ; et

2.1.6 si des informations sur les condamnations pénales sont traitées, indiquer également une condition légale du traitement de ces informations et la documenter.

2.2 Pour déterminer si les intérêts légitimes de la Société constituent le motif le plus adéquat du traitement légal, nous nous emploierons à :

2.2.1 réaliser une évaluation des intérêts légitimes (EIL) et à en conserver un enregistrement pour nous assurer de pouvoir justifier notre décision ;

2.2.2 si l'EIL permet de détecter un impact de confidentialité significatif, envisager de mener également une évaluation de l'impact de confidentialité (EIC) ;

2.2.3 réviser régulièrement l'EIL et en effectuer une nouvelle en cas d'évolution de la situation ; et

2.2.4 inclure des informations sur nos intérêts légitimes dans notre(nos) avis de confidentialité pertinent(s).

3 Informations sensibles à caractère personnel

3.1 Les informations sensibles à caractère personnel sont parfois dénommées « catégories spéciales de données à caractère personnel » ou « données sensibles à caractère personnel ».

3.2 La Société pourrait, de temps à autre, avoir besoin de traiter des informations sensibles à caractère personnel ; Nous traiterons les informations sensibles à caractère personnel uniquement si :

3.2.1 nous disposons d'un motif légal à cet effet, comme prévu au paragraphe 5.1.1 ci-dessus, p.ex. ceci est nécessaire en vue de l'exécution du contrat de travail, pour permettre à la Société de s'acquitter de ses obligations légales ou pour préserver les intérêts légitimes de la Société ; et

3.2.2 l'une des conditions spéciales du traitement d'informations sensibles à caractère personnel s'applique, p.ex. :

(a) le sujet de données y a explicitement consenti ;

(b) le traitement est nécessaire aux fins de l'exercice des droits conférés par la législation sur le travail ou de l'exécution des obligations prévues par la législation sur le travail et incombant à la Société ou au sujet de données ;

(c) Le traitement est nécessaire pour protéger les intérêts vitaux du sujet de données, lequel est physiquement incapable de donner son consentement ;

(d) le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par le sujet de données ;

(e) le traitement est nécessaire pour prouver, exercer ou se défendre contre une action en justice ; ou

(f) le traitement est nécessaire pour des motifs substantiels d'ordre public.

3.3 Avant de traiter les informations sensibles à caractère personnel, les employés doivent notifier le Responsable de la confidentialité du projet de traitement afin de permettre au Responsable de la confidentialité de déterminer si le traitement satisfait aux critères susvisés.

3.4 Les informations sensibles à caractère personnel ne seront pas traitées jusqu'à ce que :

3.4.1 l'évaluation visée au paragraphe 6.3 n'ait été réalisée ; et

3.4.2 la personne n'ait été dûment informée (par le biais d'un avis de confidentialité ou autre) de la nature du traitement, des fins auxquelles il est effectué et de son motif légal.

3.5 L'avis de confidentialité des données de la Société décrit les types d'informations sensibles à caractère personnel traitées par la Société, les fins auxquelles elles sont utilisées et le motif légal du traitement.

3.6 Relativement aux informations sensibles à caractère personnel, la Société respectera les procédures énoncées aux paragraphes 6.7 et 6.8 ci-dessous pour s'assurer qu'elles respectent les principes de confidentialité des données prévus au paragraphe 4 ci-dessus.

3.7 **Au cours de la procédure de recrutement** : le service des ressources humaines, s'appuyant sur les orientations du Responsable de la confidentialité, s'assurera de ce qui suit (sauf si la loi en dispose autrement) :

3.7.1 aux étapes de présélection, d'entretien et de prise de décision, aucune question ne soit posée concernant les informations sensibles à caractère personnel, p.ex. race ou origine ethnique, appartenance à un syndicat ou état de santé ;

3.7.2 si des informations sensibles à caractère personnel sont reçues, p.ex. le postulant les fournit de manière non sollicitée dans son CV ou au cours de l'entretien, aucun enregistrement ne soit conservé à cet égard et toute référence à ces informations soit immédiatement supprimée ou rayée ;

3.7.3 tout formulaire de contrôle de l'égalité des opportunités rempli soit conservé dans un endroit séparé du formulaire de candidature de la personne concernée et ne soit pas consulté par la personne chargée de la présélection, de l'entretien ou de la décision de recrutement ;

3.7.4 Les vérifications de permis de travail soient exécutées avant l'envoi d'une offre d'emploi inconditionnelle et non pas au cours des étapes antérieures de présélection, d'entretien ou de prise de décision ;

3.7.5 nous ne posions aucune question sur la santé dans le cadre du recrutement.

3.8 **Au cours de l'emploi** : le service des RH, s 'appuyant sur les orientations du Responsable de la confidentialité, traitera ce qui suit :

3.8.1 les informations de santé, aux fins d'administrer les congés maladie, de tenir à jour les dossiers de congé maladie, de contrôler la présence des personnels et d'organiser les prestations de santé et de maladie liées à l'emploi ;

3.8.2 des informations sensibles à caractère personnel, aux fins du contrôle de l'égalité des opportunités et de l'établissement de rapports sur l'égalité des salaires entre les hommes et les femmes. Si possible, ces informations seront anonymisées ; et

3.8.3 des informations d'adhésion à un syndicat, aux fins de l'administration du personnel ou de l'administration des cotisations.

4 Informations de casier judiciaire

Les informations de casier judiciaire ne seront traitées que lorsqu'elles auront été approuvées par le Responsable de la confidentialité.

5 Évaluations de l'impact de la confidentialité des données (EICD)

5.1 S'il est probable que le traitement fasse peser un risque élevé sur les droits de confidentialité d'une personne (p.ex. lorsque la Société prévoit d'utiliser une nouvelle forme de technologie), nous exécuterons une EICD avant de démarrer le traitement afin d'évaluer ce qui suit :

5.1.1 le fait que le traitement soit ou non nécessaire et proportionnel à son objectif ;

5.1.2 les risques qu'il fait peser sur les personnes ; et

5.1.3 les mesures pouvant être mises en place pour résoudre ces risques et protéger les informations à caractère personnel.

5.2 Avant l'introduction de toute nouvelle forme de technologie, le responsable devrait donc contacter le Responsable de la confidentialité afin de procéder à la réalisation d'une EICD.

5.3 Au cours de toute EICD, l'employeur s'appuiera sur les conseils du Responsable de la confidentialité ainsi que les avis des employés et de toute autre partie prenante concernée.

6 Documentation et dossiers

6.1 Nous conserverons des enregistrements écrits des activités de traitement à haut risque, c.-à-d. pouvant entraîner un risque pour les droits et libertés individuels ou porter sur des informations sensibles ou informations de casier judiciaire, notamment :

6.1.1 le nom et les coordonnées de l'organisation de l'employeur (et, le cas échéant, des responsables du traitement, du représentant de l'employeur et du délégué à la protection des données) ;

6.1.2 les objectifs du traitement ;

6.1.3 une description des catégories de personnes et des catégories de données à caractère personnel ;

6.1.4 les catégories de destinataires des données à caractère personnel ;

6.1.5 le cas échéant, le détail des transferts vers des pays tiers, notamment la documentation sur les mesures de protection des mécanismes de transfert mises en œuvre ;

6.1.6 le cas échéant, les calendriers de conservation ; et

6.1.7 le cas échéant, une description des mesures de sécurité techniques et organisationnelles.

6.2 Dans le cadre de notre dossier d'activités de traitement, nous documentons ou établissons des liens vers les éléments suivants :

6.2.1 informations requises pour les avis de confidentialité ;

6.2.2 registres de consentement ;

6.2.3 contrats responsable du traitement-sous-traitant ;

6.2.4 emplacement où sont stockées les informations à caractère personnel ;

6.2.5 EIC ; et

6.2.6 dossiers de violations des données.

6.3 Si nous traitons des informations sensibles à caractère personnel ou des informations de casier judiciaire, nous conservons des dossiers consignant les éléments suivants :

6.3.1 l'objectif ou les objectifs pour lequel ou lesquels le traitement a lieu, notamment (le cas échéant) la raison pour laquelle il est nécessaire à cette fin ;

6.3.2 le motif légal de notre traitement ; et

6.3.3 le fait que nous conservions et effacions les données à caractère personnel conformément à notre politique et, si ce n'est pas le cas, les motifs du non-respect de notre politique.

6.4 Nous mènerons des examens réguliers des informations à caractère personnel que nous traitons et mettrons à jour notre documentation en conséquence. Ceci peut inclure :

6.4.1 exécuter des audits sur les informations pour déterminer quelles sont les informations à caractère personnel détenues par la Société ;

6.4.2 distribuer des questionnaires et mener des entretiens avec les employés dans l'ensemble de la Société pour obtenir une vision plus complète de nos activités de traitement ; et

6.4.3 revoir nos politiques, procédures, contrats et accords pour résoudre des questions telles que la conservation des données, la sécurité et le partage des données.

6.5 Nous documentons nos activités de traitement sous forme électronique, ce qui nous permet d'ajouter, de supprimer et de modifier les informations facilement.

7 Avis de confidentialité

7.1 La Société émettra de temps à autre des avis de confidentialité vous indiquant quelles informations à caractère personnel nous recueillons et détenons à votre sujet ainsi que la manière dont vos informations à caractère personnel peuvent être utilisées et à quelles fins.

7.2 Nous mettrons en œuvre les mesures nécessaires pour fournir les informations figurant dans nos avis de confidentialité sous une forme concise, transparente, intelligible et facile d'accès, en utilisant une formulation simple et claire.

8 Droits individuels

8.1 Vous (ainsi que les autres sujets de données) disposez des droits ci-après en ce qui concerne vos informations à caractère personnel :

8.1.1 droit d'être informé de la manière, de la raison pour laquelle et du fondement sur lequel les informations sont traitées (consultez l'avis de confidentialité des données de la Société) ;

8.1.2 droit d'obtenir confirmation que vos informations font l'objet d'un traitement et d'obtenir un accès à ces informations et certaines autres en déposant une demande d'accès du sujet de données (consultez la politique de demande d'accès du sujet de données de la Société) ;

8.1.3 droit de faire rectifier les données si celles-ci sont inexactes ou incomplètes ;

8.1.4 droit de faire supprimer les données si celles-ci ne sont plus nécessaires aux fins auxquelles elles avaient été recueillies/traitées initialement ou s'il n'existe pas de motif légitime impérieux pour le traitement (ceci est parfois dénommé le « droit à l'oubli ») ;

8.1.5 droit de limiter le traitement des données à caractère personnel lorsque l'exactitude des informations est contestée ou lorsque le traitement est illégal (mais que vous ne souhaitez pas la suppression des données) ou lorsque l'employeur n'a plus besoin des informations à caractère personnel mais que vous avez besoin des données pour prouver, exercer ou vous défendre contre une action en justice ; et

8.1.6 droit de limiter provisoirement le traitement des informations à caractère personnel lorsque vous estimez qu'elles ne sont pas exactes (et que l'employeur vérifie leur exactitude) ou lorsque vous vous opposez au traitement (et que l'employeur évalue si les motifs légitimes de l'organisation priment sur vos intérêts).

8.2 Si vous souhaitez exercer tout droit prévu aux paragraphes 11.1.3 à 11.1.6, veuillez contacter le Responsable de la confidentialité.

9 Obligations individuelles

9.1 Il incombe aux sujets de données d'aider la Société à tenir leurs informations à caractère personnel à jour. Vous devriez aviser le service des RH en cas de modification des informations fournies à la Société, par exemple si vous déménagez ou si vous souhaitez être payé sur un compte ayant des coordonnées bancaires différentes.

9.2 Au cours de votre emploi ou mission, vous pourriez avoir accès aux informations à caractère personnel d'autres employés, fournisseurs et clients de la Société. Si tel est le cas, la Société attend de vous que vous respectiez les obligations de confidentialité qui lui incombent vis-à-vis de ces personnes. Par exemple, vous devriez également avoir conscience qu'elles pourraient bénéficier des droits prévus au paragraphe 11.1 ci-dessus.

9.3 Si vous avez accès à des informations à caractère personnel, vous devez :

9.3.1 accéder uniquement aux informations à caractère personnel que vous avez l'autorisation de consulter, et uniquement aux fins autorisées ;

9.3.2 permettre aux autres employés de la Société d'accéder aux informations à caractère personnel uniquement s'ils disposent des autorisations adéquates ;

9.3.3 permettre aux personnes qui ne sont pas des employés de la Société d'accéder aux informations à caractère personnel uniquement si vous avez reçu spécifiquement l'autorisation de la faire par le Responsable de la confidentialité;

9.3.4 préserver la sécurité des informations à caractère personnel (p.ex. en respectant les règles relatives à l'accès aux locaux, l'accès aux ordinateurs, la protection des mots de passe et le stockage et la destruction sécurisés des fichiers ainsi que d'autres précautions prévues par la politique de sécurité des informations de la Société) ;

9.3.5 s'abstenir de retirer des informations à caractère personnel ou appareils contenant des informations à caractère personnel (ou pouvant être utilisés pour y accéder) des locaux de la Société sans la mise en place de mesures de sécurité adéquates (telles que la pseudonymisation, le chiffrage ou la protection des mots de passe) pour assurer la sécurité des informations et de l'appareil ; et

9.3.6 s'abstenir de stocker des informations à caractère personnel sur des disques locaux ou appareils personnels utilisés à des fins professionnelles.

9.4 Vous devriez contacter le Responsable de la confidentialité si vous êtes inquiet ou soupçonnez que l'une des choses suivantes a eu lieu (ou est en train d'avoir lieu, ou est susceptible d'avoir lieu) :

9.4.1 le traitement des données à caractère personnel sans fondement légal ou, dans le cas des informations sensibles à caractère personnel, alors que l'une des conditions prévues au paragraphe 6.2.2 n'est pas remplie ;

9.4.2 toute violation des données, comme prévu au paragraphe 15.1 ci-dessous ;

9.4.3 l'accès à des informations à caractère personnel sans autorisation en bonne et due forme ;

9.4.4 Des informations à caractère personnel non conservées ou non supprimées de manière sécurisée ;

9.4.5 Le retrait d'informations à caractère personnel ou d'appareils contenant des informations à caractère personnel (ou pouvant être utilisés pour y accéder) des locaux de la Société sans que celui-ci ne s'accompagne de mesures de sécurité adéquates ;

9.4.6 toute autre violation de la présente politique ou de tout principe de confidentialité visé au paragraphe 4.1 ci-dessus.

10 Sécurité des informations

10.1 La Société mettra en œuvre des mesures techniques et organisationnelles conformes aux politiques de la Société consistant à assurer la sécurité des informations à caractère personnel et, en particulier, à les protéger contre le traitement non autorisé ou illégal et contre toute perte, toute destruction ou tout dommage accidentel. Celles-ci peuvent inclure les éléments ci-après :

10.1.1 s'assurer que, si possible, les informations à caractère personnel sont pseudonymisées ou chiffrées ;

10.1.2 s'assurer de la confidentialité, de l'intégrité, de la disponibilité et de la résilience continues des systèmes et services de traitement ;

10.1.3 s'assurer qu'en cas d'incident physique ou technique, la disponibilité et l'accès aux informations à caractère personnel puissent être rétablis rapidement ; et

10.1.4 un processus permettant de tester, d'évaluer et de mesurer régulièrement l'efficacité des mesures techniques et organisationnelles permettant d'assurer la sécurité du traitement.

10.2 Lorsque la Société fait appel à des organisations externes pour traiter les informations à caractère personnel en son nom, des accords de sécurité complémentaires doivent être mis en œuvre dans les contrats conclus avec ces organisations afin de protéger la sécurité des

informations à caractère personnel. En particulier, les contrats conclus avec les organisations externes doivent prévoir que :

10.2.1 l'organisation ne peut agir que sur consigne écrite de la Société ;

10.2.2 les personnes chargées du traitement des données sont soumises à une obligation de confidentialité ;

10.2.3 des mesures adéquates sont mises en œuvre pour assurer la sécurité du traitement ;

10.2.4 des sous-traitants sont engagés uniquement avec le consentement préalable de la Société et dans le cadre d'un contrat écrit ;

10.2.5 l'organisation aidera la Société à fournir un accès aux données par les sujets de données et à permettre aux personnes d'exercer leurs droits en ce qui concerne la protection des données ;

10.2.6 l'organisation aidera la Société à respecter ses obligations concernant la sécurité du traitement, la notification des violations des données et les études d'impact de confidentialité ;

10.2.7 l'organisation supprimera ou restituera l'ensemble des informations à caractère personnel à la Société, comme exigé, à la fin du contrat ; et

10.2.8 l'organisation se pliera aux audits et inspections, fournira à la Société toutes les informations dont elle a besoin pour s'assurer qu'elles respectent toutes les deux leurs obligations de protection des données et informera la Société sans délai si on lui demande d'enfreindre la législation relative à la confidentialité.

10.3 Avant la conclusion de tout nouvel accord nécessitant le traitement d'informations à caractère personnel par une organisation externe ou la modification d'un accord existant, les employés concernés doivent le faire avaliser par le Responsable de la confidentialité.

11 Stockage et conservation des informations à caractère personnel

11.1 Les informations à caractère personnel (et informations sensibles à caractère personnel) seront conservées de manière sécurisée, conformément à la politique de sécurité des informations de la Société.

11.2 Les informations à caractère personnel (et informations sensibles à caractère personnel) ne doivent pas être conservées plus longtemps que nécessaire. La durée de conservation des données dépend de la situation et notamment des motifs d'obtention des informations à caractère personnel. Les employés doivent respecter la politique de conservation des dossiers de la Société qui fixe la période de conservation concernée ou les critères devant être utilisés pour fixer la période de conservation. La politique de conservation des dossiers a été jointe à l'Annexe 1. En cas d'incertitude, les employés doivent consulter le Responsable de la confidentialité.

11.3 Les informations à caractère personnel (et informations sensibles à caractère personnel) qui ne sont plus nécessaires seront supprimées de manière définitive de nos systèmes informatiques et toute copie papier de ces informations sera détruite de manière sécurisée.

12 Violations des données

12.1 Une violation des données peut prendre différentes formes, notamment :

12.1.1 la perte ou le vol des données ou équipements sur lesquels les informations à caractère personnel sont stockées ;

12.1.2 l'utilisation ou l'accès non autorisé aux informations à caractère personnel par un employé ou un tiers ;

12.1.3 la perte de données découlant d'une panne d'équipements ou de systèmes (notamment les matériels et logiciels) ;

12.1.4 une erreur humaine comme une suppression ou une modification accidentelle des données ;

12.1.5 des circonstances imprévues comme un incendie ou des inondations ;

12.1.6 des attaques volontaires des systèmes informatiques telles que des actes de hacking, des virus ou des cas de hameçonnage ; et

12.1.7 les délits de « blagging » dans le cadre desquels des informations sont obtenues en trompant l'organisation qui les détient.

12.2 La Société :

12.2.1 signalera comme il se doit les violations des données au bureau du Commissaire à l'information sans délai injustifié et, si possible, dans un délai de 72 heures après en avoir pris connaissance, si ces violations sont susceptibles de faire peser un risque sur les droits et libertés des personnes ; et

12.2.2 notifiera les personnes affectées si une violation des données est susceptible de faire peser un risque important sur leurs droits et libertés et si la notification est exigée par la loi.

12.3 Pour permettra à la Société de respecter les obligations que lui confère la clause 15.2, si vous prenez connaissance de toute violation des données réelle ou potentielle, vous devez impérativement en aviser sans délai votre responsable hiérarchique et le Responsable de la confidentialité.

13 Transferts internationaux

13.1 La Société pourrait transférer des informations à caractère personnel vers des pays situés hors de l'Espace économique européen (EEE) (qui comprend les pays de l'Union européenne ainsi que l'Islande, le Liechtenstein et la Norvège), par exemple vers le Japon, sur le fondement que ce pays, ce territoire ou cette organisation est doté(e) d'un niveau de protection adéquat ou que l'organisation offre des garanties adéquates en matière de protection par le biais de clauses standard de confidentialité.

14 Formation

La Société veillera à ce que les employés reçoivent une formation adéquate concernant leurs responsabilités en matière de confidentialité. Les personnes dont le rôle exige un accès régulier aux informations à caractère personnel ou qui sont responsables de la mise en œuvre de cette politique ou de la réponse aux demandes d'accès des sujets de données en vertu de la présente politique recevront une formation supplémentaire pour les aider à comprendre leur mission et la manière de l'accomplir.

15 Conséquences du non-respect

15.1 La Société accorde beaucoup d'importance au respect de la présente politique. Le non-respect de la politique :

15.1.1 fait courir un risque aux personnes dont les informations à caractère personnel sont traitées ; et

15.1.2 entraîne un risque de sanctions civiles et pénales importantes pour la personne et pour la Société ; et

15.1.3 peut, dans certains cas, constituer un délit pénal commis par la personne.

15.2 En raison de l'importance de la présente politique, le non-respect par un employé de toute disposition pourrait donner lieu à une action disciplinaire en vertu de nos procédures et cette action pourrait entraîner un licenciement pour faute grave. En cas de violation de la présente politique par un non-employé, le contrat de la personne à l'origine de la violation pourrait être résilié avec effet immédiat.

15.3 En cas de question ou de préoccupation concernant toute disposition de la présente politique, n'hésitez pas à contacter le Responsable de la confidentialité.

Annexe 1 - conservation des registres

Ce calendrier de conservation des registres est joint et intégré à la politique de protection des données de la Société. Il fixe les durées de conservation des différents types de documents à des fins commerciales et légales. C'est un document volumineux qui énumère les nombreux types de dossiers utilisés par la société ainsi que les périodes de conservation applicables à chaque type de dossier.

Les périodes de conservation se basent sur les besoins commerciaux et les exigences légales. Si vous conservez tout type de dossier non visé dans cette annexe et que cette dernière ne stipule pas clairement quelle période de conservation s'applique à ce type de dossier, veuillez contacter le Responsable de la confidentialité pour obtenir ses conseils.

Toute non-application des périodes de conservation prévues dans la présente annexe doit être approuvée à l'avance par le Responsable de la confidentialité.

Les données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire pour atteindre les objectifs pour lesquels elles ont été recueillies. Toute donnée à caractère personnelle recueillie qui n'est pas expressément visée ci-dessous doit être examinée avec soin et éliminée en toute sécurité si elle n'est plus nécessaire, par exemple lorsqu'un employé quitte la Société.

Les sections 1 à 3 portent sur les données relatives aux employés. La section 4 porte sur les clients.

Dossiers relatifs à l'emploi

1. Dossiers du personnel

Dossier	**Période de conservation recommandée**	**Format de stockage**
Dossiers relatifs aux postulants rejetés, notamment : • lettres/formulaires de candidature • CV • recommandations • notes prises au cours de l'entretien	6 mois après la notification de rejet envoyée au candidat	papier/électronique
• Dossiers de candidature des candidats retenus, notamment : • formulaires de candidature des candidats retenus • Copies des diplômes et certificats de formation reçus • recommandations • correspondance concernant l'emploi • CV • notes prises au cours de l'entretien et formulaires d'évaluation • évaluation et tests psychologiques et résultats de ces tests	6 ans à compter de la fin du contrat de travail	Papier/électronique
Informations de casier judiciaire : • évaluations des exigences relatives aux casiers judiciaires pour un poste spécifique	L'évaluation des exigences relatives aux casiers judiciaires pour un poste spécifique (12 mois après la dernière évaluation) Toutes les autres informations de	Papier ou électronique

Dossier	**Période de conservation recommandée**	**Format de stockage**
• formulaires d'informations sur les casiers judiciaires • formulaires de vérification du Disclosure and Barring Service (DBS) • Les certificats DBS	cette catégorie (dès que possible après la vérification et l'enregistrement du résultat, c'est-à-dire le fait que la vérification ait abouti sur un résultat positif ou non) sauf si, dans des circonstances exceptionnelles, le directeur de la confidentialité détermine qu'elles sont clairement pertinentes pour la continuation de la relation d'emploi, p.ex. pour permettre d'examiner et de résoudre tout litige ou toute plainte, auquel cas, six mois Si le directeur de la confidentialité considère qu'il est nécessaire de conserver les informations pour une période supérieure à six mois, le DBS doit être consulté	
Contrats de travail, notamment : • les dossiers sur les employés et formations • les descriptions de poste écrites • les modifications apportées aux conditions générales	6 ans à compter de la fin du contrat de travail	Papier/électronique

Dossier	**Période de conservation recommandée**	**Format de stockage**
les copies des documents d'identité (p.ex. passeports)	6 ans à compter de la fin du contrat de travail	Papier/électronique
les documents d'identité des ressortissants étrangers (notamment les permis de travail)	2 ans à compter de la date de résiliation du contrat de travail	Papier/électronique
Dossiers concernant un travailleur temporaire	6 ans à compter de la fin du contrat de travail	Papier/électronique
Dossiers relatifs à la performance de l'employé • évaluations réalisées à la fin d'une période d'essai • entretiens et réunions d'évaluation • évaluations • promotions et rétrogradations	6 ans à compter de la fin du contrat de travail	Papier/électronique
Dossiers relatifs au Règlement sur le temps de travail de 1998 ou prouvant le respect dudit Règlement, notamment : • enregistrement des périodes de travail et de repos • formulaires de renonciation aux dispositions favorables sur le temps de travail	2 ans à compter de la date de création du dossier	Papier/électronique
Dossiers de licenciement	6 ans à compter de la date du licenciement	Papier/électronique
Dossier sur les congés annuels	6 ans à compter de la fin de chaque exercice fiscal	Papier/électronique

Dossier	Période de conservation recommandée	Format de stockage
Dossiers sur les congés maternité et paternité	6 ans à compter de la fin de chaque exercice fiscal	Papier/électronique
Dossiers sur les maladies	6 ans à compter de la fin de chaque exercice fiscal	Papier/électronique
Dossiers sur les réunions de retour au travail à la suite d'un congé maladie, maternité, etc.	6 ans à compter de la fin de chaque exercice fiscal	Papier/électronique

2. Dossiers sur les salaires et fiches de paie

Palmarès	Période de conservation recommandée	Format de stockage
Dossiers conservés aux fins des déclarations fiscales, notamment les dossiers sur les salaires et les dossiers sur les heures supplémentaires, le primes et les dépenses	6 ans	Papier/électronique
Dossiers relatifs à l'imposition à la source, notamment : • les feuilles de salaire • les fiches de déduction • calcul du revenu imposé à la source des employés et paiements y relatifs	3 ans	Papier/électronique
déclarations d'impôt sur le revenu et de cotisation d'assurance et correspondance avec HMRC (Trésor britannique)	3 ans à compter de la fin de l'exercice financier auquel ils se rapportent	Papier/électronique
Dossiers permettant de prouver le respect des exigences nationales relatives au salaire minimal	3 ans à compter de la date à laquelle la période de référence de la paie suivant	Papier/électronique

Palmarès	Période de conservation recommandée	Format de stockage
	immédiatement celle à laquelle elle se rapporte prend fin	
Détail des prestations en nature, dossiers sur l'impôt sur le revenu (P45, P60, P58, P48 etc.), déclaration fiscale du salaire imposable et des impôts versés	4 ans	Papier/électronique
Déclarations d'impôt sur le revenu et des cotisations d'assurance des employés et correspondance connexe avec le HMRC	3 ans à compter de la fin de l'exercice fiscal auquel ils se rapportent	Papier/électronique
Dossiers d'allocation réglementaire de congé maladie	3 ans à compter de la fin de l'exercice fiscal auquel ils se rapportent	Papier/électronique
Dossiers sur les salaires (notamment les heures supplémentaires, primes et dépenses)	6 ans	Papier/électronique
Dossiers relatifs aux heures travaillées et aux paiements versés aux travailleurs	3 ans	Papier/électronique
Dossiers, calculs, certificats ou autres justificatifs médicaux relatifs à l'allocation réglementaire de congé maternité	3 ans à compter de la fin de l'exercice fiscal au cours duquel la période de congé maternité prend fin	Papier/électronique

3. Dossiers de santé et de sécurité

Palmarès	**Période de conservation recommandée**	**Format de stockage**
Dossiers sur les blessures, maladies ou événements dangereux devant faire l'objet d'un signalement • incidents devant faire l'objet d'un signalement • diagnostics devant faire l'objet d'un signalement • blessure découlant d'un accident du travail (notamment le registre des accidents de la société)	3 ans à compter de la date de la saisie	Papier/électronique
Dossier sur les tests et examens des systèmes de contrôle et équipements de protection requis par la COSHH	5 ans à compter de la date de création du dossier	Papier/électronique

4. La Fiche Cliente

Palmarès	**Période de conservation recommandée**	**Format de stockage**
Coordonnées du client	6 ans à compter de la fin de la relation	Papier/électronique
Adresse/coordonnées de l'expéditeur	6 ans à compter de la fin de la relation	Papier/électronique
Adresse/coordonnées du destinataire	6 ans à compter de la fin de la relation	Papier/électronique