Linde Material Handling

Conditions d'utilisation de Linde Service Manager

Linde Material Handling GmbH, Carl-von-Linde-Platz, 63743 Aschaffenbourg, Allemagne (« **LMH** ») propose à certains distributeurs (désignés par les termes « **distributeur** » seuls et « **distributeurs** » conjointement), répondant aux critères pour être qualifiés d'entrepreneurs au sens du paragraphe 14 du Code civil allemand (« **BGB** »), d'utiliser « Linde Service Manager » (« **service** »), une application logicielle mobile.

Le service permet de collecter et d'associer différentes informations relatives au matériel de manutention et d'interagir avec le système de maintenance LMH dans le cadre du réseau de maintenance LMH (« **Extranet LMH** »).

Dans le cadre des conditions générales de l'Extranet LMH (« **CG Extranet** »), un distributeur peut demander à LMH d'inscrire certains de ses clients (désignés par les termes « **client** » seuls et « **clients** » conjointement), répondant aux critères pour être qualifiés d'entrepreneurs au sens du paragraphe 14 BGB, de manière à ce qu'ils puissent accéder au service au nom du distributeur et à ce que d'autres personnes (ex. employés du client) puissent accéder au service au nom du client.

1. Généralités

1.1. L'utilisation du service est uniquement soumise aux présentes conditions générales (« **CG** »). La dernière version des CG est disponible à la page : https://www.linde-mh.com/en/Legal-Notes/Privacy-Statement/. En cas de modification des présentes CG, les modifications seront publiées au plus tard quatre semaines avant leur date d'entrée en vigueur. Les modifications feront partie intégrante du contrat régissant l'utilisation du service conclu entre LMH et le distributeur, à moins que le distributeur ne les conteste.

1.2. Toute personne autorisée à accéder au service conformément aux CG Extranet, que ce soit via le distributeur (y compris, pour éviter tout doute, le client) ou via le client (désignée par les termes « **utilisateur** » seule et « **utilisateurs** » conjointement), sera considérée comme un mandataire du distributeur dans le cadre des présentes CG. Si le distributeur supprime ou modifie les droits de l'utilisateur à cet égard, LMH est en droit de résilier le présent contrat avec le distributeur pour motif valable et d'empêcher les utilisateurs d'accéder au service.

1.3. Aucune autre condition générale, y compris, mais sans s'y limiter, les conditions générales du distributeur ou du client, ne fait partie intégrante du contrat conclu entre LMH et le distributeur concernant le service, même si LMH ne s'oppose pas explicitement aux conditions générales qui lui sont présentées.

2. Conclusion du contrat et accès général au service

2.1. En tant que condition générale d'accès au service, l'utilisateur doit soit utiliser les identifiants de connexion obtenus lors de l'inscription à l'Extranet LMH pour accéder au service, soit activer le service via l'Extranet LMH. L'accès à l'Extranet LMH est soumis aux CG Extranet et, pour éviter tout doute, aucun élément contenu dans le présent contrat n'autorise le distributeur ou l'utilisateur à accéder à l'Extranet LMH.

2.2. En acceptant les CG (que ce soit de son fait ou de celui de son utilisateur), le client accepte la proposition de LMH de conclure le présent contrat relatif au service.

3. Portée du service

3.1. La portée du service est décrite de manière détaillée à la page https://www.linde-mh.de/LSMScope (« **Portée du service** ») avec les conditions du service.

3.2. Sauf accord contraire, les services à fournir par LMH peuvent uniquement émaner de la portée du service et seront fournis comme des services au sens du paragraphe 611 BGB.

3.3. LMH est en droit de modifier la portée du service pour motif important, notamment suite à l'évolution de la technique, à un changement de la juridiction compétente ou pour toute autre raison comparable. Dans la mesure où une modification de la portée du service nuit à l'équilibre contractuel entre LMH et le distributeur, LMH s'abstiendra de procéder à toute modification. À l'exception des scénarios évoqués précédemment, toute modification de la portée du service requiert le consentement du distributeur, qui peut être accordé par l'utilisateur.

4. Obligations de coopération

4.1. Les obligations de coopération des distributeurs ou les pré-requis à remplir pour permettre la fourniture du service (exigences techniques et configurations requises) sont présentés de manière détaillée dans la portée du service.

4.2. Le distributeur et ses utilisateurs doivent coopérer gratuitement. Si le distributeur ou ses utilisateurs ne coopèrent pas ou pas dans les délais, la fourniture du service sera repoussée en conséquence.

5. Droits de LMH

5.1. LMH dispose de tous les droits concernant le service et les informations qui y correspondent, dont sa configuration, et en particulier tout ce qui a trait aux droits d'auteur, droits d'inventions, droits sur les bases de données et droits de propriété technique. Il en va de même pour l'utilisation des données découlant de l'utilisation du service par l'utilisateur (« **données d'utilisation** ») et de toute autre documentation liée au service fourni par LMH.

5.2. LMH utilisera les données d'utilisation sous forme pseudonymisée dans le cadre de ses propres objectifs commerciaux.

6. Licences

6.1. Les licences des distributeurs sur le logiciel standard (si elles existent) sont soumises aux conditions de licence correspondantes. Le logiciel ne peut être mis à la disposition du distributeur que sur la base des accords de licence d'utilisateurs (EULA) correspondants ou d'autres documents similaires. Le distributeur doit s'assurer que chaque utilisateur du logiciel respecte les accords de licence correspondants.

6.2. Sauf accord contraire, et sous réserve du paiement intégral des éventuelles redevances dues pour le service, LMH accorde au distributeur une licence non exclusive et non transférable d'utilisation du service dans sa version compilée (hors code source) dans le cadre des objectifs commerciaux du distributeur et des conditions du présent contrat et permet au distributeur (dans le cadre de cette licence) d'autoriser l'utilisateur à utiliser le service de la même manière.

7. Responsabilité

7.1. La responsabilité de LMH pour tout dommage provoqué de manière intentionnelle ou par grave négligence par LMH, ses représentants légaux ou ses agents, ou en cas d'atteinte à la vie, à l'intégrité physique ou à la santé, est illimitée.

7.2. Si LMH manque à ses obligations contractuelles pour des éléments essentiels à la bonne exécution du présent contrat et dont le distributeur attend tout particulièrement l'application, la responsabilité de LMH sera limitée aux montants raisonnablement prévisibles, sauf si les conditions établies au paragraphe 7.1 s'appliquent.

7.3. Toute autre responsabilité de LMH est totalement exclue.

8. Confidentialité

8.1. Le distributeur et ses utilisateurs doivent traiter toutes les informations qui leur sont confiées de manière confidentielle. Le distributeur et ses utilisateurs ne sont pas autorisés à transmettre ou à reproduire les informations qui leur sont fournies, sauf autorisation explicite de LMH. Les informations dont le distributeur et ses utilisateurs avaient déjà connaissance auparavant ne seront pas considérées comme des informations confidentielles aux fins de cette déclaration.

8.2. Si le distributeur et ses utilisateurs se voient obligés par un tribunal, une autorité ou d'autres bureaux ou institutions dotés de pouvoirs spéciaux, ou sont tenus légalement d'une autre manière de divulguer des informations confidentielles, ils ont l'obligation d'en informer LMH dans les plus brefs délais afin de donner à LMH la possibilité soit de prendre des mesures pour empêcher la divulgation, soit de les libérer de leurs obligations de confidentialité conformément à la présente déclaration de confidentialité. Si LMH ne parvient pas à empêcher la divulgation, le distributeur et ses utilisateurs sont autorisés à révéler des informations confidentielles dans la limite de ce que le conseiller juridique considère obligatoire, même si le distributeur et ses utilisateurs n'ont pas été libérés de leur obligation de confidentialité.

9. Protection des données

9.1. LMH respecte toutes les lois applicables sur la protection des données et traite notamment les données à caractère personnel qui lui sont transmises dans le respect de ces lois.

9.2. Concernant les données à caractère personnel que lui transmettent le distributeur et ses utilisateurs, LMH agit en tant que sous-traitant au sens de l'article 4 du Règlement (UE) 2016/679 (Règlement général sur la protection des données, « **RGPD** ») et traite ces données à caractère personnel conformément au contrat de traitement des données conclu entre LMH et le distributeur pour le service (« **DPA** »).

9.3. Le distributeur respecte toutes les lois de protection des données applicables à ses activités en tant que responsable du traitement (au sens de l'article 4 RGPD) dans le cadre des CG et du DPA, notamment en ce qui concerne l'accès des utilisateurs au service et s'assure du traitement légitime des données à caractère personnel soumises à LMH dans le cadre du service, y compris, mais sans s'y limiter, les données à caractère personnel des utilisateurs.

10. Résiliation

La résiliation du présent contrat équivaut à la résiliation du service telle que définie dans la portée du service. Si la portée du service ne définit aucune résiliation spécifique, LMH et le client peuvent résilier le présent contrat à tout moment, sous réserve d'un préavis de trois mois avant la fin d'une année calendaire. Le droit de résilier le contrat pour motif valable reste inchangé. Il y a notamment motif valable

10.1. lorsque l'autre partie viole une disposition essentielle du présent contrat et ne remédie pas à cette violation dans le délai raisonnable fixé par l'autre partie,

10.2. si le DPA est résilié ou prend fin pour une raison quelconque,

10.3. si le distributeur résilie ou modifie l'autorisation de l'utilisateur à représenter le distributeur (voir 1.2).

11. Droit applicable et juridiction

Le présent contrat est soumis au droit allemand. La Convention des Nations Unies sur les contrats de vente internationale de marchandises (CVIM) et l'application des dispositions concernant les conflits de lois sont exclues. En cas de litige entre LMH et le client lié au présent contrat, la juridiction compétente est Aschaffenbourg.

Dernière mise à jour : 10/2018

Linde Material Handling

Contrat de traitement des données (« contrat ») relatif à Linde Service Manager

Le présent contrat renvoie aux conditions générales de « Linde Service Manager » (« **CG** »). Tous les termes employés dans le présent contrat sans y être définis portent la signification qui leur a été attribuée dans les CG.

Le distributeur (« **client** » ou « **responsable du traitement** »), représenté par l'utilisateur, et LMH (« **sous-traitant** » et conjointement avec le responsable du traitement les « **parties** ») concluent le présent contrat pour régir le traitement des données à caractère personnel réalisé dans le cadre du service. Le présent contrat définit les obligations de protection des données des parties en lien avec la protection des données à caractère personnel du client.

1. Définitions

Dans le présent contrat, les termes suivants porteront la signification suivante :

1.1. « **Sous-traitant** » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

1.2. « **Tiers** » : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.

1.3. « **Données à caractère personnel** » : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « **personne concernée** ») ; est réputée être une « personne physique identifiable » une personne physique 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 éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

1.4. « **Pseudonymisation** » : le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable.

1.5. « **Responsable du traitement** » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

1.6. « **Traitement** » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par

transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

1.7. « **Violation de données à caractère personnel** » : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

1.8. « **Contrat principal** » : Le contrat conclu entre LMH et le distributeur concernant les services, tel que défini dans les CG.

2. Objet et conditions du contrat

2.1. Le présent contrat établit les obligations du sous-traitant vis-à-vis des données à caractère personnel du client traitées par le sous-traitant au nom du client.

2.2. Les dispositions du présent contrat ne s'appliquent pas si, conformément à l'accord, le sous-traitant n'est pas tenu de mener des activités de traitement des données à caractère personnel du client. Dans ce cas, le client doit s'assurer que ses données à caractère personnel sont correctement isolées du sous-traitant.

2.3. Le client porte la responsabilité exclusive de déterminer si le traitement est légal et de s'assurer que les droits des personnes concernées sont protégés.

2.4. Le contrat commence à la date de début du contrat principal et s'achève à la fin du contrat principal. Si le sous-traitant traite les données à caractère personnel sur les instructions du client même après la fin du contrat principal, le présent contrat restera en vigueur jusqu'à ce que le traitement mené sur instructions du client soit terminé.

2.5. Nonobstant la disposition du paragraphe 2.4, les parties peuvent résilier le présent contrat pour motif valable. Si la cause de la résiliation est liée à la violation d'une obligation contractuelle, la résiliation est uniquement autorisée si, après expiration d'un délai fixé pour remédier à la violation, la violation n'a pas été réparée, ou si la transmission d'un avertissement n'a produit aucun effet. Il y a notamment motif valable pour le sous-traitant si

2.5.1. le client transmet à plusieurs reprises des instructions illégales, le sous-traitant en a informé le client dans les plus brefs délais et le client n'a pas modifié ses instructions ;

2.5.2. le client a violé les dispositions du présent contrat ;

2.5.3. le client s'est opposé au recours à une entreprise sous-traitante dans le cadre du présent contrat.

De plus, les conditions du contrat principal s'appliquent mutatis mutandis au présent contrat.

3. Nature, portée et lieu du traitement

3.1. Le sous-traitant est autorisé à accéder aux données à caractère personnel du client afin de fournir les services visés par le contrat principal, dans les limites décrites en annexe 1. Les dispositions du présent contrat n'élargissent pas les obligations du sous-traitant, mais les détaillent

simplement de manière plus approfondie. Le présent contrat établit également les obligations du client.

3.2. Le client peut émettre des instructions donnant davantage de précisions quant aux obligations du sous-traitant.

3.3. Le sous-traitant n'a pas le droit d'utiliser les données à caractère personnel à d'autres fins que celles décrites dans le contrat principal et dans le présent contrat et ne peut notamment, en l'absence d'instruction explicite préalable du client, transmettre les données à caractère personnel à un tiers ou les divulguer à d'autres destinataires, sauf mention contraire dans le présent contrat.

3.4. Le traitement régi par le présent contrat est limité au territoire de l'Union européenne et de l'EEE, sauf mention contraire dans la ou les annexe(s) au présent contrat.

4. Instructions du client, droits des personnes concernées, évaluation d'impact sur la protection des données

4.1. Via son ou ses instruction(s), le client peut préciser ou mettre à jour la nature, la portée et la méthode de traitement des données, les mesures de sécurité, les données à caractère personnel à traiter et les groupes de personnes concernées. Cela vaut en particulier pour les cas où une autorité réglementaire ou une modification de la législation pousse ou oblige le client à émettre des instructions. Si une personne concernée contacte directement le sous-traitant, le sous-traitant doit en informer le client sous forme écrite dans les plus brefs délais et demander des instructions sur la manière de procéder.

4.2. Si le client mène une évaluation d'impact sur la protection des données, le sous-traitant doit l'y aider selon les instructions fournies dans la limite du raisonnable et du nécessaire, y compris concernant toute consultation préalable auprès de l'autorité réglementaire compétente.

4.3. Les instructions du client se limitent à l'application des exigences légales et réglementaires de la législation sur la protection des données. Elles doivent être distinguées des demandes de modifications. Les demandes de modifications correspondent aux modifications de la portée de services non requises pour remplir les obligations légales ou réglementaires ou qui vont au-delà des mesures nécessaires à l'application de ces exigences. Il ne s'agit pas d'instructions au sens du présent contrat, mais de demandes de modification des services de la part du client. Le sous-traitant a le droit, mais pas l'obligation, d'appliquer ces demandes de modifications. L'application des demandes de modifications sera rémunérée séparément.

4.4. Le client transmet toujours ses instructions par courrier, fax ou e-mail. Le client confirme par écrit ou sous forme de texte, dans les plus brefs délais, toute instruction transmise oralement de manière exceptionnelle.

4.5. Le sous-traitant informe le client dans les plus brefs délais et sous forme de texte s'il considère qu'une instruction du client viole les dispositions sur la protection des données ou est, de manière non négligeable, erronée, incomplète, contradictoire ou légalement ou techniquement infaisable. En fournissant cette information, le sous-traitant demandera explicitement et sous forme écrite au client d'indiquer dans les plus brefs délais s'il souhaite que le sous-traitant suive les instructions ou continue de traiter les données à caractère personnel sans suivre les instructions, jusqu'à ce que le client ait examiné l'information et prenne une décision.

5. Obligations d'information du sous-traitant

5.1. En cas de violation de données à caractère personnel, le client peut être tenu de signaler la violation. Le sous-traitant doit informer le client s'il suspecte ou découvre une violation (non négligeable) de la protection des données à caractère personnel du client par le sous-traitant ou toute personne placée sous sa direction.

5.2. Le client peut exiger que le sous-traitant prenne toutes les mesures raisonnables et nécessaires pour aider le client à remplir ses obligations de signalement.

6. Obligations du client

6.1. Le client doit informer le sous-traitant dans les plus brefs délais s'il constate des erreurs ou des anomalies lors du contrôle du résultat du service rendu.

6.2. Le client doit s'assurer, avant et après le début du traitement des données, que les mesures techniques et organisationnelles mises en place par le sous-traitant sont respectées. Le résultat de ces contrôles doit être documenté.

6.3. Le client est responsable du respect des obligations émanant des articles 33 et 34 du Règlement général sur la protection des données de l'Union européenne vis-à-vis de l'autorité réglementaire ou de toute personne concernée touchée par une violation de données à caractère personnel.

6.4. Le client doit informer le sous-traitant des obligations de suppression et de conservation des données à caractère personnel et des éléments nécessaires à l'application de ces exigences.

7. Délégué à la protection des données

7.1. Le sous-traitant a désigné un délégué à la protection des données (« **DPO** »). Ses coordonnées sont les suivantes : datenschutz@kiongroup.com. Le sous-traitant doit avertir le client de tout changement ou de tout changement imminent en la matière.

7.2. Le client a désigné un délégué à la protection des données, ou – si le client n'est pas tenu de désigner un délégué à la protection des données et ne l'a pas fait – fournira au sous-traitant le nom d'un employé du client qui a accepté de porter les obligations et responsabilités d'un délégué à la protection des données. Le client doit avertir le sous-traitant de tout changement ou de tout changement imminent en la matière, sans que le sous-traitant n'ait à l'exiger de manière spécifique.

7.3. Si le client doit désigner un représentant au sens de l'article 27 du Règlement général sur la protection des données de l'Union européenne, il indiquera l'identité de son représentant au sous-traitant. Le client doit avertir le sous-traitant de tout changement ou de tout changement imminent en la matière, sans que le sous-traitant n'ait à l'exiger de manière spécifique.

8. Personnes placées sous la direction du sous-traitant

8.1. Pour mener les activités de traitement de données selon les conditions établies par le présent contrat, le sous-traitant peut uniquement faire appel à des personnes qui ont signé un accord de confidentialité documenté et qui se sont familiarisées au préalable avec les dispositions légales de protection des données qui les concernent et avec les activités de traitement à mener au nom du client.

8.2. Le sous-traitant doit s'assurer que toutes les personnes placées sous sa direction qui ont accès aux données à caractère personnel du client traitent uniquement ces données à caractère personnel dans le cadre et conformément aux instructions du client et aux dispositions du présent contrat. La seule exception à la disposition précédente concerne les activités de traitement ponctuelles, notamment le transfert de données, que le sous-traitant ou les personnes placées sous sa direction sont explicitement appelés à mener par un tribunal ou une autorité gouvernementale sur la base d'une disposition légale. À condition que la loi l'y autorise, le sous-traitant doit informer le client de la réception de telles demandes, de préférence avant que les données à caractère personnel ne soient transmises.

9. Principes d'un traitement sécurisé

9.1. En tenant compte de la technologie actuellement disponible, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des objectifs du traitement de données souhaité par le client, ainsi que de la probabilité et de la gravité potentielle du risque pour les droits et libertés des personnes (analyse des risques), le sous-traitant doit mettre en place les mesures techniques et organisationnelles nécessaires pour s'assurer que les données à caractère personnel soient correctement protégées.

9.2. Lors de l'évaluation du niveau de sécurité adapté, le sous-traitant doit tenir compte des risques inhérents au traitement des données à caractère personnel du client, y compris, mais sans s'y limiter, le risque de destruction fortuite ou délibérée et la perte, la modification ou la divulgation ou l'accès non autorisé aux données à caractère personnel du client.

9.3. Le sous-traitant doit mettre à jour et adapter les mesures techniques et organisationnelles de son plan de sécurité afin de tenir compte de l'évolution de la technologie disponible, sans que ces mesures ne tombent sous le niveau de sécurité et de protection indiqué dans le présent contrat.

9.4. Le sous-traitant doit documenter de manière détaillée les mesures techniques et organisationnelles prises en vertu du présent contrat dans l'annexe au contrat. Le sous-traitant doit maintenir la documentation à jour et documenter toute modification matérielle.

9.5. Les mesures techniques et organisationnelles présentées en annexe au présent contrat sont considérées comme approuvées et nécessaires lors de la conclusion du contrat ; elles représentent toutes les exigences que le sous-traitant doit remplir.

9.6. Le client est tenu d'examiner les mesures techniques et organisationnelles sur la base de sa propre analyse des risques. Le client doit s'assurer que les mesures techniques et organisationnelles offrent un niveau de protection des données adapté aux risques auxquels sont exposées les données à caractère personnel à traiter. Si l'analyse des risques du client débouche sur un résultat différent de l'analyse des risques du sous-traitant, le client a le droit de négocier avec le sous-traitant afin d'adapter les mesures de sécurité. Si les parties ne parviennent pas à trouver un accord, elles ont toutes deux le droit de résilier le contrat avec un préavis de 14 jours.

10. Contrôles

10.1. Le client a le droit de contrôler la bonne réalisation des services liés aux données à caractère personnel du client par le sous-traitant et le respect des dispositions du présent contrat, y compris, mais sans s'y limiter, les mesures techniques et organisationnelles permettant d'assurer la sécurité du traitement.

10.2. Sur demande, le sous-traitant doit fournir des preuves que les mesures de sécurité techniques et organisationnelles ont bien été mises en application. Cela comprend
- la preuve du respect des codes de conduite approuvés conformément à l'article 40 du Règlement général sur la protection des données ou
- un certificat délivré dans le cadre d'une procédure de certification approuvée conformément à l'article 42 du Règlement général sur la protection des données ou
- une auto-évaluation qualifiée issue d'un tiers indépendant (comme le DPO, un auditeur, un auditeur externe de protection/sécurité des données) sous forme de texte ou
- une certification adaptée délivrée suite à un audit de sécurité IT ou de protection des données (ex. ISO 27001).

Ces preuves doivent contenir toutes les informations nécessaires pour prouver que les obligations découlant du présent contrat ont bien été respectées et que les mesures techniques et organisationnelles pertinentes ont bien été mises en place afin de garantir la sécurité du traitement. Le client peut exiger ces informations une fois par année calendaire et plus fréquemment uniquement en cas de soupçon légitime de violation du présent contrat par le sous-traitant, dont le client doit informer le sous-traitant sous forme écrite.

10.3. Le client a le droit de contrôler le respect du présent contrat, et notamment le respect des règles assurant la sécurité du traitement, de mener des inspections sur site annoncées à l'avance dans les locaux commerciaux du sous-traitant aux horaires d'ouverture habituels (de 9h à 18h), une fois tous les trois ans, et de faire réaliser ces contrôles par un auditeur externe soumis aux obligations légales et contractuelles de confidentialité. Le client doit annoncer l'inspection par écrit deux semaines à l'avance. Les restrictions imposées au client ne s'appliquent pas en cas d'urgence (par exemple en cas de soupçon de plusieurs violations non négligeables du présent contrat par le sous-traitant) ; dans ce cas, le client ne doit pas avertir le sous-traitant au préalable par écrit.

11. Entreprises sous-traitantes

11.1. Si le sous-traitant est autorisé à faire appel à d'autres entreprises sous-traitantes sur la base d'un accord explicite conclu avec le client, et si la possibilité que ces entreprises sous-traitantes aient accès aux données à caractère personnel du client ne peut être exclue, le sous-traitant n'engage des entreprises sous-traitantes, et ne permet donc que des personnes aient potentiellement accès aux données à caractère personnel du client, que s'il a informé le client par écrit des détails établis au paragraphe suivant et a donné au client la possibilité de s'y opposer, et si le client n'a émis aucune contestation dans le délai imparti.

11.2. Les informations à fournir par le sous-traitant évoquées ci-dessus doivent inclure, au minimum, les éléments suivants, de manière spécifique et détaillée :

11.2.1. Identité de l'entreprise sous-traitante,

11.2.2. Services spécifiques rendus par l'entreprise sous-traitante au sous-traitant,

11.2.3. Expérience, capacité, fiabilité et mesures de sécurité IT et de protection des données essentielles au respect des obligations de protection des données du présent contrat,

11.2.4. Garanties ou assurances de l'entreprise sous-traitante s'engageant à respecter les dispositions du présent contrat.

11.3. Le client est en droit, dans un délai de sept jours suivant la réception des informations évoquées précédemment, de s'opposer au recours à une entreprise sous-traitante en respectant la forme écrite, et à condition d'avoir une raison légitime de le faire. En cas d'objection, le sous-traitant est tenu de mettre le contrat en application et de fournir ses services et remplir ses obligations sans faire appel à cette entreprise sous-traitante, mais conserve le droit de résilier le contrat.

11.4. Si une entreprise sous-traitante a accès aux données à caractère personnel du client, le sous-traitant est tenu de conclure avec l'entreprise sous-traitante un contrat de traitement des données imposant à l'entreprise sous-traitante les obligations établies dans le présent contrat. Ce contrat doit être conclu avant que l'entreprise sous-traitante n'accède pour la première fois aux données à caractère personnel du client.

12. Restitution et effacement

12.1. Si le client le demande, le sous-traitant est tenu, au plus tard à la fin du présent contrat, de restituer ou de remettre toutes les données à caractère personnel du client.

12.2. Les détails des obligations d'effacement des données peuvent être intégrés à l'annexe au contrat et, le cas échéant, peuvent être transmis par instructions explicites du client. Le sous-traitant n'est pas tenu de disposer de son propre plan d'effacement. Si le client le demande, le sous-traitant est tenu, immédiatement après la fin du présent contrat ou auparavant, d'effacer toutes les données à caractère personnel qui ne sont pas soumises à des exigences légales de stockage ou de conservation par le sous-traitant conformément au droit de l'Union européenne ou d'un État membre de l'UE, ou à tout accord explicite régissant le stockage ou l'effacement des données à caractère personnel conclu avec le client. Le sous-traitant doit procéder à l'effacement et le documenter.

13. Coûts assumés par le sous-traitant

Tous les frais engagés par le sous-traitant ou des entreprises sous-traitantes dans le cadre du traitement des données à caractère personnel mené au nom du client et selon les conditions du présent contrat, et en particulier ceux engagés sur la base

13.1. d'une obligation de répondre aux demandes des personnes concernées selon les instructions du client, notamment pour corriger, effacer ou limiter les données à caractère personnel ou restituer les données à caractère personnel au client et, le cas échéant, transmettre les données (portabilité), ou participer à ce type de mesures,

13.2. d'une obligation de participation à l'évaluation d'impact sur la protection des données,

13.3. du respect ou la mise en œuvre des instructions du client,

13.4. de l'obligation de fournir une assistance pour remplir les obligations de divulgation des informations à l'autorité réglementaire ou aux personnes concernées,

13.5. de la production d'une auto-évaluation qualifiée,

13.6. des inspections sur site par le client ou les auditeurs (externes) auxquels le client a fait appel, à moins que cette inspection n'ait permis de constater d'importants manquements ; la charge de la preuve à cet égard revient au client,

13.7. des coûts supplémentaires liés aux mesures techniques et organisationnelles permettant de garantir la sécurité du traitement, lorsque ces mesures sont mises en place suite à un écart entre les analyses des risques des deux parties,

13.8. du respect de l'obligation de restitution ou d'effacement des données à caractère personnel,

seront remboursés séparément au sous-traitant sur la base de taux horaires de marché. Le sous-traitant doit consigner tous les frais et dépenses engagés.

14. Modifications du contrat

Si le sous-traitant est tenu par la loi de procéder à des modifications et amendements, le client est obligé de le soutenir et de les approuver.

15. Responsabilité

15.1. Si une personne concernée et/ou un tiers intente une action contre le sous-traitant dans le cadre des activités de traitement des données menées par le sous-traitant au nom du client, le client est tenu d'indemniser le sous-traitant et de payer tous les frais juridiques, les dommages et/ou les amendes prévues par le droit administratif ou pénal.

15.2. La disposition précédente ne s'applique pas si le sous-traitant n'a pas rempli les obligations qui lui incombent au titre du Règlement général sur la protection des données ou n'a pas suivi les instructions dûment transmises par le client, ou a agi en contradiction avec ces instructions.

15.3. Les limites de responsabilité convenues entre le client et le sous-traitant dans le contrat principal en faveur du sous-traitant s'appliquent également à la responsabilité du sous-traitant pour les activités de traitement des données régies par le présent contrat.

Linde Material Handling

Annexe

I. Catégories de personnes concernées

- Clients
- Autres : distributeurs, partenaires de réseau

II. Types de données

- Données de base du personnel
- Données de base de communication
- Historique du client

III. Portée du traitement

Les exigences principales du client sont les suivantes :
Création et traitement des notifications et commandes de maintenance

IV. Lieu où les données à caractère personnel sont traitées

EEE

V. Système(s) de traitement, dont importation et exportation de données à caractère personnel issues d'autres systèmes

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP et autres systèmes ERP de nos distributeurs,
notifications push mobiles OneSignal

VI. Mesures de sécurité techniques et organisationnelles du sous-traitant

Mise en œuvre des mesures techniques et organisationnelles

a. Confidentialité (art. 32 (1) RGPD)

(1) Contrôle d'accès (locaux)

- Alarme
- Contrôle d'accès automatique
- Serrures de sécurité
- Vidéo-surveillance aux entrées
- Contrôle par clé/liste
- Réceptionniste/Gardien
- Liste des visiteurs
- Badge employés/visiteurs
- Visiteurs toujours accompagnés par des employés

(2) Contrôle d'accès (systèmes)

- Connexion avec nom d'utilisateur + mot de passe
- Serveur du logiciel antivirus
- Clients du logiciel antivirus
- Pare-feu
- Systèmes de détection des intrusions
- Gestion des appareils mobiles

- Utilisation d'un VPN pour les accès à distance
- Cryptage des stockages de données
- Cryptage des smartphones
- Protection BIOS (mot de passe différent)

(3) Contrôle d'accès (données)

- Gestion des droits des utilisateurs
- Création de profils d'utilisateurs
- Politique « Mot de passe sécurisé »
- Politique « Effacement / Suppression »
- Politique générale de protection des données et/ou de sécurité des données
- Manuel « Verrouillage manuel du bureau »
- Formations régulières des employés
- Utilisation d'un système d'autorisations
- Gestion des droits des utilisateurs par des administrateurs

(4) Contrôle de séparation

Séparation de l'environnement productif et de l'environnement de test

(5) Pseudonymisation (art. 32 (1) RGPD ; art. 25 (1) RGPD)

n/a

b. Disponibilité et résilience (Art. 32 (1) RGPD)

- Détecteurs d'incendies et de fumée
- Extincteur dans la salle des serveurs
- Contrôle de la température et de l'humidité dans la salle des serveurs
- Air conditionné dans la salle des serveurs
- Système UPS
- Multiprise de sécurité utilisée dans la salle des serveurs
- Système RAID/image miroir de HD
- Vidéo-surveillance dans la salle des serveurs
- Signal d'alarme en cas d'accès non autorisé dans la salle des serveurs
- Concept de sauvegarde et de restauration (formulé)
- Contrôle de sauvegarde
- Aucun équipement sanitaire dans ou au-dessus de la salle des serveurs
- Existence d'un plan d'urgence (iE BSI IT-Grundschutz 100-4)
- Partitions séparées pour le système d'exploitation et les données

c. Intégrité (art. 32 point 1 RGPD)

- Les données à caractère personnel peuvent uniquement être modifiées par les administrateurs
- Connexions cryptées telles que sftp, https
- Enregistrement d'accès et récupération
- Aperçu des processus classiques de récupération et de transfert
- Personnel soigneusement sélectionné

d. Procédure de tests et évaluations réguliers (art. 32 (1) RGPD ; art. 25 (1) RGPD)

(1) Gestion de la protection des données

- Certification de sécurité ISO 27001
- L'efficacité des mesures de sécurité techniques est vérifiée au moins une fois par an
- Employés formés et tenus au respect de la confidentialité

(2) Gestion de la réaction aux incidents

- Utilisation d'un pare-feu et mise à jour régulière
- Utilisation d'un filtre à spams et mise à jour régulière
- Utilisation d'un antivirus et mise à jour régulière
- Système de détection des intrusions (IDS)
- Système de prévention des intrusions (IPS)

Protection des données par défaut (art. 25 (2) RGPD)

- La quantité de données à caractère personnel est limitée à ce qui est nécessaire en fonction des objectifs pour lesquels elles sont traitées