Linde Material Handling

Data Processing Agreement ("Agreement") with respect to Linde Service Manager

This Agreement refers to the general terms and conditions of the "Linde Service Manager" ("**GT&Cs**"). Any capitalized terms used but not defined herein shall have the meaning as ascribed to such in the GT&Cs.

The Distributor ("**Client**" or "**Controller**"), represented by the User, and LMH ("**Processor**" and together with the Controller, the "**Parties**") enter into this Agreement for the processing of personal data with respect to the Service. This Agreement governs the data protection obligations of the Parties in relation to the protection of Client's personal data.

1. Definitions

In this Agreement, the following terms have the following meanings:

1.1. "**Processor**": A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

1.2. "**Third Party**": A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

1.3. "**Personal Data**": Any information relating to an identified or identifiable natural person ("**Data Subject**"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.4. "**Pseudonymization**": The processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

1.5. "**Controller**": The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

1.6. "**Processing**": Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.7. "**Personal Data Breach**": A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.8. "**Main Agreement**": The agreement entered into between the LMH and the Distributor with respect to the Services, as specified in the GT&Cs.

2. Subject Matter and Term of this Agreement

2.1. This Agreement governs the duties of Processor in respect of Personal Data of the Client being processed by Processor on behalf of Client.

2.2. The provisions of this Agreement do not apply if and to the extent that, in accordance with the engagement, Processor is not required to carry out processing activities in respect of Client's Personal Data. In this case Client shall ensure that its Personal Data is adequately shielded from Processor.

2.3. Solely the Client shall determine whether the Processing is lawful and ensure that the rights of the data subjects are protected.

2.4. This Agreement commences at the time when the Main Agreement commences and ends upon the end of the term of Main Agreement. If Processor processes the Personal Data on the instructions of Client even after the Main Agreement ended, this Agreement shall also remain in force until the Processing carried out on the instructions of Client has ended.

2.5. Notwithstanding the provision in 2.4, the Parties may terminate this Agreement for good cause. If the cause relates to the breach of a duty under the Agreement, termination is permitted only after a period specified for the remedy of the breach has expired without the breach being remedied or after a warning has failed to produce any effect. Good cause for Processor shall be in particular if

2.5.1. Client repeatedly issues unlawful instructions, Processor has informed Client of this without undue delay and Client has not revoked the instructions;

2.5.2. Client has violated the provisions of this Agreement;

2.5.3. Client has objected to the engagement of a subcontractor pursuant to this Agreement.

Moreover, the terms of the Main Agreement shall apply mutatis mutandis to this Agreement.

3. Nature, Scope and Place of Processing

3.1. Processor is authorized to access Client's Personal Data for the purpose of rendering the services pursuant to the Main Agreement to the extent described in Annex 1. The provisions of this Agreement do not expand the duties of Processor, but merely specify them in greater detail. This Agreement also governs the duties of Client.

3.2. Client may issue instructions that specify Processor's duties in further detail.

3.3. Processor is not permitted to use the Personal Data for other purposes as described in the Main Agreement and in this Agreement and in particular must not, without the prior explicit instruction of Client, transfer the Personal Data to a third party or disclose it to other recipients, unless otherwise specified in this Agreement

3.4. Processing under this Agreement is restricted to the territory of the European Union and the EEA, unless otherwise specified in the Annex(es) to this Agreement.

4. Instructions of Client, Rights of Data Subjects, Data Protection Impact Assessment

4.1. Through its instruction(s), Client is entitled to specify or to update the nature, scope, and method of data processing, security measures, Personal Data to be processed, and the groups of data subjects. This applies primarily to cases when a regulatory authority or changes to the legislation cause or require Client to issue instructions. If a Data Subject contacts Processor directly, Processor shall inform Client in text form without undue delay and ask for instructions as to how to proceed.

4.2. If Client carries out a data protection impact assessment, Processor shall assist it as instructed as far as is reasonable and necessary, including in respect of any prior consultations with the competent regulatory authority.

4.3. Instructions of Client are limited to the implementation of statutory or regulatory requirements of data protection law. They are to be distinguished from change requests. Change requests refer to changes to the scope of services that are not required in order to implement statutory or regulatory requirements or which go further than the measures necessary to implement such requirements. They are not instructions in the sense of this Agreement, but requests by Client for changes to services. Processor is entitled, but not obliged, to implement such change requests. The implementation of change requests will be remunerated separately.

4.4. Client will always issue instructions in writing, by fax, or by email. Client will confirm any instructions issued orally, by way of exception, without undue delay in writing or in text form.

4.5. Processor shall inform Client without undue delay in text form if Processor is of the view that an instruction of Client is in breach of data protection provisions or is, other than in a merely negligible way, erroneous, incomplete, contradictory, or legally or technically infeasible. When providing this information, Processor will explicitly notify Client in text form to state without undue delay whether it wishes Processor to comply with the instruction or to continue processing the Personal Data without following the instruction, until Client has reviewed the information and come to a decision.

5. Duties of the Processor to Provide Information

5.1. In the event of a Personal Data Breach, Client may have a duty to report the breach. Processor shall inform Client if it suspects or is aware of a (more than merely negligible) breach of the protection of Client's Personal Data by Processor or by persons under Processor's control.

5.2. Client may demand that Processor takes all reasonable and necessary steps to assist Client in complying with its reporting requirements.

6. Duties of Client

6.1. Client shall inform Processor without undue delay if it ascertains errors or irregularities when checking the output of the rendered service.

6.2. Client must satisfy itself, both before data processing commences and thereafter, that the technical and organizational measures put in place at Processor are being complied with. The outcome of such checks must be documented.

6.3. Client is responsible for compliance with the duties arising from Art. 33, 34 of the EU General Data Protection Regulation vis-à-vis the regulatory authority or vis-à-vis any data subjects affected by a Personal Data Breach.

6.4. Client shall inform Processor of the requirements for erasure and retention of Personal Data, and for the implementation of these requirements.

7. Data Protection Officer

7.1. Processor has appointed a data protection officer ("**DPO**"). The contact details are as follows: datenschutz@kiongroup.com. Processor shall notify Client of changes or imminent changes in this respect.

7.2. Client appointed a data protection officer, or – to the extent Client is not required to appoint a data protection officer and has not done so – will provide Processor with the name of a person at Client who has accepted the duties and the responsibility of a data protection officer. Client shall notify Processor of changes or imminent changes in this respect, without being specifically requested to do so by Processor.

7.3. If Client is required to appoint a representative within the meaning of Art. 27 of the EU General Data Protection Regulation, it will notify Processor of the identity of this representative. Client shall notify Processor of changes or imminent changes in this respect, without being specifically requested to do so by Processor.

8. Persons Under Control of Processor

8.1. In carrying out data processing under the terms of this Agreement, Processor shall use only persons who have given a documented confidentiality undertaking and who have been familiarized in advance with the statutory data protection provisions of relevance to them and to the processing activities to be carried out on behalf of Client.

8.2. Processor shall ensure that all persons under its control that have access to Client's Personal Data only process such Personal Data within the scope of and in accordance with the instructions of Client and the provisions of this Agreement. The sole exception to the above provision concerns individual instances of processing activities, particularly data transfers, which Processor or the persons under its control is/are explicitly ordered to perform by a court or government authority on the basis of a statutory provision. To the extent permitted by law, Processor shall inform Client of such orders, preferably before any Personal Data is transferred.

9. Secure Processing Principles

9.1. Taking into account the currently available technology, the implementation costs, and the nature, scope, circumstances, and purposes of the Data Processing stipulated with Client, as well as the likelihood and potential severity of the risk to the rights and freedoms of individuals (risk analysis), Processor shall put in place the technical and organizational measures that are necessary to ensure that the Personal Data is appropriately protected.

9.2. When assessing the appropriate security level, Processor shall take account of the risks inherent in processing Client's Personal Data, including, but not limited to, the risk of inadvertent or unlawful destruction, and the loss, amendment, or unauthorized disclosure of or unauthorized access to Client's Personal Data.

9.3. Processor shall update and adjust the technical and organization measures in its security plan to take account of changes to the available technology, although these measures must not fall below the security and protection level specified in this Agreement.

9.4. Processor shall document the technical and organizational measures pursuant to this Agreement in detail in the Annex to this Agreement. Processor must keep the documentation up to date and must document any material changes.

9.5. The technical and organizational measures in the Annex of this Agreement are deemed to be approved and necessary when the contract is entered into; they represent all requirements which Processor is required to meet.

9.6. Client is obliged to review the technical and organizational measures based on its own risk analysis. Client is responsible for ensuring that the technical and organizational measures offer a level of data protection that is commensurate to the risks of the Personal Data to be processed. If the Client's risk analysis produces a result that differs from Processor's risk analysis, Client is entitled to negotiate with Processor on the adjustment of the security measures. If the Parties are unable to agree, they each have a right to terminate the Agreement by giving 14 days prior notice.

10. Controls

10.1. Client is entitled to check the performance of the services by Processor in respect of Client's Personal Data and compliance with the provisions of this Agreement, including, but not limited to, the technical and organizational measures to ensure security of the processing.

10.2. Upon request, Processor shall provide Client with evidence that the technical and organizational security measures have been implemented. This includes

- evidence of compliance with approved codes of conduct pursuant to Art. 40 of the General Data Protection Regulation or
- certification in accordance with an approved certification procedure pursuant to Art. 42 of the General Data Protection Regulation or
- qualified self-assessment from an independent third party (such as DPO, auditor, external data protection/security auditors) in text form or
- appropriate certification through an IT security or data protection audit (e.g. ISO 27001).

Such evidence must contain all information necessary to prove compliance with and implementation of the duties under this Agreement and of the relevant technical and organizational measures, that are intended to guarantee the security of the processing. Client may request this information once per calendar year and at shorter intervals only in the event of a legitimate suspicion of a breach by Processor of this Agreement, of which Client must inform Processor in text form.

10.3. Client is entitled to check compliance with the Agreement, in particular compliance with the security of the processing, by carrying out pre-announced on-site inspections at the business premises of Processor during usual business hours (9 a.m. to 6 p.m.) once every three years or to have such checks conducted by an external auditor who is subject to statutory or contractual non-disclosure obligations. Client must give two weeks' advance notice in text form of such inspections. This restriction upon Client does not apply in urgent cases (for example if there is a

suspicion of more than merely negligible breaches of this Agreement by Processor); Client must notify Processor in text form in advance in such cases.

11. Subcontractors

11.1. If and to the extent that Processor is entitled on the basis of an explicit agreement with Client to engage additional processors (subcontractors), and if the possibility that these subcontractors will have access to Client's Personal Data cannot be excluded, Processor may only engage such subcontractors and thereby potentially enable Client's Personal Data to be accessed if it has informed Client in text form of the details set out in the next paragraph and has given Client the opportunity to object, and Client has not objected within the stipulated period.

11.2. The information to be provided by Processor as set out above must, as a minimum, include the following in specific and detailed form:

11.2.1. Identity of the subcontractor,

11.2.2. The specific services to be rendered by the subcontractor for Processor,

11.2.3. The experience, capacity, reliability, and IT security and data protection measures that are essential for compliance with the data protection obligations in this Agreement,

11.2.4. The guarantees or assurances of the subcontractor that it will comply with the provisions of this Agreement.

11.3. Client is entitled, within seven days of receiving the information above, to raise an objection in text form to the engagement of a subcontractor, provided it has legitimate reason to do so. In the event of such an objection Processor is obliged to perform this Agreement and to render its services and fulfill its duties without using this subcontractor, while remaining entitled to terminate this Agreement.

11.4. If and to the extent that a subcontractor is given access to Client's Personal Data, Processor is obliged to enter into a data processing agreement with the subcontractor which imposes upon the subcontractor the duties set out in this Agreement. Such agreement must be established before the subcontractor first gains access to Client's Personal Data.

12. Return and Erasure

12.1. Processor is obliged, after the end of this Agreement or earlier, if so requested by Client, to return or to hand over all Personal Data of Client.

12.2. Details of the obligations to erase data are contained may be added in the Annex of this Agreement and, where applicable, by explicit instructions of Client. Processor is not required to have its own erasure plan. Processor is obliged without undue delay after the end of this Agreement or earlier, if so requested by Client, to erase all Personal Data that is not subject to a statutory storage or retention requirement on the part of Processor under the law of the EU or of an EU Member State, or to an explicit agreement to the contrary governing the storage or erasure of Personal Data that has been agreed with Client. Processor shall make and keep records of the erasure.

13. Costs to be Borne by Processor

All costs incurred by Processor or by subcontractors through processing Personal Data on behalf of Client under the terms of this Agreement, particularly those incurred on the basis of

13.1. an obligation to respond to data subject requests on the instructions of Client, in particular to correct, erase, or restrict Personal Data or to return Personal Data to Client and, where applicable, to transfer data (portability), or assisting in such measures,

13.2. an obligation to assist with the data protection impact assessment,

13.3. compliance with or implementation of Client's instructions,

13.4. the obligation to provide assistance in the fulfillment of requirements to disclose information to the regulatory authority or to data subjects,

13.5. the production of a qualified self-assessment,

13.6. on-site inspections by Client or (external) auditors required by Client, unless such inspection has identified considerable shortcomings; the burden of proof in this regard shall be with the Client,

13.7. additional costs for technical and organizational measures for guaranteeing security of the processing, where such measures are put in place as a result of the Parties' differing risk analyses,

13.8. compliance with duties to return or erase Personal Data,

will be reimbursed separately to Processor based on market hourly rates. Processor shall keep records of the costs and expenses incurred.

14. Amendments to this Agreement

If Processor is obliged by law to implement changes and amendments, Client is obliged to support and approve them.

15. Liability

15.1. If a data subject and/or a third party brings action against Processor in connection with data processing activities carried out by Processor on behalf of Client, Client is obliged to indemnify Processor and to pay the associated legal costs, damages, and/or fines under administrative or criminal law.

15.2. Above provision does not apply if Processor has failed to comply with the duties incumbent upon it under the General Data Protection Regulation or has failed to comply with lawfully issued instructions of Client or has acted in contravention of such instructions.

15.3. Liability limits agreed between Client and Processor in favor of Processor in the Main Agreement, also apply to Processor's liability for data processing activities under this Agreement.

Annex

I. Categories of Data Subjects

- Customers
- Others: distributors, network partners

II. Types of Data

- Personnel Master data
- Communication master data
- Customer history

III. Scope of Processing

Client's core requirements are as follows:
Creation and processing of service notifications and orders

IV. Place where Personal Data is to be Processed

EEA

V. Processing System(s), incl. Import and Export of Personal Data from Other Systems

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP und other ERP systems of our distributors, OneSignal Mobile Push Notifications

VI. Processor's Technical and Organizational Security Measures

Implementation of technical and organizational measures

a. Confidentiality (Art. 32 (1) GDPR)

(1) Access control (premises)

- Alarm
- Automatic control of access
- Security locks
- Video surveillance of entries
- Key control / List
- Reception / Gate keeper
- Visitors' list
- Employee / Visitors' ID
- Visitors are in employee's company

(2) Access control (systems)

- Login w/ user name + password
- Antivirus-software server
- Antivirus-software clients
- Firewall
- Intrusion detection systems
- Mobile device management
- use of VPN for remote-access
- Encryption of data storages
- Encryption of smartphones
- BIOS protection (separate password)

(3) Access control (data)

- Administration of user's rights
- Creation of user profiles
- Guideline „Safe passwords"
- Guideline „Deletion / Destruction"
- General guideline data protection and/or data security
- Manual „Manual desktop-lock"
- Frequent training of employees
- Use of authorization scheme
- User-right's administration by admins

(4) Separation control

Separation of productive and test environment

(5) Pseudonymization (Art. 32 (1) GDPR; Art. 25 (1) GDPR)

n/a

b. Availability and resilience (Art. 32 (1) GDPR)

- Fire and smoke detectors
- Fire extinguisher in server room
- Control of temperature and humidity in server room
- Air-conditioned server room
- UPS system
- Safety outlet strip used in server room
- RAID System / mirror image of HD
- Video-surveillance server room
- Alarm signal for unauthorized access to server room
- Backup & recovery-concept (worded)
- Control of backup
- No sanitary equipment in or above server room
- Existence of an emergency plan (iE BSI IT-Grundschutz 100-4)
- Separated partitions for operating systems and data

c. Integrity (Art. 32 Sec. 1 GDPR)

- Personal data can solely be changed by admins
- Supply of encrypted connections such as sftp, https
- Logging of access and retrieval
- Overview on regular processes of retrieval and transfer
- Carefully selected staff

d. Process for regularly testing, assessing and evaluating (Art. 32 (1) GDPR; Art. 25 (1) GDPR)

(1) Data protection management

- Security certification by ISO 27001
- The effectiveness of the technical security measures is reviewed at least once a year
- Employees trained and are obliged to maintain confidentiality

(2) Incident response management

- Use of a firewall and regular updating
- Use of spam-filters and regular updating
- Use of virus-scanner and regular updating
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)

Data protection by default (Art. 25 (2) GDPR)

- The amount of personal data is limited to what is necessary in relation to the purposes for which they are processed

Linde Material Handling

Auftragsverarbeitungsvertrag („Vertrag") in Zusammenhang mit dem Linde Service Manager

Der vorliegende Vertrag verweist auf die allgemeinen Geschäftsbedingungen des „Linde Service Managers" („**AGB**"). Etwaige hervorgehobenen Begriffe, die hierin nicht definiert sind, haben die in den AGB festgelegte Bedeutung.

Der Vertriebspartner („**Klient**" oder „**Verantwortliche**"), vertreten durch den Benutzer, und LMH („**Auftragsverarbeiter**"; zusammen mit dem Verantwortlichen die „**Parteien**") schließen den vorliegenden Vertrag über die Verarbeitung von personenbezogenen Daten in Zusammenhang mit dem Service ab. Der vorliegende Vertrag regelt die Datenschutzverpflichtungen der Parteien in Bezug auf den Schutz der personenbezogenen Daten des Klienten.

1. Begriffsbestimmungen

Im vorliegenden Vertrag haben folgende Begriffe die folgende Bedeutung:

1.1. „**Auftragsverarbeiter**": Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

1.2. „**Dritter**": Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

1.3. „**Personenbezogene Daten**": Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („**betroffene Person**") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

1.4. „**Pseudonymisierung**": Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

1.5. „**Verantwortlicher**": Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

1.6. „**Verarbeitung**": Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung,

das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

1.7. „**Verletzung des Schutzes personenbezogener Daten**": Eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

1.8. „**Hauptvertrag**": Der zwischen LMH und dem Vertriebspartner über den in den AGB definierten Service abgeschlossene Vertrag.

2. Gegenstand und Laufzeit des vorliegenden Vertrags

2.1. Der vorliegende Vertrag regelt die Pflichten des Auftragsverarbeiters in Zusammenhang mit personenbezogenen Daten, die durch diesen für den Klienten verarbeitet werden.

2.2. Die Bestimmungen des vorliegenden Vertrags gelten nicht, wenn und in dem Ausmaß, in dem der Auftragsverarbeiter gemäß seiner Verpflichtung keine Verarbeitungstätigkeiten in Bezug auf die personenbezogenen Daten des Klienten durchzuführen hat. In diesem Fall stellt der Klient sicher, dass seine personenbezogenen Daten auf geeignete Weise vor dem Auftragsverarbeiter geschützt sind.

2.3. Nur der Klient bestimmt, ob die Verarbeitung rechtmäßig ist und stellt sicher, dass die Rechte der betroffenen Personen gewahrt sind.

2.4. Der vorliegende Vertrag tritt mit Inkrafttreten des Hauptvertrags in Kraft und endet mit Laufzeitende des Hauptvertrags. Verarbeitet der Auftragsverarbeiter die personenbezogenen Daten auf Anweisung des Klienten nach Laufzeitende des Hauptvertrags, bleibt der vorliegende Vertrag bestehen, bis die Verarbeitung auf Anweisung des Klienten abgeschlossen ist.

2.5. Ungeachtet der Bestimmung in 2.4 können die Parteien den vorliegenden Vertrag aus wichtigem Grund kündigen. Betrifft der Grund die Verletzung einer Verpflichtung gemäß dem Vertrag, ist eine Kündigung nur nach Ablauf einer für die Behebung der Verletzung festgelegten Frist, in der die Verletzung nicht behoben wurde, oder nach erfolgloser Mahnung zulässig. Ein wichtiger Grund seitens des Auftragsverarbeiters besteht insbesondere, wenn

2.5.1. der Klient wiederholt unrechtmäßige Anweisungen erteilt, der Auftragsverarbeiter den Klienten darüber unverzüglich in Kenntnis setzt und der Klient die Anweisungen nicht zurückzieht;

2.5.2. der Klient die Bestimmungen des vorliegenden Vertrags verletzt;

2.5.3. der Klient der Verpflichtung eines Unterauftragnehmers gemäß dem vorliegenden Vertrag widerspricht.

Des Weiteren gelten die Bestimmungen des Hauptvertrags entsprechend für den vorliegenden Vertrag.

3. Art, Umfang und Ort der Verarbeitung

3.1. Der Auftragsverarbeiter ist berechtigt, auf die personenbezogenen Daten des Klienten zum Zweck der Erbringung von Dienstleistungen gemäß dem Hauptvertrag im in Anhang 1 beschriebenen Ausmaß zuzugreifen. Die Bestimmungen des vorliegenden Vertrags stellen keine Erweiterung der Pflichten des Auftragsverarbeiters dar, sondern legen diese nur ausführlicher dar. Der vorliegende Vertrag regelt auch die Pflichten des Klienten.

3.2. Der Klient kann Anweisungen erteilen, die die Pflichten des Auftragsverarbeiters ausführlicher definieren.

3.3. Der Auftragsverarbeiter darf die personenbezogenen Daten nur für die im Hauptvertrag und im vorliegenden Vertrag beschriebenen Zwecke verwenden und darf ohne ausdrückliche vorhergehende Anweisung des Klienten insbesondere die personenbezogenen Daten nicht an Dritte weitergeben oder sie anderen Empfängern offenlegen, sofern dies durch den vorliegenden Vertrag nicht anders festgelegt ist.

3.4. Sofern im Anhang/in den Anhängen des vorliegenden Vertrags nicht anders festgelegt, ist die Verarbeitung gemäß dem vorliegenden Vertrag auf das Gebiet der Europäischen Union und des EWR beschränkt.

4. Anweisungen des Klienten, Rechte von betroffenen Personen, Datenschutz-Folgenabschätzung

4.1. Der Klient kann durch seine Anweisung(en) die Art, den Umfang und die Art der Datenverarbeitung, Sicherheitsmaßnahmen, die zu verarbeitenden personenbezogenen Daten und die Gruppen betroffener Personen definieren oder aktualisieren. Dies gilt vorwiegend in Fällen, in welchen eine Aufsichtsbehörde oder Änderungen der Rechtsprechung den Klienten veranlassen oder verlangen, Anweisungen zu erteilen. Tritt eine betroffene Person direkt mit dem Auftragsverarbeiter in Kontakt, informiert dieser den Klienten unverzüglich schriftlich und bittet um Anweisungen bezüglich des weiteren Vorgehens.

4.2. Führt der Klient eine Datenschutz-Folgenabschätzung durch, unterstützt ihn der Auftragsverarbeiter gemäß den Anweisungen, sofern dies vernünftig und notwendig ist, einschließlich hinsichtlich etwaiger früherer Konsultationen der zuständigen Aufsichtsbehörde.

4.3. Anweisungen des Klienten sind auf die Umsetzung gesetzlicher oder behördlicher Vorschriften des Datenschutzrechts beschränkt. Sie sind von Änderungsersuchen zu unterscheiden. Änderungsersuchen betreffen Änderungen des Umfangs von Dienstleistungen, die nicht erforderlich sind, um gesetzliche oder behördliche Vorschriften umzusetzen oder die über die zur Umsetzung solcher Vorschriften notwendigen Maßnahmen hinausgehen. Es handelt sich nicht um Anweisungen im Sinne des vorliegenden Vertrags, sondern um Ersuchen durch den Klienten in Bezug auf Änderungen an Dienstleistungen. Der Auftragsverarbeiter hat das Recht, ist aber nicht verpflichtet, solchen Änderungsersuchen nachzukommen. Die Umsetzung von Änderungsersuchen wird separat bezahlt.

4.4. Der Klient erteilt Anweisungen immer schriftlich per Fax oder E-Mail. Der Klient bestätigt etwaige ausnahmsweise mündlich erteilten Anweisungen unverzüglich in Schrift- oder Textform.

4.5. Der Auftragsverarbeiter informiert den Klienten unverzüglich in Textform, wenn er der Ansicht ist, dass eine Anweisung des Klienten Datenschutzbestimmungen verletzt oder über ein nur vernachlässigbares Ausmaß hinaus fehlerhaft, unvollständig, widersprüchlich oder rechtlich oder technisch nicht durchführbar ist. Im Zuge dieses Informierens bringt der Auftragsverarbeiter den

Klienten ausdrücklich in Textform in Kenntnis, dass dieser unverzüglich festlegt, ob er wünscht, dass der Auftragsverarbeiter die Anweisung ausführt oder die personenbezogenen Daten ohne Ausführung der Anweisung weiter verarbeitet, bis er die Informationen geprüft und zu einer Entscheidung gefunden hat.

5. Pflichten des Auftragsverarbeiter in Hinblick auf die Zurverfügungstellung von Informationen

5.1. Im Falle der Verletzung des Schutzes personenbezogener Daten kann es sein, dass der Klient verpflichtet ist, die Verletzung zu melden. Der Auftragsverarbeiter informiert den Klienten, wenn er die Verletzung des Schutzes der personenbezogenen Daten des Klienten durch den Auftragsverarbeiter oder Personen, für die der Auftragsverarbeiter verantwortlich ist, vermutet oder sich dieser sicher ist (wenn diese über ein vernachlässigbares Ausmaß hinausgeht).

5.2. Der Klient kann verlangen, dass der Auftragsverarbeiter alle vernünftigen und notwendigen Schritte ergreift, um den Klienten bei der Erfüllung seiner Meldepflichten zu unterstützen.

6. Pflichten des Klienten

6.1. Der Klient informiert den Auftragsverarbeiter unverzüglich, wenn bei Überprüfung des Ergebnisses der erbrachten Dienstleistung Fehler oder Unregelmäßigkeiten festgestellt werden.

6.2. Der Klient muss sich sowohl vor Beginn der Datenverarbeitung als auch danach selbst überzeugen, dass die durch den Auftragsverarbeiter ergriffenen technischen und organisatorischen Maßnahmen eingehalten werden. Das Ergebnis solcher Überprüfungen muss dokumentiert werden.

6.3. Der Klient ist verantwortlich für die Einhaltung der aus Art. 33, 34 der Datenschutzgrundverordnung der EU hervorgehenden Verpflichtungen gegenüber der Aufsichtsbehörde oder etwaigen durch eine Verletzung des Schutzes personenbezogener Daten betroffenen Personen.

6.4. Der Klient informiert den Auftragsverarbeiter in Bezug auf Vorschriften hinsichtlich der Löschung und der Speicherung von personenbezogenen Daten und die Einhaltung dieser Vorschriften.

7. Datenschutzbeauftragter

7.1. Der Auftragsverarbeiter ernennt einen Datenschutzbeauftragten („**DSB**"). Dieser kann unter datenschutz@kiongroup.com kontaktiert werden. Der Auftragsverarbeiter informiert den Klienten in Bezug auf Änderungen oder bevorstehende Änderungen in diesem Zusammenhang.

7.2. Der Klient hat einen Datenschutzbeauftragten ernannt oder, sollte der Klient keinen Datenschutzbeauftragten ernennen müssen und dies auch nicht getan haben, nennt dem Auftragsverarbeiter den Namen einer für den Klienten tätigen Person, die die Pflichten und Verantwortung eines Datenschutzbeauftragten übernommen hat. Der Klient informiert den Auftragsverarbeiter, ohne Aufforderung durch diesen, in Bezug auf Änderungen oder bevorstehende Änderungen in diesem Zusammenhang.

7.3. Wenn der Klient einen Vertreter im Sinne von Art. 27 der Datenschutzgrundverordnung der EU ernennen muss, informiert er den Auftragsverarbeiter darüber, wer dieser Vertreter ist. Der Klient informiert den Auftragsverarbeiter, ohne Aufforderung durch diesen, in Bezug auf Änderungen oder bevorstehende Änderungen in diesem Zusammenhang.

8. Personen, für die der Auftragsverarbeiter verantwortlich ist

8.1. Bei Durchführung von Datenverarbeitung gemäß dem vorliegenden Vertrag setzt der Auftragsverarbeiter nur Personen ein, die eine dokumentierte Vertraulichkeitsvereinbarung unterzeichnet haben und vorab mit den für sie und die für den Klienten durchzuführenden Datenverarbeitungstätigkeiten relevanten gesetzlichen Datenschutzbestimmungen vertraut gemacht wurden.

8.2. Der Auftragsverarbeiter stellt sicher, dass alle Personen, für die er verantwortlich ist und die Zugriff auf die personenbezogenen Daten des Klienten haben, personenbezogene Daten nur im Umfang gemäß den Anweisungen des Klienten und gemäß den Bestimmungen des vorliegenden Vertrags verarbeiten. Die einzige Ausnahme in Bezug auf die oben angeführte Bestimmung betrifft einzelne Fälle von Verarbeitungstätigkeiten, insbesondere die Übertragung von Daten, zu welchen der Auftragsverarbeiter oder die Personen, für die dieser verantwortlich ist, durch ein Gericht oder eine Regierungsbehörde auf Grundlage einer gesetzlichen Bestimmung ausdrücklich aufgefordert wird/werden. Der Auftragsverarbeiter informiert den Klienten im gesetzlich zulässigen Ausmaß über solche Anordnungen, vorzugsweise bevor personenbezogene Daten übertragen werden.

9. Grundsätze der sicheren Verarbeitung

9.1. In Anbetracht der derzeit verfügbaren Technologie, der Umsetzungskosten und der Art, des Umfangs, der Umstände und der Zwecke der mit dem Klienten vereinbarten Datenverarbeitung sowie der Wahrscheinlichkeit und möglichen Schwere des Risikos für die Rechte und Freiheiten von Einzelpersonen (Risikoanalyse) ergreift der Auftragsverarbeiter die zur Sicherstellung eines geeigneten Schutzes der personenbezogenen Daten erforderlichen technischen und organisatorischen Maßnahmen.

9.2. Bei der Bewertung der Sicherheitsstufe berücksichtigt der Auftragsverarbeiter die der Verarbeitung der personenbezogenen Daten des Klienten innewohnenden Risiken, einschließlich, aber nicht beschränkt auf das Risiko der versehentlichen oder unrechtmäßigen Zerstörung und des Verlusts, der Änderung oder unzulässigen Offenbarung von oder des unzulässigen Zugriffs auf personenbezogene Daten des Klienten.

9.3. Der Auftragsverarbeiter aktualisiert und adaptiert die technischen und organisatorischen Maßnahmen, die Teil seines Sicherheitsplans sind, um einer geänderten verfügbaren Technologie Rechnung zu tragen, wobei diese Maßnahmen jedoch nicht die im vorliegenden Vertrag angeführte Sicherheits- und Schutzstufe unterschreiten dürfen.

9.4. Der Auftragsverarbeiter dokumentiert die technischen und organisatorischen Maßnahmen gemäß dem vorliegenden Vertrag ausführlich im Anhang des vorliegenden Vertrags. Der Auftragsverarbeiter muss die Dokumentation aktuell halten und jede erhebliche Veränderung dokumentieren.

9.5. Die technischen und organisatorischen Maßnahmen im Anhang des vorliegenden Vertrags werden bei Vertragsabschluss als genehmigt und notwendig erachtet; sie repräsentieren alle Vorschriften, denen der Auftragsverarbeiter nachkommen muss.

9.6. Der Klient ist verpflichtet, die technischen und organisatorischen Maßnahmen auf Grundlage seiner eigenen Risikoanalyse zu prüfen. Der Klient ist verantwortlich dafür, sicherzustellen, dass

die technischen und organisatorischen Maßnahmen ein Ausmaß an Datenschutz bieten, das den Risiken für die zu verarbeitenden personenbezogenen Daten angemessen ist. Liefert die Risikoanalyse des Klienten ein Ergebnis, das sich von der Risikoanalyse des Auftragsverarbeiters unterscheidet, hat der Klient das Recht, mit dem Auftragsverarbeiter eine Anpassung der Sicherheitsmaßnahmen auszuhandeln. Können sich die Parteien nicht einigen, haben beide das Recht, den Vertrag nach einer 14-tägigen Kündigungsfrist zu kündigen.

10. Kontrollen

10.1. Der Klient ist berechtigt, die Erbringung der Dienstleistungen durch den Auftragsverarbeiter in Bezug auf die personenbezogenen Daten und die Einhaltung der Bestimmungen des vorliegenden Vertrags zu überprüfen, einschließlich, aber nicht beschränkt auf die technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

10.2. Auf Anfrage stellt der Auftragsverarbeiter dem Klienten Nachweise in Bezug auf die Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen bereit. Dies umfasst

- einen Nachweis der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 der Datenschutzgrundverordnung oder
- eine Zertifizierung gemäß einem genehmigten Zertifizierungsverfahren gemäß Art. 42 der Datenschutzgrundverordnung oder
- eine qualifizierte Selbstbewertung von unabhängigen Dritten (wie z.B. DSB, Prüfer, externen Datenschutz-/Sicherheitsprüfern) in Textform oder
- eine geeignete Zertifizierung durch eine IT-Sicherheits- oder Datenschutzprüfung (z.B. ISO 27001).

Ein solcher Nachweis muss alle Informationen enthalten, die erforderlich sind, um die Erfüllung und Umsetzung der Pflichten gemäß dem vorliegenden Vertrag und der relevanten technischen und organisatorischen Maßnahmen zu beweisen, welche die Sicherheit der Verarbeitung gewährleisten sollen. Der Klient kann diese Informationen ein Mal pro Kalenderjahr und in kürzeren Abständen nur dann einfordern, wenn ein berechtigter Verdacht vorliegt, dass der Auftragsverarbeiter den vorliegenden Vertrag gebrochen hat, worüber der Klient den Auftragsverarbeiter in Textform informieren muss.

10.3. Der Klient ist berechtigt, die Erfüllung des Vertrags, insbesondere die Erfüllung in Bezug auf die Sicherheit der Verarbeitung, durch Durchführung vorab angekündigter Inspektionen in den Geschäftsräumen des Auftragsverarbeiters während der üblichen Geschäftszeiten (9:00 bis 18:00 Uhr) ein Mal alle drei Jahre zu überprüfen oder solche Überprüfungen durch einen externen Prüfer durchführen zu lassen, der gesetzlichen oder vertraglichen Geheimhaltungsverpflichtungen unterliegt. Der Klient muss solche Inspektionen zwei Wochen im Voraus schriftlich ankündigen. Diese Einschränkung für den Klienten gilt nicht in dringenden Fällen (z.B. wenn ein Verdacht bezüglich mehr als vernachlässigbarer Verletzungen des vorliegenden Vertrags durch den Auftragsverarbeiter besteht); der Klient muss den Auftragsverarbeiter in solchen Fällen schriftlich vorab nicht benachrichtigen.

11. Unterauftragnehmer

11.1. Falls und in dem Ausmaß, in dem der Auftragsverarbeiter auf Grundlage einer ausdrücklichen Vereinbarung mit dem Klienten berechtigt ist, zusätzliche Auftragsverarbeiter (Unterauftragnehmer) zu beschäftigen, und wenn nicht ausgeschlossen werden kann, dass diese Unterauftragnehmer Zugriff auf die personenbezogenen Daten des Klienten haben, darf der Auftragsverarbeiter nur Unterauftragnehmer beschäftigen und diesen dadurch Zugriff auf die

personenbezogenen Daten des Klienten gewähren, wenn er den Klienten schriftlich über die im nachstehenden Absatz angeführten Angaben informiert hat und dem Klienten die Möglichkeit eingeräumt hat, Einspruch zu erheben, und der Klient innerhalb der festgelegten Frist keinen Einspruch erhoben hat.

11.2. Die wie oben dargelegt durch den Auftragsverarbeiter zur Verfügung zu stellenden Informationen müssen zumindest folgende Angaben in konkreter und ausführlicher Form einschließen:

11.2.1. die Identität des Unterauftragnehmers,

11.2.2. die konkreten Dienstleistungen, die der Unterauftragnehmer für den Auftragsverarbeiter erbringt,

11.2.3. die Erfahrung, Fähigkeiten, Zuverlässigkeit, IT-Sicherheits- und Datenschutzmaßnahmen, die für die Einhaltung von Datenschutzverpflichtungen im vorliegenden Vertrag wesentlich sind,

11.2.4. die Garantien oder Zusicherungen des Unterauftragnehmers, dass dieser die Bestimmungen des vorliegenden Vertrags einhält.

11.3. Der Klient ist berechtigt, innerhalb von sieben Tagen nach Erhalt der oben angeführten Informationen schriftlich Einspruch gegen die Beschäftigung eines Unterauftragnehmers zu erheben, vorausgesetzt er hat einen legitimen Grund dafür. Wird derart Einspruch erhoben, ist der Auftragsverarbeiter verpflichtet, den vorliegenden Vertrag zu erfüllen und seine Dienstleistungen zu erbringen und seine Verpflichtungen zu erfüllen, ohne diesen Unterauftragnehmer zu beschäftigen, wobei er weiterhin berechtigt ist, den vorliegenden Vertrag zu kündigen.

11.4. Falls und in dem Ausmaß, in dem ein Unterauftragnehmer Zugriff zu den personenbezogenen Daten des Klienten erhält, ist der Auftragsverarbeiter verpflichtet, einen Datenverarbeitungsvertrag mit dem Unterauftragnehmer abzuschließen, welcher dem Unterauftragnehmer die im vorliegenden Vertrag dargelegten Pflichten auferlegt. Ein solcher Vertrag muss abgeschlossen werden, bevor der Unterauftragnehmer erstmals Zugriff auf die personenbezogenen Daten des Klienten erhält.

12. Rückgabe und Löschung

12.1. Der Auftragsverarbeiter ist verpflichtet, alle personenbezogenen Daten des Klienten nach Ende des vorliegenden Vertrags oder nach Aufforderung durch den Klienten auch früher zurückzugeben oder auszuhändigen.

12.2. Details in Bezug auf die Verpflichtungen zum Löschen von Daten können im Anhang des vorliegenden Vertrags und gegebenenfalls durch ausdrückliche Anweisungen des Klienten hinzugefügt werden. Der Auftragsverarbeiter ist nicht verpflichtet, einen eigenen Plan für die Löschung zu erstellen. Der Auftragsverarbeiter ist verpflichtet, nach Ende des vorliegenden Vertrags oder nach Aufforderung durch den Klienten auch früher alle personenbezogenen Daten unverzüglich zu löschen, die keinen gesetzlichen Speicherverpflichtungen seitens des Auftragsverarbeiters gemäß EU-Recht oder dem Recht eines EU-Mitgliedsstaats oder einer mit dem Klienten abgeschlossenen, ausdrücklichen gegenteiligen Vereinbarung in Bezug auf das Speichern und Löschen von personenbezogenen Daten unterliegen. Der Auftragsverarbeiter muss eine Aufzeichnung der Löschung anfertigen und aufheben.

13. Durch den Auftragsverarbeiter zu tragende Kosten

Alle dem Auftragsverarbeiter oder Unterauftragnehmer durch die Verarbeitung personenbezogener Daten im Auftrag des Klienten gemäß den Bestimmungen des vorliegenden Vertrags entstandenen Kosten, insbesondere jene, die aufgrund

13.1. einer Verpflichtung zur Beantwortung von Anfragen von betroffenen Personen nach Anweisungen des Klienten, insbesondere zur Korrektur, Löschung oder Einschränkung von personenbezogenen Daten oder zur Rückgabe personenbezogener Daten an den Klienten und gegebenenfalls zur Übertragung von Daten (Portabilität) oder durch Unterstützung solcher Maßnahmen,

13.2. einer Verpflichtung zur Unterstützung einer Datenschutz-Folgenabschätzung,

13.3. die Erfüllung oder Umsetzung von Anweisungen des Klienten,

13.4. die Verpflichtung zur Unterstützung bei der Erfüllung von Verpflichtungen zur Offenlegung von Informationen gegenüber der Aufsichtsbehörde oder betroffenen Personen,

13.5. die Erstellung einer qualifizierten Selbsteinschätzung,

13.6. durch den Klienten oder (externe) Prüfer auf Ansuchen des Klienten vor Ort durchgeführte Inspektionen, wenn durch diese nicht beträchtliche Mängel aufgezeigt wurden, wobei die Beweislast in diesem Fall beim Klienten liegt,

13.7. zusätzliche Kosten für technische und organisatorische Maßnahmen zur Sicherstellung der Verarbeitungssicherheit, wenn solche Maßnahmen infolge unterschiedlicher Risikoanalysen der Parteien ergriffen werden,

13.8. die Erfüllung von Verpflichtungen zur Rückgabe oder Löschung von personenbezogenen Daten

entstandene Kosten werden dem Auftragsverarbeiter auf Grundlage marktüblicher Stundensätze separat rückerstattet. Der Auftragsverarbeiter führt Aufzeichnungen über die angefallenen Kosten und Ausgaben.

14. Änderungen des vorliegenden Vertrags

Ist der Auftragsverarbeiter gesetzlich verpflichtet, Änderungen und Ergänzungen umzusetzen, ist der Klient verpflichtet, diese zu unterstützen und zu genehmigen.

15. Haftung

15.1. Erhebt eine betroffene Person und/oder ein Dritter Klage gegen den Auftragsverarbeiter in Zusammenhang mit durch diesen für den Klienten durchgeführten Datenverarbeitungstätigkeiten ist der Klient verpflichtet, den Auftragsverarbeiter schadlos zu halten und die entstandenen Prozesskosten, Schadenersatzkosten und/oder Verwaltungs- oder strafrechtlichen Strafen zu tragen.

15.2. Die oben angeführte Bestimmung gilt nicht, wenn der Auftragsverarbeiter seinen Verpflichtungen gemäß der Datenschutzgrundverordnung nicht nachgekommen ist oder rechtmäßig erteilte Anweisungen des Klienten nicht eingehalten hat oder solchen Anweisungen zuwidergehandelt hat.

15.3. Die zwischen dem Klienten und dem Auftragsverarbeiter im Hauptvertrag vereinbarten Haftungsgrenzen zugunsten des Auftragsverarbeiters gelten auch für die Haftung des Auftragsverarbeiters für Datenverarbeitungstätigkeiten gemäß dem vorliegenden Vertrag.

Linde Material Handling

Anhang

I. Kategorien betroffener Personen

- Kunden
- Weitere: Vertriebspartner, Netzwerkpartner

II. Datentypen

- Personalstammdaten
- Kommunikationsstammdaten
- Kunden-Chronik

III. Verarbeitungsumfang

Dies sind die wichtigsten Anforderungen des Klienten:
Erstellen und Verarbeiten von Service-Benachrichtigungen und Befehlen

IV. Ort, an dem die Verarbeitung personenbezogener Daten erfolgt

EWR

V. Verarbeitungssystem(e), inkl. Import und Export von personenbezogenen Daten aus anderen Systemen

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP und andere ERP-Systeme unserer Vertriebspartner,
OneSignal Mobile Push Notifications

VI. Technische und organisatorische Sicherheitsmaßnahmen des Auftragsverarbeiters

Umsetzung technischer und organisatorischer Maßnahmen

a. Vertraulichkeit (Art. 32 (1) DSGVO)

(1) Zutrittskontrolle (Räumlichkeiten)

- Alarm
- Automatische Zutrittskontrolle
- Sicherheitsschlösser
- Videoüberwachung der Eingänge
- Schlüsselüberprüfung / Liste
- Empfang / Pförtner
- Besucherliste
- ID von Angestellten / Besuchern
- Besucher befinden sich in Begleitung eines Angestellten

(2) Zugriffskontrolle (Systeme)

- Login mit Benutzername + Passwort
- Antivirus-Software Server
- Antivirus-Software Clients
- Firewall
- Angriffserkennungssysteme
- Mobilgerätmanagement
- Nutzung von VPN für Fernzugriff

- Verschlüsselung Datenspeicherung
- Verschlüsselung Smartphones
- BIOS-Schutz (eigenes Passwort)

(3) Zugriffskontrolle (Daten)

- Verwaltung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Richtlinie „Sichere Passwörter“
- Richtlinie „Löschen / Zerstören“
- Allgemeine Richtlinie zu Datenschutz und/oder Datensicherheit
- Handbuch „Manuelle Desktop-Sperre“
- Häufige Weiterbildung von Angestellten
- Verwendung eines Autorisierungsschemas
- Verwaltung von Benutzerrechten durch Administratoren

(4) Trennungskontrolle

Trennung von Produktiv- und Testumgebung

(5) Pseudonymisierung (Art. 32 (1) DSGVO; Art. 25 (1) DSGVO)

k.A.

b. Verfügbarkeit und Belastbarkeit (Art. 32 (1) DSGVO)

- Feuer- und Rauchdetektoren
- Feuerlöscher im Serverraum
- Steuerung von Temperatur und Luftfeuchtigkeit im Serverraum
- Klimatisierter Serverraum
- UPS-System
- Verwendung von Sicherheitssteckdosenleiste im Serverraum
- RAID-System / Spiegelfestplatte
- Videoüberwachung Serverraum
- Alarmsignal bei unautorisiertem Zutritt zu Serverraum
- Backup- & Wiederherstellungskonzept (ausformuliert)
- Backup-Kontrolle
- Keine Sanitäreinrichtungen in oder über dem Serverraum
- Vorliegen eines Notfallplans (iE BSI IT-Grundschutz 100-4)
- Getrennte Partitionen für Betriebssysteme und Daten

c. Integrität (Art. 32 Abschnitt 1 DSGVO)

- Personenbezogene Daten können nur durch Administratoren geändert werden
- Verfügbarkeit verschlüsselter Verbindungen wie sftp, https
- Aufzeichnung von Zugriff und Abfrage
- Überblick über reguläre Abfrage- und Übertragungsprozesse
- Sorgfältig ausgewählte Mitarbeiter

d. Prozess für regelmäßige Überprüfung, Bewertung und Evaluierung (Art. 32 (1) DSGVO; Art. 25 (1) DSGVO)

(1) Datenschutzmanagement

- Sicherheitszertifizierung gemäß ISO 27001
- Die Wirksamkeit der technischen Sicherheitsmaßnahmen wird zumindest ein Mal pro Jahr überprüft
- Ausgebildete Mitarbeiter sind zur Vertraulichkeit verpflichtet

(2) Vorfalls-Reaktions- Management

- Verwendung einer Firewall und regelmäßige Updates
- Verwendung von Spamfiltern und regelmäßige Updates
- Verwendung eines Virus-Scanners und regelmäßige Updates
- Angriffserkennungssysteme
- Angriffspräventionssystem

Datenschutzfreundliche Voreinstellungen (Art. 25 (2) DSGVO)

- Die Menge an personenbezogenen Daten ist auf die für den Zweck von deren Verarbeitung erforderliche Menge beschränkt

Linde Material Handling

Smlouva o zpracování údajů (dále označovaná jako „Smlouva“) vztahující se k aplikaci Linde Service Manager

Tato Smlouva se vztahuje ke všeobecným smluvním podmínkám aplikace „Linde Service Manager“ (dále označovaným jako „**Všeobecné smluvní podmínky**“). Jakékoli pojmy s velkým počátečním písmenem, které jsou zde použity, ale které zde nejsou definovány, mají význam, který je jim připsán ve Všeobecných smluvních podmínkách.

Distributor (dále označovaný jako „**Klient**“ nebo „**Správce**“), zastoupený Uživatelem, a společnost LMH (dále označovaná jako „**Zpracovatel**“ a společně se Správcem označované jako „**Smluvní strany**“) uzavírají tuto Smlouvu o zpracování osobních údajů vztahující se ke Službě. Tato Smlouva řídí ochranu údajů a povinnosti Smluvních stran související s ochranou osobních údajů Klienta.

1. Výklad pojmů

V této Smlouvě mají následující pojmy níže uvedený význam:

1.1. „**Zpracovatel**“: fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo jiný orgán, který zpracovává osobní údaje jménem Správce.

1.2. „**Třetí osoba**“: fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo orgán jiný než subjekt údajů, správce, zpracovatel nebo osoby, které jsou správcem nebo zpracovatelem přímo oprávněny zpracovávat osobní údaje.

1.3. „**Osobní údaje**“: jakékoli informace vztahující se k identifikované nebo identifikovatelné osobě (dále označované jako „**Subjekt údajů**“); identifikovatelnou fyzickou osobou je míněna taková osoba, kterou lze přímo nebo nepřímo identifikovat, zejména odkazem na identifikátor, jako je například jméno, identifikační číslo, údaje o místě, on-line identifikátorem, či odkazem na jeden nebo více faktorů, které jsou specifické z hlediska fyzické, psychické, genetické, duševní, ekonomické, kulturní nebo sociální identity dané fyzické osoby.

1.4. „**Pseudonymizace**“: zpracování osobních údajů takovým způsobem, že osobní údaje již nebude možné připsat konkrétnímu subjektu údajů bez použití dalších informací, a to za předpokladu, že tyto další informace jsou uchovávány odděleně a vztahují se na ně technická a organizační opatření, jejichž cílem je zajistit, že tyto osobní údaje nebudou připsány žádné identifikované nebo identifikovatelné fyzické osobě.

1.5. „**Správce**“: fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo jiný orgán, který sám nebo společně s jinými stanoví účely a prostředky zpracování osobních údajů; v případě, že jsou účely a prostředky takového zpracování stanoveny legislativou Unie nebo Členského státu, mohou být správce nebo konkrétní kritéria pro jeho nominaci zajištěna legislativou Unie nebo Členského státu.

1.6. „**Zpracování**“: jakékoli operace nebo soubor operací, které se provádějí s osobními údaji nebo soubory osobních údajů, bez ohledu na to, zda automatickými prostředky, jako je například shromažďování, zaznamenávání, organizování, strukturování, uchovávání, úprava nebo změna, vyhledávání, konzultování, využití, zpřístupnění převodem, rozšiřováním nebo jiným způsobem, srovnávání či kombinování, omezování, výmaz nebo zničení.

1.7. „**Porušení ochrany osobních údajů**“: porušení zabezpečení, které vede k náhodnému nebo nezákonnému zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k přenášeným, uchovávaným či jinak zpracovávaným osobním údajům.

1.8. „**Rámcová smlouva**“: smlouva uzavřená mezi společností LMH a Distributorem, která se vztahuje ke Službám, jak je uvedeno ve Všeobecných smluvních podmínkách.

2. Předmět a doba platnosti této Smlouvy

2.1. Tato Smlouva řídí povinnosti Zpracovatele, které se týkají Osobních údajů Klienta zpracovávaných Zpracovatelem jménem Klienta.

2.2. Ustanovení této Smlouvy se nepoužijí v tom rozsahu, v němž podle ujednání Zpracovatel nemusí provádět činnosti zpracování Osobních údajů Klienta. V takovém případě Klient zajistí, že jeho Osobní údaje nebudou Zpracovateli k dispozici.

2.3. Výhradně Klient musí určit, zda je Zpracování zákonné, a zajistit, aby byla chráněna práva subjektů údajů.

2.4. Počátek platnosti této Smlouvy se shoduje s počátkem platnosti Rámcové smlouvy a její konec se shoduje s koncem doby platnosti Rámcové smlouvy. Pokud Zpracovatel zpracovává Osobní údaje na základě pokynů Klienta i po uplynutí platnosti Rámcové smlouvy, zůstává i tato Smlouva v platnosti, dokud není Zpracování prováděné podle pokynů Klienta dokončeno.

2.5. Bez ohledu na ustanovení uvedené v odstavci 2.4 mohou Smluvní strany tuto Smlouvu ukončit z dobré příčiny. Pokud se tato příčina vztahuje k porušení povinnosti vyplývající ze Smlouvy, je ukončení možné až po marném uplynutí lhůty stanovené k nápravě takového porušení nebo pokud výstraha neměla žádný účinek. Dobrou příčinou na straně Zpracovatele může být zejména, když

2.5.1. Klient opakovaně vydává nezákonné pokyny, o čemž Zpracovatel Klienta neprodleně informoval a Klient své pokyny nezrušil;

2.5.2. Klient porušil ustanovení této Smlouvy;

2.5.3. Klient měl námitky proti kontrahování subdodavatele podle této Smlouvy.

Podmínky Rámcové smlouvy dále platí analogicky podle této Smlouvy.

3. Charakter, rozsah a místo Zpracování

3.1. Zpracovatel je oprávněn přistupovat k Osobním údajům Klienta za účelem poskytování služeb podle Rámcové smlouvy v rozsahu popsaném v Příloze 1. Ustanovení této Smlouvy nerozšiřují povinnosti Zpracovatele, ale pouze je podrobněji specifikují. Touto Smlouvou se také řídí povinnosti Klienta.

3.2. Klient může vydávat pokyny, které podrobněji specifikují povinnosti Zpracovatele.

3.3. Zpracovatel nesmí používat Osobní údaje pro jiné účely, než jak je popsáno v Rámcové smlouvě a v této Smlouvě, a zejména nesmí bez předchozího výslovného pokynu Klienta převádět Osobní údaje na třetí osobu nebo je zpřístupňovat jiným příjemcům, není-li v této Smlouvě uvedeno něco jiného.

3.4. Zpracování podle této Smlouvy je omezeno na území Evropské unie a EHP, není-li něco jiného uvedeno v Příloze/Přílohách k této Smlouvě.

4. Pokyny Klienta, práva Subjektů údajů a posouzení vlivu na ochranu osobních údajů

4.1. Prostřednictvím svého pokynu / svých pokynů je Klient oprávněn specifikovat nebo aktualizovat charakter, rozsah a způsob zpracování údajů, bezpečnostní opatření, Osobní údaje, které mají být zpracovávány, a skupiny subjektů údajů. Výše uvedené se vztahuje především na případy, kdy regulační orgán nebo změny v legislativě způsobí či vyžadují vydání pokynů na straně Klienta. Obrátí-li se Subjekty údajů na Zpracovatele přímo, Zpracovatel je povinen neprodleně informovat Klienta písemnou formou a požádat jej o pokyny, jak má postupovat.

4.2. Pokud Klient provádí hodnocení vlivu na ochranu osobních údajů, Zpracovatel je povinen mu pomoci v souladu s pokyny, které obdrží, do té míry, do jaké jsou tyto pokyny přiměřené a potřebné, a to i s ohledem na případné předchozí konzultace s kompetentním regulačním orgánem.

4.3. Pokyny Klienta jsou omezeny na zavádění zákonných či regulačních požadavků legislativy týkající se ochrany údajů. Tyto požadavky je třeba odlišovat od změnových požadavků. Změnové požadavky se vztahují ke změnám rozsahu služeb, které nejsou vyžadovány za účelem zavádění zákonných či regulačních požadavků nebo které překračují rámec opatření potřebných k zavedení takových požadavků. Nejedná se o pokyny ve smyslu této Smlouvy, ale o požadavky Klienta na změny služeb. Zpracovatel je oprávněn, ale nikoli povinen, tyto změnové požadavky realizovat. Realizace změnových požadavků bude uhrazena zvlášť.

4.4. Klient bude vždy vydávat pokyny písemně, faxem nebo e-mailem. Klient neprodleně písemně nebo textovou formou potvrdí jakékoli pokyny výjimečně vydané ústně.

4.5. Zpracovatel je povinen neprodleně informovat Klienta písemnou formou, pokud Zpracovatel dospěje k názoru, že nějaký pokyn Klienta je v rozporu s ustanoveními na ochranu údajů, nebo pokud je jinak než zcela zanedbatelným způsobem chybný, nekompletní, rozporný nebo neuskutečnitelný z právního či technického hlediska. Při poskytování těchto informací je Zpracovatel povinen výslovně upozornit Klienta písemnou formou, aby se neprodleně vyjádřil, zda si přeje, aby Zpracovatel daný pokyn splnil, nebo pokračoval ve zpracování Osobních údajů bez splnění daného pokynu, dokud Klient neprovede revizi informací a nedospěje k rozhodnutí.

5. Povinnosti zpracovatele poskytovat informace

5.1. V případě porušení ochrany osobních údajů má Klient případně povinnost takové porušení ohlásit. Zpracovatel je povinen informovat Klienta, pokud má podezření nebo si je vědom (více než pouze zanedbatelným způsobem), že došlo k porušení Osobních údajů Klienta Zpracovatelem nebo osobami, nad nimiž má Zpracovatel kontrolu.

5.2. Klient může požadovat, aby Zpracovatel podnikl veškeré přiměřené a potřebné kroky a pomohl Klientovi splnit všechny požadavky vztahující se k jeho ohlašovací povinnosti.

6. Povinnosti Klienta

6.1. Klient je povinen neprodleně informovat Zpracovatele, zjistí-li chyby nebo nesrovnalosti při kontrole výstupu z poskytované služby.

6.2. Klient je povinen se uspokojivě přesvědčit (jak před zahájením zpracování údajů, tak poté), že technická a organizační opatření zavedená na straně Zpracovatele jsou dodržována. Výstup z těchto kontrol musí být zdokumentován.

6.3. Klient nese odpovědnost za dodržování povinností vyplývajících z článků 33 a 34 Obecného nařízení o ochraně osobních údajů EU vůči regulačnímu orgánu nebo jakémukoliv subjektu údajů, jehož se porušení ochrany osobních údajů dotýká.

6.4. Klient je povinen informovat Zpracovatele o požadavcích na výmaz a uchování Osobních údajů a nese odpovědnost za realizaci těchto požadavků.

7. Pověřenec pro ochranu osobních údajů

7.1. Zpracovatel jmenoval pověřence pro ochranu osobních údajů (dále označovaného jako „**DPO**“, z angl. *Data Protection Officer*). Jeho kontaktní údaje jsou následující: datenschutz@kiongroup.com. Zpracovatel je povinen oznámit Klientovi změny nebo předpokládané změny týkající se výkonu této funkce.

7.2. Klient ustanovil pověřence pro ochranu osobních údajů nebo (v případě, že Klient není povinen ustanovit pověřence pro ochranu osobních údajů a tohoto pověřence neustanovil) Klient poskytne Zpracovateli jméno osoby na straně Klienta, která převzala povinnosti a odpovědnost pověřence pro ochranu osobních údajů. Klient je povinen informovat Zpracovatele o změnách nebo předpokládaných změnách v tomto směru, aniž by jej Zpracovatel o uvedené konkrétně požádal.

7.3. Pokud je Klient povinen jmenovat zástupce ve smyslu článku 27 Obecného nařízení o ochraně osobních údajů EU, bude Zpracovatele informovat o osobě tohoto zástupce. Klient je povinen informovat Zpracovatele o změnách nebo předpokládaných změnách v tomto směru, aniž by jej Zpracovatel o uvedené konkrétně požádal.

8. Osoby pod kontrolou Zpracovatele

8.1. Pro výkon zpracování údajů v souladu s podmínkami této Smlouvy je Zpracovatel povinen využívat pouze osoby, které se písemně zavázaly zachovávat mlčenlivost a které byly předem seznámeny se zákonnými ustanoveními na ochranu osobních údajů, která se vztahují na ně a na činnosti zpracování, které mají být vykonávány jménem Klienta.

8.2. Zpracovatel je povinen zajistit, že všechny osoby pod jeho kontrolou, které mají přístup k Osobním údajům Klienta, budou tyto Osobní údaje zpracovávat pouze v souladu s pokyny Klienta a v rozsahu daném těmito pokyny a ustanoveními této Smlouvy. Jediná výjimka z výše uvedeného ustanovení se týká jednotlivých případů činností zpracování, zejména přenosu dat, kdy je Zpracovateli nebo osobám pod jeho kontrolou výslovně nařízeno provést úkon ze strany soudu nebo orgánu státní správy na základě zákonného ustanovení. V rozsahu, v jakém to umožňuje zákon, je Zpracovatel povinen informovat Klienta o těchto nařízeních, a to nejlépe dříve, než je proveden jakýkoliv převod Osobních údajů.

9. Zásady zabezpečení zpracování

9.1. S ohledem na současnou technologii, pořizovací náklady a charakter, rozsah, okolnosti a účely Zpracování údajů sjednaného s Klientem i na pravděpodobnost a případnou závažnost rizik pro práva a svobody fyzických osob (analýza rizik) Zpracovatel zavede technická a organizační opatření, která jsou zapotřebí pro zajištění, že Osobní údaje budou vhodným způsobem chráněny.

9.2. Při posuzování vhodné úrovně zabezpečení je Zpracovatel povinen zohlednit rizika vyplývající ze zpracování Osobních údajů Klienta, včetně například rizika nenávratného a protiprávního zničení a ztráty, úpravy či neoprávněného zpřístupnění Osobních údajů Klienta nebo neoprávněného přístupu k nim.

9.3. Zpracovatel je povinen aktualizovat a upravit technická a organizační opatření ve svém plánu zabezpečení tak, aby byly zohledněny všechny změny technologie, která je k dispozici, přičemž však tato opatření nesmějí vést k zajištění nižší úrovně zabezpečení a ochrany, než je úroveň uvedená v této Smlouvě.

9.4. Zpracovatel je povinen zdokumentovat technická a organizační opatření podle této Smlouvy podrobně formou přílohy k této Smlouvě. Zpracovatel je povinen uchovávat dokumentaci v aktuálním stavu a je povinen zdokumentovat jakékoli podstatné změny.

9.5. Technická a organizační opatření uvedená v příloze této Smlouvy se považují za schválená a potřebná v době uzavření smlouvy; představují všechny požadavky, které je Zpracovatel povinen splnit.

9.6. Klient je povinen provádět kontrolu technických a organizačních opatření na základě své vlastní analýzy rizik. Klient nese odpovědnost za zajištění, že tato technická a organizační opatření nabízejí úroveň ochrany údajů, která odpovídá rizikům spojeným se zpracovávanými Osobními údaji. Liší-li se výsledek analýzy rizik na straně Klienta od výsledku analýzy rizik provedené Zpracovatelem, Klient je oprávněn jednat se Zpracovatelem a požadovat úpravu bezpečnostních opatření. Pokud se Smluvní strany nedohodnou, každá z nich může Smlouvu ukončit na základě výpovědi doručené 14 dnů předem.

10. Kontrolní mechanismy

10.1. Klient je oprávněn zkontrolovat výkonnost služeb na straně Zpracovatele, pokud se jedná o Osobní údaje Klienta a dodržování ustanovení této Smlouvy, včetně například technických a organizačních opatření pro zajištění bezpečnosti zpracování.

10.2. Na základě požadavku Zpracovatel Klientovi doloží, že technická a organizační opatření byla zavedena. Uvedené zahrnuje

- doložení dodržování schválených pravidel chování podle čl. 40 Obecného nařízení o ochraně osobních údajů nebo
- certifikaci v souladu se schváleným postupem pro certifikaci podle čl. 42 Obecného nařízení o ochraně osobních údajů nebo
- kvalifikovanou autoevaluaci nezávislou třetí osobou (jako je například DPO, auditor, externí auditoři ochrany údajů / zabezpečení) v písemné formě nebo
- vhodnou certifikaci prostřednictvím auditu zabezpečení informačních technologií (IT) a ochrany dat (např. ISO 27001).

Tyto podklady musí obsahovat veškeré informace, které jsou zapotřebí k prokázání shody a plnění povinností vyplývajících z této Smlouvy a příslušných technických a organizačních opatření, která jsou míněna jako záruka zabezpečení zpracování. Klient může požadovat tyto informace jednou za kalendářní rok a v kratších intervalech pouze v případě, že existuje oprávněné podezření, že Zpracovatel porušil tuto Smlouvu, a v takovém případě je Klient povinen Zpracovatele o této skutečnost informovat písemně.

10.3. Klient je oprávněn zkontrolovat dodržování Smlouvy, zejména dodržování zabezpečení zpracování, provedením předem oznámených kontrol v provozovně Zpracovatele během normální pracovní doby (od 9:00 do 18:00 hodin) jednou za tři roky či nechat takovou kontrolu provést externím auditorem, který je vázán povinností zachovávat mlčenlivost vyplývající ze zákona nebo danou smluvně. Klient je povinen o těchto kontrolách informovat dva týdny předem formou písemného oznámení. Toto restriktivní opatření se na Klienta nevztahuje v naléhavých případech (například existuje-li podezření, že Zpracovatel porušuje tuto Smlouvu více než zanedbatelným způsobem). V takovém případě je Klient povinen Zpracovatele informovat písemně předem.

11. Subdodavatelé

11.1. V rozsahu, v jakém je Zpracovatel oprávněn na základě výslovného svolení Klienta subkontrahovat další zpracovatele (subdodavatele), a pokud nelze vyloučit možnost, že tito subdodavatelé budou mít přístup k Osobním údajům Klienta, může Zpracovatel takové subdodavatele subkontrahovat, a tím jim případně umožnit přístup k Osobním údajům Klienta, pouze pokud Klientovi písemně sdělil informace uvedené v následujícím odstavci a poskytl-li Klientovi příležitost vznést námitku, a pokud Klient ve sjednané lhůtě námitku nevznesl.

11.2. Informace, které mají být poskytnuty Zpracovatelem, jak je stanoveno výše, musí přinejmenším obsahovat následující údaje, a to v konkrétní a podrobné podobě:

11.2.1. identitu subdodavatele,

11.2.2. konkrétní služby, které má subdodavatel Zpracovateli poskytnout,

11.2.3. zkušenosti, kapacitu, spolehlivost a opatření týkající se zabezpečení informačních technologií a ochrany dat, které jsou zásadní z hlediska splnění povinností souvisejících s ochranou údajů,

11.2.4. záruky či garance subdodavatele, že splní ustanovení této Smlouvy.

11.3. Klient je oprávněn ve lhůtě sedmi dnů od data, kdy obdrží výše uvedené informace, podat námitku v písemné podobě proti subkontrahování daného subdodavatele za předpokladu, že má k uvedenému legitimní důvod. V případě takové námitky je Zpracovatel povinen vykonávat plnění podle této Smlouvy a poskytovat své služby a plnit své povinnosti bez využití tohoto subdodavatele a zůstává mu právo tuto Smlouvu ukončit.

11.4. Pokud a v rozsahu, v jakém je subdodavateli umožněn přístup k Osobním údajům Klienta, je Zpracovatel povinen uzavřít se subdodavatelem smlouvu o zpracování údajů, která ukládá subdodavateli povinnosti stanovené v této Smlouvě. Smlouva musí být uzavřena se subdodavatelem předtím, než získá první přístup k Osobním údajům Klienta.

12. Vrácení a výmaz

12.1. Zpracovatel je povinen při ukončení této Smlouvy nebo dříve, bude-li o to Klientem požádán, vrátit či předat všechny Osobní údaje Klientovi.

12.2. Podrobnosti týkající se povinnosti vymazat údaje jsou obsaženy (v této Smlouvě) a mohou být přidány formou Přílohy k této Smlouvě a podle okolností na základě výslovných pokynů Klienta. Zpracovatel není povinen mít svůj vlastní plán výmazu. Zpracovatel je povinen neprodleně po ukončení této Smlouvy nebo dříve, bude-li o to Klientem požádán, vymazat všechny Osobní údaje,

na které se nevztahuje zákonný požadavek skladování či uchování na straně Zpracovatele vyplývající z legislativy EU nebo Členského státu EU, nebo na které se nevztahuje výslovná dohoda s Klientem v rozporu s legislativou, kterou se řídí uchovávání nebo výmaz Osobních údajů. Zpracovatel je povinen uchovávat záznamy o výmazu.

13. Náklady, které uhradí Zpracovatel

Veškeré náklady vynaložené Zpracovatelem nebo jeho subdodavateli při zpracování Osobních údajů jménem Klienta podle podmínek této Smlouvy, zejména náklady vynaložené v souvislosti

13.1. s povinností reagovat na požadavky subjektů údajů podle pokynů Klienta, zejména pokud se jedná o opravu, výmaz či omezení Osobních údajů nebo vrácení Osobních údajů Klientovi a (podle okolností) převod údajů (přenositelnost) nebo součinnost poskytnutou v souvislosti s těmito opatřeními,

13.2. s povinností poskytnout součinnost při posuzování vlivu na ochranu osobních údajů,

13.3. s dodržováním nebo realizací pokynů Klienta,

13.4. s povinností poskytnout součinnost při plnění požadavků týkajících se zpřístupnění informací regulačnímu orgánu nebo subjektům údajů,

13.5. s provedením kvalifikované autoevaluace,

13.6. s kontrolami Klienta nebo (externích) auditorů na místě na základě požadavku Klienta, pokud taková kontrola neodhalí významné nedostatky, přičemž břemeno dokazování je v tomto případě na straně Klienta,

13.7. s dalšími náklady na technická a organizační opatření pro zajištění zabezpečení zpracování, kde tato opatření jsou zaváděna v důsledku odlišných výsledků analýzy rizik provedené Smluvními stranami,

13.8. s plněním povinností vrátit či vymazat Osobní údaje,

budou proplaceny Zpracovateli zvlášť na základě tržních hodinových sazeb. Zpracovatel je povinen uchovávat záznamy o vynaložených nákladech a výdajích.

14. Úpravy této Smlouvy

Má-li Zpracovatel povinnost zavádět změny a úpravy uloženou zákonem, je Klient povinen tyto změny a úpravy podporovat a schválit.

15. Odpovědnost

15.1. Podá-li subjekt údajů, případně třetí osoba žalobu proti Zpracovateli v souvislosti s výkonem zpracování, které Zpracovatel provádí jménem Klienta, je Klient povinen odškodnit Zpracovatele a uhradit související náklady na právní zastupování, náhradu škody, případně peněžité tresty uložené v přestupkovém řízení nebo podle trestního práva.

15.2. Výše uvedené ustanovení se neuplatní, pokud Zpracovatel nedodržel povinnosti mu uložené podle Obecného nařízení na ochranu osobních údajů nebo nedodržel právoplatně vydané pokyny Klienta nebo jednal v rozporu s takovými pokyny.

15.3. Limit odpovědnosti sjednaný mezi Klientem a Zpracovatelem ve prospěch Zpracovatele v Rámcové smlouvě se také vztahuje na odpovědnost Zpracovatele za výkon zpracování údajů podle této Smlouvy.

Linde Material Handling

Příloha

I. Kategorie Subjektů údajů

- Zákazníci
- Jiné subjekty údajů: distributoři, partneři v síti

II. Druhy údajů

- Kmenové údaje pracovníků
- Kmenové údaje o přenosu údajů
- Historie zákazníků

III. Rozsah zpracování

Hlavní požadavky Klienta jsou následující:
Vytvoření a zpracování servisních oznámení a objednávek

IV. Místo, kde mají být Osobní údaje zpracovávány

EHP

V. Systém(y) pro zpracování, včetně importu a exportu Osobních údajů z jiných systémů

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP a další ERP systémy našich distributorů, OneSignal Mobile Push Notifications

VI. Technická a organizační opatření pro zabezpečení na straně Zpracovatele

Realizace technických a organizačních opatření

a. Povinnost zachovávat mlčenlivost (čl. 32 (1) GDPR)

(1) Kontrola přístupu (do objektu)

- Alarm
- Automatické řízení přístupu
- Bezpečnostní zámky
- Kamerový dozor u vchodů
- Správa klíčů / seznam
- Recepce/vrátný
- Kniha návštěv
- Průkaz totožnosti zaměstnance/návštěvníka
- Návštěvníci musí být doprovázeni zaměstnancem společnosti

(2) Kontrola přístupu (systémy)

- Přihlášení pomocí uživatelského jména a hesla
- Server vybavený antivirovým softwarem
- Klienti vybavení antivirovým softwarem
- Firewall
- Systémy pro zjištění neoprávněného vniknutí
- Správa mobilních zařízení
- Používání VPN pro vzdálený přístup
- Šifrování datových úložišť
- Šifrování smartphonů
- Ochrana na úrovni BIOSu (samostatné heslo)

(3) Kontrola přístupu (data)

- Správa uživatelských práv
- Vytvoření profilů uživatelů
- Metodický pokyn „Bezpečná hesla“
- Metodický pokyn „Výmaz/Zničení“
- Obecný metodický pokyn o ochraně dat, případně zabezpečení dat
- Příručka „Ruční uzamčení počítače“
- Častá školení zaměstnanců
- Používání schématu oprávnění
- Správa uživatelských práv prováděná správci systému

(4) Kontrola oddělení

Oddělení produktivního a testovacího prostředí

(5) Pseudonymizace (čl. 32 (1) GDPR; čl. 25 (1) GDPR)

nevztahuje se

b. Dostupnost a odolnost (čl. 32 (1) GDPR)

- Požární hlásiče a detektory kouře
- Hasicí přístroj v serverovně
- Řízení teploty a vlhkosti v serverovně
- Klimatizace serverovny
- Systém UPS
- Bezpečnostní napájecí moduly použité v serverovně
- Systém RAID / zrcadlení disků
- Kamerová ochrana serverovny
- Poplachová signalizace v případě neoprávněného přístupu do serverovny
- Koncepce zálohování a obnovy provozu v případě havárie (slovně)
- Řízení zálohování
- Žádné zdravotně technické zařízení v serverovně ani nad ní
- Existence havarijního plánu (iE BSI IT-Grundschutz 100-4)
- Oddělené oddíly pro provozní systémy a data

c. Integrita (čl. 32 odst. 1 GDPR)

- Osobní údaje mohou upravovat pouze správci systému
- Realizace šifrovaných připojení, jako je např. sftp, https
- Protokolování přístupu a vyhledávání
- Přehled pravidelných procesů vyhledávání a převodu
- Pečlivý výběr pracovníků

d. Proces pro pravidelné testování, posuzování a hodnocení (čl. 32 (1) GDPR; čl. 25 (1) GDPR)

(1) Řízení ochrany osobních údajů

- Certifikace zabezpečení podle ISO 27001
- Účinnost technických bezpečnostních opatření se kontroluje nejméně jednou za rok
- Pracovníci jsou vyškoleni a jsou povinni zachovávat mlčenlivost

(2) Řízení reakce na incident

- Používání firewallu a pravidelné aktualizace
- Používání spamových filtrů a pravidelné aktualizace
- Používání virových skenerů a pravidelné aktualizace
- Systémy pro zjištění neoprávněného vniknutí (IDS)
- Systémy pro prevenci neoprávněného vniknutí (IPS)

Standardní ochrana údajů (čl. 25 (2) GDPR)

- Objem osobních údajů je omezen na nezbytně nutný pro účely, pro které jsou údaje zpracovávány

Linde Material Handling

Acuerdo de tratamiento de datos («Acuerdo») relativo a Linde Service Manager

El presente Acuerdo establece las condiciones generales de Linde Service Manager («**Condiciones generales**»). Todos los términos escritos en mayúscula que se usen pero que no se definan a continuación tendrán el significado que se les atribuya en las Condiciones generales.

El Proveedor («**Cliente**» o «**Responsable**»), representado por el Usuario, y LMH («**Encargado**» y, de forma conjunta con el Responsable, las «**Partes**») suscriben el presente Acuerdo de tratamiento de datos personales con respecto al Servicio. Este Acuerdo regula las obligaciones de protección de datos de las Partes con respecto a la protección de los datos personales del Cliente.

1. Definiciones

En este Acuerdo, los siguientes términos tienen los siguientes significados:

1.1. «**Encargado**»: una persona física o jurídica, autoridad pública, agencia u otro organismo que trate los datos personales en nombre del Responsable.

1.2. «**Tercero**»: una persona física o jurídica, autoridad pública, agencia u organismo que no sean el sujeto de los datos, el responsable, el encargado o cualquier persona que esté autorizada a tratar datos personales bajo la autoridad directa del responsable o del encargado.

1.3. «**Datos personales**»: cualquier información relativa a una persona física identificada o identificable («**Sujeto de los datos**»). Una persona física identificable es aquella a la que se puede identificar, de forma directa o indirecta, en virtud de un identificador como el nombre, un número de identificación, datos de ubicación, un identificador virtual o uno o más factores relacionados con la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona física.

1.4. «**Pseudonimización**»: el tratamiento de datos personales de modo que dichos datos personales no se puedan asignar a un Sujeto de los datos concreto sin recurrir a información adicional, siempre y cuando dicha información adicional se almacene por separado y esté sujeta a medidas técnicas y organizativas que garanticen que dichos datos no se asignen a una persona física identificada o identificable.

1.5. «**Responsable**»: la persona física o jurídica, autoridad pública, agencia u otro organismo que, solo o junto a otros, establece los fines y medios del tratamiento de los datos personales. En aquellos supuestos en los que determine los fines y medios de dicho tratamiento la legislación europea o del estado miembro, será esta quien determine el responsable o los criterios específicos para su nombramiento.

1.6. «**Tratamiento**»: cualquier operación o conjunto de operaciones que se realicen con respecto a datos personales o conjuntos de datos personales, ya sea o no con medios automatizados, como la recopilación, el registro, la organización, la estructuración, el almacenamiento, la adaptación o modificación, la recuperación, la consulta, el uso, la divulgación mediante transmisión o difusión o la publicación, alineación o combinación, restricción, supresión o destrucción.

1.7. «**Infracción de datos personales**»: una infracción de seguridad que provoca la destrucción accidental o ilegal, la pérdida, la modificación, la divulgación no autorizada o el acceso a los datos personales transmitidos, almacenados o tratados de otro modo.

1.8. «**Acuerdo principal**»: el acuerdo suscrito entre LMH y el Proveedor con respecto a los Servicios, tal y como se establece en las Condiciones generales.

2. Asunto y Período del presente Acuerdo

2.1. Este Acuerdo establece los deberes del Encargado por lo que a los Datos personales del Cliente que trate el Encargado en nombre de este se refiere.

2.2. Las disposiciones del presente Acuerdo no se aplican si y en la medida en que, de conformidad con lo establecido, el Encargado no tiene la obligación de realizar actividades de tratamiento con respecto a los Datos personales del Cliente. En ese caso, el Cliente deberá garantizar que sus Datos personales estén debidamente resguardados frente al Encargado.

2.3. Solo el Cliente puede determinar si el Tratamiento es legal y garantizar la protección de los derechos de los sujetos de los datos.

2.4. Este Acuerdo comienza en el mismo momento que el Acuerdo principal y termina cuando lo hace ese. Si el Encargado trata los Datos personales por instrucción del Cliente incluso después de que haya finalizado el Acuerdo principal, el presente Acuerdo también se mantendrá en vigor hasta que se finalice el Tratamiento realizado por instrucción del Cliente.

2.5. Sin perjuicio de la disposición en 2.4, las partes pueden rescindir el presente Acuerdo por motivos justificados. Si el motivo está relacionado con el incumplimiento de un deber en virtud del Acuerdo, solo se permite la rescisión cuando haya terminado el plazo para subsanar dicha infracción sin que esta se subsane o después de que las advertencias al respecto no hayan surtido efecto alguno. Para el Encargado serán motivos justificados, en especial:

2.5.1. Que el Cliente emita de forma reiterada instrucciones ilegales, que el Encargado haya informado al Cliente de ello sin dilación y que el Cliente no revoque dichas instrucciones.

2.5.2. Que el Cliente haya infringido las disposiciones del presente Acuerdo.

2.5.3. Que el Cliente se haya opuesto a la contratación de un subcontratista en el marco del presente Acuerdo.

Asimismo, las condiciones del Acuerdo principal se aplicarán *mutatis mutandis* al presente Acuerdo.

3. Naturaleza, alcance y lugar del Tratamiento

3.1. El Encargado está autorizado a acceder a los Datos personales del Cliente para prestar los servicios, de conformidad con el Acuerdo principal, en la medida que se establece en el Anexo 1. Las disposiciones del presente Acuerdo no amplían los deberes del Encargado, sino que se limitan a describirlas en mayor profundidad. El presente Acuerdo rige también los deberes del Cliente.

3.2. El Cliente puede emitir instrucciones que describan los deberes del Encargado en mayor profundidad.

3.3. El Encargado no puede usar los Datos personales para fines que no sean los que se describen en el Acuerdo principal y en el presente Acuerdo y, en especial, no podrá, sin la autorización previa

explícita del Cliente, transferir los Datos personales a terceros o facilitárselos a otras partes, a menos que se establezca lo contrario en el presente Acuerdo.

3.4. El Tratamiento en virtud del presente Acuerdo se limita al territorio de la Unión Europea y al EEE, a menos que se indique lo contrario en los Anexos del presente Acuerdo.

4. Instrucciones del Cliente, derechos de los Sujetos de los datos, evaluación del impacto de la Protección de datos

4.1. En sus instrucciones, el Cliente tiene derecho a especificar o actualizar la naturaleza, el alcance y el método del tratamiento de datos, las medidas de seguridad, los datos personales que se deben tratar y los grupos de Sujetos de los datos. Esto se aplica, en especial, a aquellos supuestos en los que una autoridad reguladora o cambios en la legislación exijan al Cliente que imparta instrucciones. Si un Sujeto de los datos se pone en contacto directamente con el Encargado, este deberá informar al Cliente por escrito sin dilaciones indebidas y solicitar instrucciones sobre cómo proceder.

4.2. Si el Cliente realiza una evaluación del impacto de la protección de datos, el Encargado deberá ayudarle como sea debido y necesario, incluso con respecto a consultas anteriores a la autoridad reguladora competente.

4.3. Las instrucciones del Cliente se limitan a la aplicación de los requisitos legales o regulatorios de la ley de protección de datos. Deben distinguirse de las solicitudes de cambios. Las solicitudes de cambios se refieren a cambios en el alcance de los servicios, los cuales no sean necesarios para aplicar los requisitos legales o regulatorios o que vayan más allá de las medidas necesarias para aplicar dichos requisitos. No constituyen instrucciones según lo establecido en el presente Acuerdo, sino solicitudes por parte del Cliente para aplicar cambios en los servicios. El Encargado tiene el derecho, pero no la obligación, de aplicar dichas solicitudes de cambios. La aplicación de dichas solicitudes de cambios se remunerará por separado.

4.4. El Cliente deberá impartir sus instrucciones siempre por escrito, por fax o por correo electrónico. El Cliente confirmará todas las instrucciones que imparta oralmente de forma excepcional sin dilación por escrito.

4.5. El Encargado informará al Cliente por escrito y sin dilación si considera que una instrucción del Cliente constituye una infracción de las disposiciones de protección de datos o si es errónea, incompleta, contradictoria o legal o técnicamente inviable de modo negligente. Al informar de ello, el Encargado señalará de forma explícita al Cliente por escrito que debe indicar si desea que el Encargado cumpla la instrucción o que siga tratando los Datos personales sin cumplir dicha instrucción hasta que el Cliente revise la información y adopte una decisión.

5. Deber del Encargado de facilitar información

5.1. En el supuesto de Infracción de datos personales, es posible que el Cliente tenga la obligación de informar de dicha infracción. El Encargado informará al Cliente si sospecha de o constata una infracción (que vaya más allá de una mera negligencia) de la protección de los Datos personales del Cliente por su parte o por parte de personas bajo su mando.

5.2. El Cliente podrá exigir al Encargado que adopte todas las medidas razonables y necesarias para ayudarle a cumplir su deber de notificación.

6. Deberes del Cliente

6.1. El Cliente informará al Encargado sin dilación en caso de constatar errores o irregularidades cuando compruebe el resultado del servicio prestado.

6.2. El Cliente deberá asegurarse, tanto antes de que comience el tratamiento de datos como después de este, de que el Encargado haya aplicado medidas técnicas y organizativas y de que las cumpla. Se deberá documentar el resultado de dichas comprobaciones.

6.3. El Cliente es responsable del cumplimiento de los deberes que se derivan de los art. 33 y 34 del Reglamento de Protección de Datos de la UE, los que establezca la autoridad reguladora y con respecto a los Sujetos de los datos a quienes afecte la Infracción de datos personales.

6.4. El Cliente informará al Encargado de los requisitos de supresión y conservación de los Datos personales, así como de la aplicación de dichos requisitos.

7. Delegado de protección de datos

7.1. El Encargado debe nombrar a un delegado de protección de datos («**Delegado**»). Los datos de contacto son los siguientes: datenschutz@kiongroup.com. El Encargado informará al Cliente de los cambios y de los cambios inminentes al respecto.

7.2. El Cliente nombrará a un Delegado de protección de datos o, en la medida en que no tenga la obligación de nombrar a un Delegado de protección de datos y de que no lo haya hecho, facilitará al Encargado el nombre de una persona que haya aceptado los deberes y la responsabilidad del Delegado de protección de datos. El Cliente notificará al Encargado los cambios o cambios inminentes al respecto, sin que el Encargado se lo deba pedir de forma específica.

7.3. Si el Cliente tiene la obligación de nombrar a un representante según lo establecido en el art. 27 del Reglamento General de Protección de Datos de la UE, informará al Encargado de la identidad de dicho representante. El Cliente notificará al Encargado los cambios o cambios inminentes al respecto, sin que el Encargado se lo deba pedir de forma específica.

8. Personas bajo el mando del Encargado

8.1. Al tratar los datos en virtud de las condiciones del presente Acuerdo, el Encargado solo recurrirá a personas que documenten la obligación de confidencialidad por escrito y que ya estén familiarizadas con las disposiciones legales de protección de datos relevantes para ellos y para las actividades de tratamiento que realicen en nombre del Cliente.

8.2. El Encargado deberá garantizar que todas las personas bajo su mando que tengan acceso a los Datos personales del Cliente solo puedan tratar dichos Datos personales con el alcance y de conformidad con las instrucciones del Cliente y las disposiciones del presente Acuerdo. La única excepción a las disposiciones anteriores se refiere a casos concretos de actividades de tratamiento, sobre todo a transferencias de datos al Encargado o a las personas bajo su mando que ordenen realizar de forma explícita un tribunal u organismo gubernamental en virtud de una disposición legal. En la medida en que la ley así lo permita, el Encargado informará al Cliente de dichas órdenes, preferiblemente antes de transferir los Datos personales.

9. Principios de tratamiento seguro

9.1. Teniendo en cuenta la tecnología disponible en la actualidad, los costes de aplicación y la naturaleza, el alcance, las circunstancias y los fines del Tratamiento de Datos acordado con el Cliente, así como la probabilidad y la posible gravedad de los riesgos para los derechos y libertades de las personas (análisis de riesgos), el Encargado aplicará las medidas técnicas y organizativas necesarias para garantizar que los Datos personales estén debidamente protegidos.

9.2. Al valorar el nivel de seguridad adecuado, el Encargado tendrá en cuenta los riesgos inherentes al tratamiento de los Datos personales del Cliente, incluidos a título enunciativo el riesgo de destrucción involuntaria o ilegal y de riesgo, modificación o divulgación o acceso no autorizados a los Datos personales del Cliente.

9.3. El Encargado actualizará y ajustará las medidas técnicas y organizativas de su plan de seguridad para incorporar los cambios de la tecnología disponible, aunque dichas medidas no deben caer por debajo del nivel de protección y seguridad que se indica en este Acuerdo.

9.4. El Encargado documentará en detalle las medidas técnicas y organizativas conformes con el presente Acuerdo en el Anexo al mismo. El Encargado mantendrá la documentación actualizada y documentará cualquier cambio sustancial.

9.5. Se considera que las medidas técnicas y organizativas del Anexo al presente Acuerdo se aprueban y son necesarias en el momento de suscribir el contrato, y constituyen todos los requisitos que debe satisfacer el Encargado.

9.6. El Cliente tiene la obligación de revisar las medidas técnicas y organizativas que se basen en su propio análisis de riesgos. El Cliente es responsable de garantizar que las medidas técnicas y organizativas ofrezcan un nivel de protección de datos proporcional a los riesgos de los Datos personales que se traten. Si el análisis de riesgo del Cliente arroja un resultado que difiera del análisis de riesgo del Encargado, el Cliente tendrá derecho a negociar con este el ajuste de las medidas de seguridad. Si las Partes no logran alcanzar un acuerdo, tendrán derecho a rescindir el Acuerdo con un preaviso de 14 días.

10. Controles

10.1. El Cliente tiene derecho a comprobar el desempeño de los servicios por parte del Encargado con respecto a los Datos personales del Cliente, así como su cumplimiento de las disposiciones del presente Acuerdo, incluidas a título enunciativo las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

10.2. Si así se le solicita, el Encargado deberá facilitar al Cliente pruebas de que ha aplicado las medidas de seguridad técnicas y organizativas. Se incluyen aquí:

- Pruebas del cumplimiento de los códigos de conducta aprobados en virtud del art. 40 del Reglamento General de Protección de Datos.
- Certificado conforme con un procedimiento de certificación aprobado en virtud del art. 42 del Reglamento General de Protección de Datos.
- Autoevaluación cualificada de un tercero independiente (como el Delegado, auditor, auditores de seguridad o de protección de datos) por escrito.
- Certificado correspondiente de una auditoría de protección de datos o de seguridad informática (p. ej. ISO 27001).

Dichas pruebas deben incluir toda la información necesaria para acreditar el cumplimiento con y la aplicación de los deberes en virtud del presente Acuerdo y de las medidas técnicas y organizativas relevantes destinadas a garantizar la seguridad del tratamiento. El Cliente puede solicitar esta información una vez cada año natural y en intervalos más frecuentes solo en caso de que exista una sospecha legítima de infracción del Acuerdo por parte del Encargado, de la cual el Cliente deberá informar al Encargado por escrito.

10.3. El Cliente tiene derecho a comprobar el cumplimiento del Acuerdo, en especial el cumplimiento de la seguridad del tratamiento, realizando inspecciones *in situ* anunciadas con antelación en las instalaciones del Encargado durante el horario comercial habitual (de 9:00 h a 18:00 h) una vez cada tres años, o a instar a que un auditor externo sujeto a obligaciones de confidencialidad legales o contractuales lo compruebe en su nombre. El Cliente debe informar por escrito con dos semanas de antelación de dichas inspecciones. Esta restricción al Cliente no se aplica en casos urgentes (p. ej., si existe una sospecha de infracciones del presente Acuerdo por parte del Encargado que vayan más allá de una mera negligencia). El Cliente no deberá informar al Encargado por escrito con antelación en dichos casos.

11. Subcontratistas

11.1. Si y en la medida en que el Encargado tenga derecho en virtud de un pacto explícito con el Cliente a recurrir a encargados adicionales (subcontratistas) y si no puede excluirse la posibilidad de que dichos subcontratistas tengan acceso a los Datos personales del Cliente, el Encargado solo podrá recurrir a dichos subcontratistas y permitir el acceso a los Datos personales del Cliente si ha informado al Cliente por escrito de los detalles que se establecen en el párrafo siguiente y si ha otorgado al Cliente la oportunidad de objetar, y si el Cliente no ha objetado en el plazo estipulado.

11.2. La información que debe facilitar el Encargado, según se establece arriba, debe incluir, como mínimo y en detalle:

11.2.1. La identidad del subcontratista.

11.2.2. Los servicios concretos que vaya a prestar el subcontratista al Encargado.

11.2.3. La experiencia, la capacidad, la fiabilidad y las medidas de protección de datos y de seguridad informática fundamentales para cumplir con las obligaciones de protección de datos en virtud del presente Acuerdo.

11.2.4. Las garantías de que el subcontratista vaya a cumplir las disposiciones del presente Acuerdo.

11.3. El Cliente tiene derecho, en un plazo de siete días tras recibir la información anterior, a objetar por escrito a la contratación de dicho subcontratista, siempre que tenga un motivo legítimo para hacerlo. En el supuesto de que se produzca una objeción, el Encargado tiene la obligación de cumplir el contrato, prestar sus servicios y satisfacer sus obligaciones sin recurrir a dicho subcontratista, con el derecho de rescindir el presente Acuerdo.

11.4. Si y en la medida en que el subcontratista obtenga acceso a los Datos personales del Cliente, el Encargado tendrá la obligación de suscribir un acuerdo de protección de datos con el subcontratista que le imponga los deberes establecidos en el presente Acuerdo. Dicho acuerdo se deberá suscribir antes de que el subcontratista obtenga acceso a los Datos personales del Cliente.

12. Devolución y supresión

12.1. El Encargado tiene la obligación, tras finalizar este Acuerdo o antes, si así lo solicita el Cliente, de devolver o entregar todos los Datos personales del Cliente.

12.2. Es posible que se incluyan los detalles de las obligaciones de suprimir datos en el Anexo del presente Acuerdo y, si procede, en instrucciones explícitas del Cliente. El Encargado no tiene la obligación de contar con un plan de supresión propio. El Encargado tiene la obligación, sin dilación tras finalizar el Acuerdo o antes, si así lo solicita el Cliente, de suprimir todos los Datos personales que no estén sujetos a un requisito de conservación o almacenamiento legal por su parte en virtud de la legislación de la UE o de un estado miembro de la UE, o de un pacto explícito en contrario relativo al almacenamiento o la supresión de Datos personales que se haya alcanzado con el Cliente. El Encargado registrará la supresión y conservará tales registros.

13. Costes con los que deberá correr el Encargado

Todos los costes en los que incurran el Encargado o los subcontratistas al tratar Datos personales en nombre del Cliente en virtud de las condiciones del presente Acuerdo, en especial los incurridos con motivo de

13.1. una obligación de responder a solicitudes del Sujeto de los datos por instrucción del Cliente y, en especial, de corregir, suprimir o limitar los Datos personales, o de devolver los Datos personales al Cliente y, si procede, de transferir datos (portabilidad) o de asistir en tales medidas;

13.2. una obligación de asistir en la evaluación del impacto de la protección de datos;

13.3. el cumplimiento o la aplicación de las instrucciones del Cliente;

13.4. la obligación de asistir en el cumplimiento de los requisitos de divulgar información a la autoridad reguladora o a los Sujetos de los datos;

13.5. la realización de una evaluación propia cualificada;

13.6. inspecciones *in situ* por parte del Cliente o de auditores (externos) que exija el Cliente, a menos que dichas inspecciones hayan constatado carencias considerables, que deberá probar el Cliente;

13.7. costes adicionales de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento, si se aplican dichas medidas como resultado de los diferentes análisis de riesgo de las Partes;

13.8. el cumplimiento de los deberes de devolver o suprimir Datos personales;

se reembolsarán por separado al Encargado según las tarifas por hora del mercado. El Encargado registrará los costes y gastos en los que incurra y conservará dichos registros.

14. Enmiendas al presente Acuerdo

Si el Encargado tiene la obligación legal de aplicar cambios y enmiendas, el Cliente tendrá la obligación de asistirle y de aprobarlas.

15. Responsabilidad

15.1. Si el Sujeto de los datos o un tercero emprenden acciones legales contra el Encargado con respecto a las actividades de tratamiento de datos que realiza el Encargado en nombre del Cliente, el Cliente tendrá la obligación de eximir al Encargado y de abonar los costes legales, las indemnizaciones y las multas administrativas o penales que de ello se deriven.

15.2. No se aplicará la disposición anterior si el Encargado hubiera incumplido los deberes que le corresponden en virtud del Reglamento General de Protección de Datos o hubiera incumplido las instrucciones que hubiese impartido legalmente el Cliente o si hubiera contravenido dichas instrucciones.

15.3. Las limitaciones a la responsabilidad que hubieran acordado el Cliente y el Encargado a favor del Encargado en el Acuerdo principal se aplicarán también a la responsabilidad del Encargado por las actividades de tratamiento de datos en virtud del presente Acuerdo.

Linde Material Handling

Anexo

I. Categorías de Sujetos de los datos

- Clientes
- Otros: proveedores, socios de la red

II. Tipos de datos

- Datos maestros del personal
- Datos maestros de comunicación
- Historial del cliente

III. Ámbito del tratamiento

Los requisitos fundamentales del Cliente son estos:
Creación y tratamiento de notificaciones y órdenes de servicio

IV. Lugar en el que se tratan los Datos personales

EEE

V. Sistemas de tratamiento, incluidas la importación y la exportación de Datos personales desde otros sistemas

Extranet global de Linde, pasarela SAP Netweaver, SAP ERP y otros sistemas ERP de nuestros proveedores,
notificaciones push móviles OneSignal

VI. Medidas de seguridad técnicas y organizativas del Encargado

Aplicación de medidas técnicas y organizativas

a. Confidencialidad (art. 32 [1] del RGPD)

(1) Control de acceso (instalaciones)

- Alarma
- Control automático del acceso
- Cierres de seguridad
- Videovigilancia de las entradas
- Control y lista de llaves
- Guarda en la entrada y recepcionista
- Lista de visitantes
- Identificación de empleados y visitantes
- Los visitantes van acompañados de un empleado

(2) Control de acceso (sistemas)

- Inicio de sesión con nombre de usuario y contraseña
- Servidor de software de antivirus
- Clientes de software de antivirus
- Cortafuegos
- Sistemas de detección de intrusos
- Gestión de dispositivos móviles

- Uso de RPV para acceso remoto
- Cifrado del almacenamiento de datos
- Cifrado de smartphones
- Protección BIOS (contraseña independiente)

(3) Control de acceso (datos)

- Gestión de los derechos de los usuarios
- Creación de perfiles de usuario
- Directriz «Contraseñas seguras»
- Directriz «Supresión y destrucción»
- Directriz general de protección y seguridad de datos
- Manual «Manual de bloqueo de escritorio»
- Formación frecuente de los empleados
- Uso de un plan de autorizaciones
- Gestión de los derechos de los usuarios por parte de los administradores

(4) Control de separación

Separación del entorno de producción y del de ensayos

(5) Pseudonimización (art. 32 [1] del RGPD; art. 25 [1] del RGPD)

n/a

b. Disponibilidad y resiliencia (art. 32 [1] del RGPD)

- Detectores de fuego y de humo
- Extintor de incendios en la sala de servidores
- Control de la temperatura y la humedad en la sala de servidores
- Sala de servidores con aire acondicionado
- SAI
- Uso de regleta de salida de seguridad en la sala de servidores
- Sistema RAID o imagen de *mirror* de HD
- Videovigilancia en la sala de servidores
- Señalización por alarma de accesos no autorizados a la sala de servidores
- Concepto (escrito) de copias de seguridad y recuperación
- Control de las copias de seguridad
- Ningún equipo médico en la sala de servidores o encima de esta
- Existencia de un plan de emergencia (iE BSI IT-Grundschutz 100-4)
- Particiones independientes de los sistemas operativos y los datos

c. Integridad (art. 32 [1] del RGPD)

- Solo los administradores pueden modificar datos personales
- Disposición de conexiones cifradas como sftp, https
- Inicio de sesión para el acceso y la consulta
- Revisión de los procesos habituales de consulta y transferencia
- Personal cuidadosamente seleccionado

d. Proceso de pruebas, valoraciones y evaluaciones habituales (art. 32 [1] del RGPD; art. 25 [1] del RGPD)

(1) Gestión de la protección de datos

- Certificado de seguridad conforme con ISO 27001
- La efectividad de las medidas de seguridad técnicas se revisa al menos una vez al año
- Se forma a los empleados y se les obliga a mantener la confidencialidad

(2) Gestión de respuesta a incidentes

- Uso de un cortafuegos y actualizaciones habituales
- Uso de filtros de *spam* y actualizaciones habituales
- Uso de un escáner de virus y actualizaciones habituales
- Sistema de detección de intrusos (IDS, por sus siglas en inglés)
- Sistema de prevención de intrusiones (IPS, por sus siglas en inglés)

Protección de datos por defecto (art. 25 [2] del RGPD)

- La cantidad de datos personales se limita a la necesaria para los fines del tratamiento

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

Linde Material Handling

Adatfeldolgozási Megállapodás (a továbbiakban: „Megállapodás") a Linde Service Manager vonatkozásában

A jelen Megállapodás hivatkozik a „Linde Service Manager" alkalmazásra vonatkozó általános szerződési feltételekre (a továbbiakban: „**ÁSZF**"). A jelen Megállapodásban meg nem határozott, de nagy betűvel kezdődő kifejezések az ÁSZF-ben meghatározott jelentéssel bírnak.

A Felhasználó által képviselt Forgalmazó (a továbbiakban: „**Ügyfél**" vagy „**Adatkezelő**") és az LMH (a továbbiakban: „**Adatfeldolgozó**", az Adatkezelővel együttesen: „**Felek**") a jelen Megállapodást kötik a Szolgáltatást érintő személyes adatok feldolgozása tekintetében. A jelen Megállapodás szabályozza a Felek adatvédelmi kötelezettségeit az Ügyfél személyes adatainak védelme tekintetében.

1. Fogalommeghatározások

A jelen Megállapodás alkalmazásában az alábbi fogalmak az itt meghatározott jelentéssel bírnak:

1.1. **Adatfeldolgozó:** Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel.

1.2. **Harmadik Fél:** Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

1.3. **Személyes Adat:** Azonosított vagy azonosítható természetes személyre (a továbbiakban: „**Érintett**") vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

1.4. **Álnevesítés:** A személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni.

1.5. **Adatkezelő:** Az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

1.6. **Adatkezelés:** A személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

1.7. **Adatvédelmi Incidens:** A biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését,

megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

1.8. **Alapszerződés:** Az LMH és a Forgalmazó között az ÁSZF szerinti Szolgáltatások tekintetében létrejött szerződés.

2. A jelen Megállapodás tárgya és időtartama

2.1. A jelen Megállapodás határozza meg az Adatfeldolgozó azon kötelezettségeit, amelyek az Ügyfélnek az Adatfeldolgozó által az Ügyfél nevében kezelt Személyes Adatai tekintetében fennállnak.

2.2. A jelen Megállapodás rendelkezései nem alkalmazandók, ha és amennyiben az Adatfeldolgozó megbízatása alapján nem köteles adatkezelési tevékenységet végezni az Ügyfél Személyes Adatai tekintetében. Ilyen esetben az Ügyfél köteles gondoskodni a Személyes Adatok megfelelő védelméről az Adatfeldolgozóval szemben.

2.3. Kizárólag az Ügyfél jogosult meghatározni az Adatkezelés jogszerűségét és biztosítani az Érintettek jogainak védelmét.

2.4. A jelen Megállapodás az Alapszerződéssel azonos időpontban lép hatályba és azzal azonos időpontban jár le. Ha az Adatkezelő az Ügyfél utasítása alapján az Alapszerződés lejáratát követően is kezel Személyes Adatot, a jelen Megállapodás az Ügyfél utasítása alapján végzett Adatkezelés megszűnéséig hatályban marad.

2.5. **A Felek jogosultak a jelen Megállapodást indokolt esetben felmondani a** 2.4 **pontban meghatározott rendelkezések sérelme nélkül.** Ha a felmondás indoka a jelen Megállapodás szerinti kötelezettség megsértése, a Megállapodás felmondása kizárólag a kötelezettségszegés orvoslására nyitva álló időtartam eredménytelen leteltét követően vagy az arra vonatkozó figyelmeztetés eredménytelensége esetén lehetséges. Az Adatfeldolgozó számára elfogadható indok különösen, ha

2.5.1. az Ügyfél ismételten jogellenes utasítást ad és az utasítást az Adatfeldolgozó indokolatlan késlekedés nélküli tájékoztatása ellenére sem vonja vissza;

2.5.2. az Ügyfél a jelen Megállapodás rendelkezéseit megsérti;

2.5.3. az Ügyfél a jelen Megállapodásnak megfelelően tiltakozott valamely alvállalkozó igénybevétele ellen.

Az Alapszerződés rendelkezései megfelelően alkalmazandóak a jelen Megállapodás tekintetében.

3. Az Adatkezelés jellege, terjedelme és helye

3.1. Az Adatfeldolgozó jogosult az Alapszerződés szerinti szolgáltatások nyújtása érdekében az 1. Mellékletben meghatározott mértékben hozzáférni az Ügyfél Személyes Adataihoz. A jelen Megállapodás rendelkezései nem kiterjesztik, hanem részletesebben meghatározzák az Adatfeldolgozó kötelezettségeinek tartalmát. A jelen Megállapodás határozza meg az Ügyfél kötelezettségeit is.

3.2. Az Ügyfél jogosult az Adatfeldolgozó kötelezettségeit tovább részletező utasításokat adni.

3.3. Az Adatfeldolgozó nem jogosult Személyes Adatot az Alapszerződésben meghatározott céltól eltérő célra felhasználni, és – a jelen Megállapodás eltérő rendelkezése hiányában – köteles különösen – az Ügyfél előzetes kifejezett utasítása hiányában – Személyes Adat harmadik fél vagy más átvevő fél részére történő átadásától tartózkodni.

3.4. A jelen Megállapodás alapján – a jelen Megállapodás mellékletének vagy mellékleteinek eltérő rendelkezése hiányában – kizárólag az Európai Unió és az EGT területén végezhető adatkezelés.

4. Az Ügyfél utasításai, az Érintettek jogai, adatvédelmi hatásvizsgálat

4.1. Az Ügyfél jogosult utasítások útján meghatározni vagy aktualizálni az adatkezelés jellegét, terjedelmét és módját, a biztonsági intézkedéseket, a kezelendő Személyes Adatokat, valamint az érintettek csoportjait. E körbe tartozik különösen, ha az Ügyfél utasítása szabályozó hatóság vagy jogszabályi változás előírása alapján válik szükségessé. Ha az Érintett közvetlenül kapcsolatba lép az Adatkezelővel, az Adatkezelő köteles indokolatlan késlekedés nélkül írásban tájékoztatni az Ügyfelet és utasítást kérni a követendő eljárás tekintetében.

4.2. Ha az Ügyfél adatvédelmi hatásvizsgálatot végez, az Adatfeldolgozó köteles számára a kapott utasítások szerint észszerű és szükséges mértékben támogatást nyújtani, ideértve az illetékes szabályozó hatósággal folytatott előzetes konzultációt is.

4.3. Az Ügyfél utasításai az adatvédelmi jogszabályok jogszabályi vagy szabályozási követelményeinek végrehajtására korlátozódnak. Nem azonosak a módosításra irányuló igényekkel. A módosításra irányuló igény a szolgáltatások terjedelmének olyan megváltoztatására utal, amely nem szükséges jogszabályi vagy szabályozási követelmény megvalósításához, vagy amely túlmutat az ilyen követelmények megvalósításához szükséges intézkedéseken. A módosításra irányuló igény a jelen Megállapodás alkalmazásában nem utasításnak, hanem az Ügyfél szolgáltatások módosítására irányuló kérésének minősül. Az Adatfeldolgozó jogosult, de nem köteles a módosításra irányuló igénynek eleget tenni. A módosításra irányuló igény megvalósításáért külön ellenszolgáltatás jár.

4.4. Az Ügyfél köteles az utasításait írásban, fax, vagy email útján elküldeni. Az Ügyfél köteles a kivételesen szóban adott utasítást indokolatlan késlekedés nélkül írásban vagy szöveges formában is megerősíteni.

4.5. Az Adatfeldolgozó köteles indokolatlan késlekedés nélkül szöveges formában értesíteni az Ügyfelet, ha az Adatfeldolgozó álláspontja szerint az Ügyfél által adott utasítás sérti az adatvédelmi szabályokat, vagy ha a jelentéktelen mértéket meghaladó körben hibás, hiányos, ellentmondásos, vagy jogi vagy műszaki szempontból megvalósíthatatlan. A tájékoztatás keretében az Adatfeldolgozó kifejezetten és szöveges formában felhívja az Ügyfelet, hogy indokolatlan késlekedés nélkül nyilatkozzon arról, hogy az Adatfeldolgozó tegyen-e eleget az utasításnak, vagy az utasítást figyelmen kívül hagyva folytassa a Személyes Adatok kezelését mindaddig, amíg az Ügyfél a kapott tájékoztatás alapján dönt.

5. Az Adatfeldolgozó tájékoztatási kötelezettségei

5.1. Adatvédelmi Incidens esetén előfordulhat, hogy az Ügyfél köteles az incidensről bejelentést tenni. Az Adatfeldolgozó köteles értesíteni az Ügyfelet, ha gyanúja vagy tudomása szerint az

Ügyfél Személyes Adatainak védelmét az Adatfeldolgozó vagy annak irányítása alatt álló személy (a jelentéktelen mértéket meghaladóan) megsértette.

5.2. Az Ügyfél követelheti, hogy az Adatfeldolgozó minden észszerű és szükséges intézkedés megtételével támogassa az Ügyfelet a bejelentésre vonatkozó követelményeknek való megfelelésben.

6. Az Ügyfél kötelezettségei

6.1. Az Ügyfél köteles indokolatlan késlekedés nélkül tájékoztatni az Adatfeldolgozót a szolgáltatásnyújtás eredményének ellenőrzése során talált hibáról vagy szabálytalanságról.

6.2. Az Ügyfél köteles az adatkezelés megkezdése előtt és azt követően egyaránt meggyőződni arról, hogy az Adatfeldolgozó által bevezetett technikai és szervezési intézkedéseket betartják. Az erre irányuló ellenőrzés eredményét dokumentálni kell.

6.3. Az Ügyfél köteles az általános adatvédelmi rendelet 33. és 34. cikke alapján a szabályozó hatóság vagy az Adatvédelmi Incidens által érintett érintettek felé fennálló kötelezettségeinek eleget tenni.

6.4. Az Ügyfél köteles tájékoztatni az Adatfeldolgozót a Személyes Adatok törlésére és megőrzésére vonatkozó követelményekről és azok megvalósításáról.

7. Adatvédelmi Tisztviselő

7.1. Az Adatfeldolgozó adatvédelmi tisztviselőt (a továbbiakban: „**Adatvédelmi Tisztviselő**") jelöl ki. Az Adatvédelmi Tisztviselő elérhetősége: datenschutz@kiongroup.com. Az Adatfeldolgozó köteles tájékoztatni az Ügyfelet ennek változásáról.

7.2. Az Ügyfél adatvédelmi tisztviselőt jelölt ki, vagy – ha az Ügyfél nem köteles adatvédelmi tisztviselőt kijelölni, és így nem is jelölt ki azt – tájékoztatja az Adatfeldolgozót az Ügyfél részéről eljáró olyan személy nevéről, aki vállalta az adatvédelmi tisztviselő kötelezettségeinek és feladatainak ellátását. Az Ügyfél köteles – az Adatfeldolgozó kifejezett kérése hiányában is – értesíteni az Adatfeldolgozót ennek változásáról.

7.3. Ha az Ügyfél köteles az általános adatvédelmi rendelet 27. cikke szerinti képviselőt kijelölni, köteles a képviselő személyéről tájékoztatni az Adatfeldolgozót. Az Ügyfél köteles – az Adatfeldolgozó kifejezett kérése hiányában is – értesíteni az Adatfeldolgozót ennek változásáról.

8. Az Adatfeldolgozó irányítása alatt álló személyek

8.1. A jelen Megállapodás szerinti adatkezelés végzése során az Adatfeldolgozó kizárólag dokumentált módon titoktartási kötelezettséget vállaló személyeket vehet igénybe, akiket előre tájékoztatott a rájuk és az Ügyfél nevében végzendő adatkezelési tevékenységre vonatkozó adatvédelmi jogszabályi előírásokról.

8.2. Az Adatfeldolgozó köteles gondoskodni arról, hogy az irányítása alatt álló és az Ügyfél Személyes Adataihoz hozzáférő személyek a Személyes Adatok kezelését kizárólag az Ügyfél utasításainak és a jelen Megállapodás rendelkezéseinek megfelelő módon és mértékben végezzék. A fenti rendelkezés alóli egyedüli kivételt az adatkezelési tevékenységek olyan egyedi esetei, így az adattovábbítások képezik, amelyeket az Adatkezelő vagy az annak irányítása alatt álló személy

bíróság vagy állami hatóság jogszabályi előíráson alapuló kifejezett utasítására köteles végrehajtani. Az Adatkezelő köteles a jog által megengedett legteljesebb mértékben tájékoztatni az Ügyfelet az ilyen utasításokról, lehetőleg még a Személyes Adat továbbítása előtt.

9. A biztonságos adatkezelés elvei

9.1. Az Adatkezelő köteles megtenni a Személyes Adatok megfelelő védelmének biztosításához szükséges technikai és szervezési intézkedéseket, figyelembe véve az elérhető technológiát, a megvalósítás költségeit, az Ügyféllel meghatározott Adatkezelés jellegét, terjedelmét, körülményeit és céljait, valamint a természetes személyek jogait és szabadságait érintő fenyegető kockázat valószínűségét és súlyosságát (kockázatelemzés).

9.2. A megfelelő biztonsági szint értékelésekor az Adatkezelő köteles figyelembe venni az Ügyfél Személyes Adatai kezelésének természetéből fakadó kockázatokat, így – többek között – az Ügyfél Személyes Adatai véletlen vagy jogellenes megsemmisítésének, elvesztésének, megváltoztatásának, jogosulatlan közlésének vagy az azokhoz való jogosulatlan hozzáférésnek a kockázatát.

9.3. Az Adatkezelő köteles az elérhető technológiának megfelelően aktualizálni és pontosítani a biztonsági tervében található technikai és szervezési intézkedéseket, azonban ezen intézkedések nem maradhatnak el a biztonság és védelem jelen Megállapodásban meghatározott szintjétől.

9.4. Az Adatfeldolgozó köteles a jelen Megállapodás szerinti technikai és szervezési intézkedéseket részletesen dokumentálni a jelen Megállapodás mellékletében. Az Adatfeldolgozó köteles a dokumentációt naprakészen tartani és minden lényeges változást rögzíteni.

9.5. A jelen Megállapodás mellékletében meghatározott technikai és szervezési intézkedések a szerződés hatálybalépésének időpontjában jóváhagyottnak és szükségesnek tekintendők; ezek képezik azokat a követelményeket, amelyeknek az Adatkezelőnek meg kell felelnie.

9.6. Az Ügyfél köteles a technikai és szervezési intézkedéseket saját kockázatelemzése alapján ellenőrizni. Az Ügyfél köteles biztosítani, hogy a technikai és szervezési intézkedések a kezelt Személyes Adatokat érintő kockázatoknak megfelelő adatvédelmi szintet nyújtanak. Ha az Ügyfél kockázatelemzése az Adatkezelő kockázatelemzésétől eltérő eredményre jut, az Ügyfél jogosult az Adatkezelővel egyeztetni a biztonsági intézkedések átalakításáról. Ha a Felek nem jutnak megállapodásra e tekintetben, a jelen Megállapodást bármelyik fél jogosult írásbeli nyilatkozattal 14 napos felmondási idő mellett felmondani.

10. Ellenőrzések

10.1. Az Ügyfél jogosult az Ügyfél Személyes Adatai tekintetében a szolgáltatások nyújtását és a jelen Megállapodás rendelkezéseinek betartását – így, többek között, az adatkezelés biztonságának biztosítása érdekében tett technikai és szervezési intézkedéseket – ellenőrizni.

10.2. Az Adatfeldolgozó kérésre köteles az Ügyfél részére a technikai és szervezési intézkedések végrehajtására vonatkozóan bizonyítékot nyújtani. E körbe tartozik

- az általános adatvédelmi rendelet 40. cikke szerinti jóváhagyott magatartási kódexek betartására vonatkozó bizonyíték, vagy
- az általános adatvédelmi rendelet 42. cikke szerinti jóváhagyott tanúsítási mechanizmus keretében szerzett tanúsítvány, vagy

- független harmadik fél (például adatvédelmi tisztviselő, auditor, külső adatvédelmi/biztonsági auditorok) által készített minősített önértékelés szöveges formában, vagy
- informatikai biztonsági vagy adatvédelmi audit során szerzett megfelelő tanúsítvány (pl. ISO 27001).

A bizonyítéknak tartalmaznia kell mindazokat az adatokat, amelyek a jelen Megállapodásban és a vonatkozó technikai és szervezési intézkedésekben az adatfeldolgozás biztonságának biztosítása érdekében meghatározott kötelezettségek betartásának és teljesítésének bizonyításához szükségesek. Az Ügyfél jogosult naptári évente egy alkalommal erre vonatkozó információt igényelni; ennél rövidebb időszak alkalmazása abban az esetben lehetséges, ha jogos gyanú merül fel a jelen Megállapodás Adatfeldolgozó általi megszegésével kapcsolatban, amelyről az Ügyfél köteles az Adatfeldolgozót írásban értesíteni.

10.3. Az Ügyfél jogosult a jelen Megállapodás betartását – és különösen az adatkezelés biztonságát – előre bejelentett és háromévente az Adatfeldolgozó telephelyén rendes munkaidőben (9:00 és 18:00 között) végzett helyszíni ellenőrzés útján ellenőrizni, vagy ilyen ellenőrzés útján jogszabályi vagy szerződéses titoktartási kötelezettség alatt álló külső auditor bevonásával ellenőriztetni. Az Ügyfél köteles az ellenőrzést két héttel előre írásban bejelenteni. Ez az Ügyfélre vonatkozó korlátozás sürgős esetben nem alkalmazandó (például a jelen Megállapodás Adatfeldolgozó általi, nem elhanyagolható mértékű megsértésére vonatkozó gyanú fennállása); ilyen esetben az Ügyfél nem köteles az Adatfeldolgozót írásban előre értesíteni.

11. Alvállalkozók

11.1. Ha és amennyiben az Adatfeldolgozó az Ügyféllel létrejött kifejezett megállapodás alapján jogosult további adatfeldolgozót (alvállalkozót) igénybe venni és nem lehetséges kizárni, hogy az alvállalkozó hozzáférjen az Ügyfél Személyes Adataihoz, az Adatfeldolgozó csak abban az esetben veheti igénybe az alvállalkozót és teheti számára esetlegesen hozzáférhetővé az Ügyfél Személyes Adatait, ha az Ügyfelet írásban előre tájékoztatta a következő bekezdésben meghatározott részletekről és tiltakozási lehetőséget biztosított az Ügyfél számára, az Ügyfél pedig az erre nyitva álló időszakban nem tiltakozott.

11.2. Az Adatfeldolgozó által a fentiek alapján adandó tájékoztatásnak tartalmaznia kell legalább a következő információkat konkrétan és részletezve:

11.2.1. az alvállalkozó személye,

11.2.2. az alvállalkozó által az Adatfeldolgozó részére nyújtott konkrét szolgáltatások,

11.2.3. a jelen Megállapodás szerinti adatvédelmi kötelezettségek teljesítéséhez elengedhetetlen tapasztalat, kapacitás, megbízhatóság, valamint informatikai biztonsági és adatvédelmi intézkedések,

11.2.4. az alvállalkozó által a jelen Megállapodás rendelkezéseinek betartása tekintetében nyújtott garanciák és biztosítékok.

11.3. Az Ügyfél jogosult a fenti információk kézhezvételétől számított hét napon belül írásban, megfelelő indok alapján tiltakozni az alvállalkozó igénybevétele ellen. Az Ügyfél tiltakozása esetén az Adatfeldolgozó köteles az alvállalkozó igénybevétele nélkül teljesíteni a jelen

Megállapodást, nyújtani a szolgáltatásait és teljesíteni a kötelezettségeit, azzal, hogy a jelen Megállapodást változatlanul jogosult felmondani.

11.4. Ha és amennyiben az alvállalkozó hozzáféréssel rendelkezik az Ügyfél Személyes Adataihoz, az Adatfeldolgozó köteles a jelen Megállapodásban meghatározott kötelezettségeket az alvállalkozó számára előíró adatfeldolgozási szerződést kötni az alvállalkozóval. A szerződést még azt megelőzően kell megkötni, hogy az alvállalkozó hozzáférést szerez az Ügyfél Személyes Adataihoz.

12. Visszaszolgáltatás és törlés

12.1. Az Adatfeldolgozó köteles a jelen Megállapodás lejáratát követően vagy – az Ügyfél kérése alapján – azt megelőzően az Ügyfél minden Személyes Adatát visszaszolgáltatni.

12.2. A törlési kötelezettségre vonatkozó részletes előírások a jelen Megállapodás mellékletében és – adott esetben – az Ügyfél kifejezett utasítása útján határozhatók meg. Az Adatfeldolgozó nem köteles saját törlési tervet készíteni. Az Adatfeldolgozó köteles a jelen Megállapodás lejáratát követően vagy – az Ügyfél kérése alapján – azt megelőzően indokolatlan késlekedés nélkül törölni mindazon személyes adatokat, amelyeket az Adatfeldolgozó nem köteles uniós vagy tagállami jogszabályi előírás alapján tárolni vagy megőrizni, vagy amelyekre nem vonatkozik az Ügyféllel a Személyes Adatok tárolása és törlése tekintetében létrejött olyan megállapodás, amely kifejezetten ennek az ellenkezőjéről rendelkezik. Az Adatfeldolgozó köteles a törlésről jegyzőkönyvet készíteni.

13. Az Adatfeldolgozó által viselt költségek

A Személyes Adatoknak az Ügyfél nevében a jelen Megállapodás alapján az Adatfeldolgozó vagy annak alvállalkozója által történő kezelése során felmerülő minden költséget – különösen az alábbiak alapján felmerülő költségeket:

13.1. érintettől érkező megkeresés alapján az Ügyfél utasításai szerint történő válaszadásra vonatkozó kötelezettség, különösen Személyes Adat helyesbítése, törlése vagy korlátozása, Személyes Adat Ügyfél részére történő visszaszolgáltatása, vagy – adott esetben – adattovábbítás (hordozhatóság), vagy ilyen intézkedéssel összefüggő segítségnyújtás tekintetében,

13.2. adatvédelmi hatásvizsgálat során történő együttműködésre irányuló kötelezettség,

13.3. az Ügyfél utasításainak teljesítése vagy végrehajtása,

13.4. szabályozó hatóság vagy érintett részére történő információnyújtásra vonatkozó követelménynek való megfeleléssel kapcsolatos támogatási kötelezettség,

13.5. minősített önértékelés készítése,

13.6. az Ügyfél vagy általa igénybe vett (külső) auditor által végzett helyszíni ellenőrzés, kivéve, ha az ellenőrzés jelentős hiányosságokat tár fel; a bizonyítási terhet e tekintetben az Ügyfél viseli,

13.7. az adatkezelés biztonságát garantáló technikai és szervezési intézkedésekkel összefüggő további költségek, ha az intézkedéseket a Felek kockázatelemzése közötti eltérésekre tekintettel vezetik be,

13.8. a Személyes Adat visszaszolgáltatásával vagy törlésével összefüggő kötelezettség teljesítése

– piaci óradíj alapon külön visszatérítik az Adatfeldolgozó részére. Az Adatfeldolgozó köteles a felmerült költségekről és kiadásokról nyilvántartást vezetni.

14. A jelen Megállapodás módosítása

Az Ügyfél köteles támogatni és jóváhagyni az Adatfeldolgozó által jogszabályi előírás alapján végrehajtandó módosításokat és változtatásokat.

15. Felelősség

15.1. Ha az Adatfeldolgozó által az Ügyfél nevében végzett adatkezeléssel összefüggésben az érintett és/vagy harmadik fél peres eljárást kezdeményez az Adatfeldolgozóval szemben, az Ügyfél köteles mentesíteni az Adatfeldolgozót és viselni a jogi költségeket és károkat és/vagy megfizetni a közigazgatási és büntetőjogi bírságokat.

15.2. A fenti rendelkezés nem alkalmazandó, ha az Adatfeldolgozó megsértette az általános adatvédelmi rendelet alapján fennálló kötelezettségét, vagy nem teljesítette vagy tartotta be az Ügyfél jogszerű utasítását.

15.3. Az Ügyfél és az Adatfeldolgozó tekintetében az Alapszerződésben az Adatfeldolgozó javára meghatározott felelősségkorlátozások az Adatfeldolgozó jelen Megállapodás szerinti adatkezelési tevékenységével összefüggő felelőssége vonatkozásában is irányadók.

Linde Material Handling

Melléklet

I. Érintettek kategóriái

- Ügyfelek
- Mások: forgalmazók, hálózati partnerek

II. Adattípusok

- Személyzeti törzsadatok
- Kommunikációs törzsadatok
- Ügyfél előzményei

III. Adatkezelés köre

Az Ügyfél legfontosabb követelményei:
Kézbesítési értesítések és megrendelések létrehozása és kezelése

IV. Személyes Adatok kezelésének helye

EGT

V. Adatkezelő rendszer(ek), ideértve a más rendszerekből származó személyes adatok importálását és exportálását

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP és a forgalmazóink más ERP rendszerei, OneSignal Mobile Push Notifications

VI. Az Adatkezelő technikai és szervezési biztonsági intézkedései

Technikai és szervezési intézkedések végrehajtása

a. Titoktartás (a GDPR 32. cikkének (1) bekezdése)

(1) Hozzáférés ellenőrzése (telephelyek)

- Riasztó
- Automatikus hozzáférés-ellenőrzés
- Biztonsági zárak
- Belépést rögzítő videófelvétel
- Kulcsellenőrzés / lista
- Recepció / portás
- Látogatók listája
- Munkavállalói / látogatói igazolvány
- A látogatókat munkavállaló kíséri

(2) Hozzáférés ellenőrzése (rendszerek)

- Belépés felhasználói névvel és jelszóval
- Antivírusszoftver-szerver
- Antivírusszoftver-kliensek
- Tűzfal
- Behatolásészlelő rendszerek
- Mobileszköz-kezelés
- VPN használata távoli eléréshez

- Adattárolók titkosítása
- Okostelefonok titkosítása
- BIOS-védelem (külön jelszóval)

(3) Hozzáférés ellenőrzése (adatok)

- Felhasználói jogosultságok kezelése
- Felhasználói profilok létrehozása
- Biztonságos jelszavakra vonatkozó útmutató
- Törlése / megsemmisítésre vonatkozó útmutató
- Adatvédelemre és/vagy adatbiztonságra vonatkozó általános útmutató
- Manuális számítógépzárra vonatkozó kézikönyv
- Munkavállalók gyakori képzése
- Engedélyezési sémák használata
- Felhasználói jogok rendszergazdai kezelése

(4) Elválasztás irányítása

Termelési és tesztkörnyezet elválasztása

(5) Álnevesítés (a GDPR 32. cikkének (1) bekezdése és 25. cikkének (1) bekezdése)

Nem alkalmazandó

b. Rendelkezésre állás és ellenálló képesség (a GDPR 32. cikkének (1) bekezdése)

- Tűz- és füstérzékelők
- Tűzoltókészülék a szerverszobában
- Hőmérséklet és páratartalom szabályozása a szerverszobában
- Légkondicionálás a szerverszobában
- UPS-rendszer
- Biztonsági elosztók használata a szerverszobában
- RAID-rendszer / merevlemez tükrözése
- Videómegfigyelés a szerverszobában
- Riasztás a szerverszobába történő jogosulatlan belépés esetén
- Biztonsági mentésre és helyreállításra vonatkozó koncepció (szöveges dokumentum)
- Biztonsági mentések szabályozása
- Nincs vizesblokk a szerverszobában vagy afölött
- Vészhelyzeti terv megléte (iE BSI IT-Grundschutz 100-4)
- Operációs rendszer és adatok külön partíción vannak

c. Integritás (a GDPR 32. cikkének (1) bekezdése)

- Személyes adatot kizárólag rendszergazda módosíthat
- Titkosított kapcsolatok (pl. sftp, https) biztosítása
- Hozzáférés és adatkérés naplózása
- Rendszeres adatlekérdezési és -továbbítási folyamatok vizsgálata
- Munkatársak gondos kiválasztása

d. Rendszeres tesztelésre, felmérésre és értékelésre szolgáló eljárás (a GDPR 32. cikkének (1) bekezdése és 25. cikkének (1) bekezdése)

(1) Adatvédelem kezelése

- ISO 27001 biztonsági tanúsítvány
- A technikai biztonsági intézkedések hatékonyságának ellenőrzése évente legalább egy alkalommal
- A munkavállalók titoktartási képzésben részesülnek és titoktartási kötelezettség alatt állnak

(2) Incidenskezelés

- Tűzfal használata és rendszeres frissítése
- Spamszűrők használata és rendszeres frissítése
- Vírusszkenner használata és rendszeres frissítése
- Behatolásészlelő rendszer (IDS)
- Behatolásmegelőző rendszer (IPS)

Alapértelmezett adatvédelem (a GDPR 25. cikkének (2) bekezdése)

- A személyes adatok mennyisége az adatkezelés céljához szükséges mértékre korlátozódik

Linde Material Handling

Accordo sul trattamento dei dati ("Accordo") rispetto a Linde Service Manager

Questo Accordo si riferisce ai termini e alle condizioni generali di "Linde Service Manager" ("**TeCG**"). Qualsivoglia termine in maiuscolo usato ma non definito nel presente avrà il significato attribuito ad esso nei TeCG.

Il Distributore ("**Cliente**" o "**Titolare del trattamento**"), rappresentato dall'Utente, e LMH ("**Responsabile del trattamento**" e insieme al Titolare del trattamento, le "**Parti**") concludono il presente Accordo per il trattamento dei dati personali relativamente al Service. Il presente Accordo regola gli obblighi sulla protezione dei dati delle Parti in rapporto alla protezione dei dati personali del Cliente.

1. Definizioni

Nel presente Accordo, i termini seguenti hanno i significati indicati qui sotto:

1.1. "**Responsabile del trattamento**": una persona fisica o giuridica, un'autorità pubblica, un ente o un altro organismo che si occupa del trattamento dei dati personali per conto del Responsabile del trattamento.

1.2. "**Terzo**": una persona fisica o giuridica, un'autorità pubblica, un ente o un organismo diverso dall'interessato, dal titolare del trattamento, dal responsabile del trattamento e dalle persone che, sotto l'autorità diretta del titolare o del responsabile del trattamento, è autorizzata a trattare i dati personali.

1.3. "**Dati personali**": qualsiasi informazione relativa a una persona fisica identificata o identificabile ("**Interessato**"); una persona fisica identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare attraverso un identificatore come un nome, un numero identificativo o uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di tale persona fisica.

1.4. "**Pseudonimizzazione**": il trattamento dei dati personali effettuato in modo tale che i dati personali non possono più essere attribuiti a un Interessato specifico senza l'uso di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e siano soggette a misure tecniche e organizzative tali da garantire che i dati personali non siano attribuibili a una persona fisica identificata o identificabile.

1.5. "**Titolare del trattamento**": la persona fisica o giuridica, l'autorità pubblica, l'ente o l'organismo che, da sola o congiuntamente ad altri, determina i fini e i mezzi del trattamento dei dati personali; nei casi in cui i fini e i mezzi di tale trattamento sono determinati dalla legge dell'Unione o degli Stati Membri, il titolare del trattamento o i criteri specifici per la sua nomina possono essere stabiliti dalla legge dell'Unione o degli Stati Membri.

1.6. "**Trattamento**": qualsiasi operazione o insieme di operazioni effettuata sui dati personali o su insiemi di dati personali, mediante o meno mezzi automatici, quale acquisizione, registrazione, organizzazione, strutturazione, archiviazione, adattamento o alterazione, recupero, consultazione, uso, divulgazione mediante trasmissione, disseminazione o messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.

1.7. "**Violazione dei dati personali**": una violazione della sicurezza che causa la distruzione accidentale o illegale, la perdita, l'alterazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, archiviati o in altro modo trattati.

1.8. "**Accordo principale**": l'accordo concluso tra LMH e il Distributore relativamente ai Servizi, specificato nei TeCG.

2. Oggetto e durata del presente accordo

2.1. Il presente Accordo regola gli obblighi del Responsabile del trattamento rispetto ai Dati personali del Cliente trattati dal Responsabile del trattamento per conto del Cliente.

2.2. Le disposizioni del presente Accordo non si applicano qualora e nella misura in cui, in conformità con l'incarico, il Responsabile del trattamento non sia tenuto a svolgere attività di trattamento dei dati rispetto ai Dati personali del Cliente. In questo caso il Cliente si assicurerà che i suoi Dati personali siano protetti in maniera appropriata dal Responsabile del trattamento.

2.3. Il Cliente determinerà se il Trattamento è legale e si assicurerà che i diritti degli interessati siano protetti.

2.4. Il presente Accordo decorre a partire dalla data di efficacia dell'Accordo principale e si risolve al momento della risoluzione dell'Accordo principale. Nel caso in cui il Responsabile del trattamento tratti i Dati personali sulla base delle istruzioni del Cliente anche dopo la risoluzione dell'Accordo principale, il presente Accordo resterà valido fino al termine del Trattamento eseguito sulla base delle istruzioni del Cliente.

2.5. Nonostante la disposizione contenuta nel paragrafo 2.4, le Parti possono risolvere il presente Accordo per giusta causa. Qualora la causa sia correlata alla violazione di un obbligo previsto dall'Accordo, la risoluzione è consentita solo dopo il termine di un periodo specificato per porre rimedio alla violazione senza che sia stato posto rimedio alla violazione o dopo che un avvertimento fornito non abbia sortito alcun effetto. La giusta causa per il Responsabile del trattamento dei dati si ha in particolare nel caso in cui

2.5.1. Il Cliente fornisca ripetutamente istruzioni illegali senza revocarle nonostante il Responsabile abbia informato prontamente il Cliente di ciò;

2.5.2. Il Cliente abbia violato le disposizioni del presente Accordo;

2.5.3. Il Cliente si sia opposto all'ingaggio di un subappaltatore ai sensi del presente Accordo.

Inoltre, i termini dell'Accordo principale devono applicarsi mutatis mutandis al presente Accordo.

3. Natura, ambito e luogo del trattamento

3.1. Il Responsabile del trattamento è autorizzato ad accedere ai Dati personali del Cliente per poter fornire i servizi ai sensi dell'Accordo principale nella misura descritta nell'Appendice 1. Le disposizioni del presente Accordo non estendono in alcun modo gli obblighi del Responsabile del trattamento, ma li descrivono in modo più dettagliato. Il presente Accordo regola anche gli obblighi del Cliente.

3.2. Il Cliente può fornire istruzioni che specificano in maniera più dettagliata gli obblighi del Responsabile del trattamento.

3.3. Al Responsabile del trattamento non è consentito usare i Dati personali per fini diversi da quelli descritti nell'Accordo principale e nel presente Accordo e, in particolare, non è consentito, senza istruzioni esplicite precedenti del Cliente, trasmettere i Dati personali a terzi o ad altri destinatari, fatto salvo quanto altrimenti specificato nel presente Accordo.

3.4. Il Trattamento ai sensi del presente Accordo è limitato al territorio dell'Unione europea e del SEE, fatto salvo quanto altrimenti specificato negli Allegati al presente Accordo.

4. Istruzioni del Cliente, diritti degli Interessati, valutazione dell'impatto della protezione dei dati

4.1. Il Cliente, mediante le istruzioni, ha la facoltà di specificare o aggiornare la natura, l'ambito e il metodo di trattamento dei dati, delle misure di sicurezza, dei Dati personali da trattare e dei gruppi di interessati. Ciò si applica principalmente ai casi in cui un ente regolatore o eventuali modifiche legislative obblighino o richiedano al Cliente di fornire delle istruzioni. Qualora un Interessato contatti direttamente il Responsabile del trattamento, il Responsabile del trattamento è tenuto a informare tempestivamente il Cliente per iscritto richiedendo istruzioni su come procedere.

4.2. Se il Cliente effettua una valutazione sull'impatto della protezione dei dati, il Responsabile del trattamento deve fornirgli assistenza nella misura massima possibile, anche in merito a eventuali consultazioni precedenti con l'ente regolatore competente.

4.3. Le istruzioni del Cliente sono limitate all'attuazione delle disposizioni giuridiche o normative della legge sulla protezione dei dati, e devono essere distinte dalle richieste di modifica. Le richieste di modifica si riferiscono alle modifiche all'ambito dei servizi che non sono richieste al fine di attuare disposizioni giuridiche o normative o che vanno oltre le misure necessarie per attuare tali disposizioni. Non sono istruzioni nel senso usato nel presente Accordo, ma richieste di modifica dei servizi effettuate dal Cliente. Il Responsabile del trattamento ha la facoltà, ma non l'obbligo, di adottare tali richieste di modifica. L'adozione di tali richieste di modifica sarà remunerata separatamente.

4.4. Il Cliente fornirà le istruzioni sempre per iscritto, via fax o via e-mail. Il Cliente confermerà tempestivamente qualsiasi istruzione fornita verbalmente, in via eccezionale, per iscritto o in forma testuale.

4.5. Il Responsabile del trattamento informerà prontamente il Cliente per iscritto qualora ritenga che un'istruzione fornita dal Cliente violi le disposizioni in materia di protezione dei dati o sia, in maniera non trascurabile, errata, incompleta, contraddittoria o impraticabile dal punto di vista tecnico o legale. Al momento di fornire tale informazione, il Responsabile del trattamento richiederà espressamente per iscritto al Cliente di decidere prontamente se desidera che il Responsabile del trattamento agisca in maniera conforme all'istruzione o continui a trattare i Dati personali senza seguire l'istruzione fintanto che il Cliente avrà rivisto l'informazione e avrà preso una decisione in merito.

5. Obblighi di fornitura di informazioni del Responsabile del trattamento

5.1. In caso di Violazione dei dati personali, il Cliente potrebbe avere l'obbligo di segnalare tale violazione. Il Responsabile del trattamento dovrà informare il Cliente qualora sospetti o sia a conoscenza (in maniera più che trascurabile) di una violazione della protezione dei Dati personali del Cliente da parte del Responsabile del trattamento o delle persone che operano sotto la supervisione del Responsabile del trattamento.

5.2. Il Cliente potrà richiedere al Responsabile del trattamento di adottare tutte le misure ragionevoli e necessarie per assistere il Cliente nell'adempimento agli obblighi di segnalazione.

6. Obblighi del Cliente

6.1. Il Cliente è tenuto a informare prontamente il Responsabile del trattamento nel caso in cui riscontri la presenza di errori o irregolarità durante il controllo dei risultati del servizio fornito.

6.2. Il Cliente deve accertarsi che, sia prima dell'inizio del trattamento dei dati che dopo, siano rispettate le misure tecniche e organizzative adottate presso il Responsabile del trattamento. Il risultato di tali controlli deve essere documentato.

6.3. Il Cliente è tenuto a conformarsi agli obblighi derivanti dagli Artt. 33 e 34 del Regolamento generale sulla protezione dei dati dell'UE nei confronti dell'ente regolatore o di qualsiasi interessato coinvolto in una Violazione dei dati personali.

6.4. Il Cliente è tenuto a comunicare al Responsabile del trattamento le disposizioni per la cancellazione e la conservazione dei Dati personali e per l'attuazione di tali disposizioni.

7. Responsabile della protezione dei dati

7.1. Il Responsabile del trattamento ha nominato un Responsabile della protezione dei dati ("**DPO**"). Di seguito sono indicati i dati di contatto: datenschutz@kiongroup.com. Il Responsabile del trattamento deve comunicare al Cliente eventuali modifiche o modifiche imminenti in tal senso.

7.2. Il cliente ha nominato un responsabile della protezione dei dati, o, nella misura in cui il Cliente non sia tenuto a nominare un responsabile della protezione dei dati e non lo abbia fatto, fornirà al Responsabile del trattamento il nominativo di un collaboratore del Cliente che si sia fatto carico degli obblighi e delle responsabilità previste per un responsabile della protezione dei dati. Il Cliente comunicherà al Responsabile del trattamento eventuali modifiche o modifiche imminenti in tal senso, senza che gli sia appositamente richiesto dal Responsabile del trattamento.

7.3. Qualora il Cliente sia tenuto a nominare un rappresentante ai sensi dell'Art. 27 del Regolamento generale sulla protezione dei dati, comunicherà al Responsabile del trattamento l'identità di tale rappresentante. Il Cliente comunicherà al Responsabile del trattamento eventuali modifiche o modifiche imminenti in tal senso, senza che gli sia appositamente richiesto dal Responsabile del trattamento.

8. Persone sotto la supervisione del Responsabile del trattamento

8.1. Nell'esecuzione del trattamento dei dati ai sensi dei termini del presente Accordo, il Responsabile del trattamento dovrà avvalersi esclusivamente di persone di cui possa essere documentata la riservatezza e che siano state previamente rese edotte sulle disposizioni obbligatorie in materia di protezione dei dati applicabili nei loro confronti e di quelli delle attività di trattamento da eseguire per conto del Cliente.

8.2. Il Responsabile del trattamento si accerterà che tutte le persone sotto la sua supervisione che abbiano accesso ai Dati personali del Cliente trattino tali Dati personali esclusivamente nel rispetto dell'ambito e in conformità alle istruzioni fornite dal Cliente e alle disposizioni del presente Accordo. La sola eccezione alla disposizione soprastante riguarda casi individuali di

attività di trattamento, in particolare trasmissioni di dati, che il Responsabile del trattamento o le persone sotto la sua supervisione sono espressamente tenute a eseguire su richiesta di un tribunale o di un ente regolatore sulla base di una disposizione normativa. Nella misura consentita dalla legge, il Responsabile del trattamento è tenuto a informare il Cliente di tali ordinanze, preferibilmente prima della trasmissione di qualsiasi Dato personale.

9. Principi per il trattamento sicuro

9.1. Prendendo in considerazione la tecnologia attualmente disponibile, i costi di attuazione e la natura, l'ambito, le circostanze e i fini del Trattamento dei dati stipulato con il Cliente, nonché la probabilità e la gravità potenziale del rischio di violazione dei diritti e della libertà delle persone (analisi del rischio), il Responsabile del trattamento dovrà adottare le misure tecniche e organizzative necessarie a garantire la protezione appropriata dei Dati personali.

9.2. Al momento di stabilire il livello di sicurezza appropriato, il Responsabile del trattamento dovrà considerare i rischi inerenti al trattamento dei Dati personali del Cliente, incluso a titolo esemplificativo il rischio di distruzione imprevista o illegale, perdita, modifica, divulgazione non autorizzata o accesso non autorizzato ai Dati personali del Cliente.

9.3. Il Responsabile del trattamento è tenuto ad aggiornare e adattare le misure tecniche e organizzative al suo piano di sicurezza per tenere conto dei cambiamenti alla tecnologia disponibile, sebbene tali misure non devono scendere al di sotto del livello di sicurezza e protezione specificato nel presente Accordo.

9.4. Il Responsabile del trattamento deve documentare le misure tecniche e organizzative ai sensi del presente Accordo in maniera dettagliata nell'Allegato del presente Accordo. Il Responsabile del trattamento deve tenere aggiornata la documentazione e segnalare eventuali modifiche materiali.

9.5. Le misure tecniche e organizzative indicate nell'Allegato del presente Accordo devono essere approvate e necessarie al momento della conclusione del contratto; rappresentano tutti i requisiti che il Responsabile del trattamento è tenuto a soddisfare.

9.6. Il Cliente è tenuto a rivedere le misure tecniche e organizzative sulla base dell'analisi del rischio da lui condotta. Il Cliente ha la responsabilità di assicurarsi che le misure tecniche e organizzative offrano un livello di protezione dei dati che sia commensurato ai rischi dei Dati personali da trattare. Qualora l'analisi del rischio condotta dal Cliente generi un risultato che differisce dall'analisi del rischio condotta dal Responsabile del trattamento, il Cliente ha la facoltà di trovare un accordo con il Responsabile del trattamento per la regolazione delle misure di sicurezza. Nel caso in cui le Parti non siano in grado di trovare un accordo, hanno il diritto di risolvere l'Accordo con un preavviso di 14 giorni.

10. Controlli

10.1. Il Cliente ha la facoltà di verificare la performance dei servizi forniti dal Responsabile del trattamento rispetto ai Dati personali del Cliente e la conformità alle disposizioni del presente Accordo, incluse a titolo esemplificativo, le misure tecniche e organizzative adottate per garantire la sicurezza del trattamento.

10.2. Su richiesta, il Responsabile del trattamento deve fornire al Cliente prove dell'adozione delle misure di sicurezza tecniche e organizzative. Tra queste sono incluse

- prova della conformità ai codici di condotta approvati ai sensi dell'Art. 40 del Regolamento generale sulla protezione dei dati o
- certificazione in conformità con una procedura di certificazione approvata ai sensi dell'Art. 42 del Regolamento generale sulla protezione dei dati o
- auto-valutazione qualificata da parte di un terzo indipendente (come DPO, auditor, auditor esterni per la protezione/sicurezza dei dati) per iscritto o
- certificazione appropriata mediante un audit sulla protezione dei dati o della sicurezza IT (es. ISO 27001).

Tale prova deve contenere tutte le informazioni necessarie per dimostrare la conformità agli obblighi previsti ai sensi del presente Accordo e l'adozione delle misure tecniche e organizzative rilevanti, necessarie per garantire la sicurezza del trattamento. Il Cliente può richiedere tali informazioni una volta ogni anno solare e a intervalli più brevi solo in caso di sospetto legittimo di una violazione da parte del Responsabile del trattamento del presente Accordo, del quale il Cliente deve informare il Responsabile del trattamento per iscritto.

10.3. Il Cliente ha la facoltà di verificare la conformità al presente Accordo, in particolare la conformità alle norme di sicurezza previste per il trattamento, effettuando ispezioni preannunciate presso le sedi aziendali del Responsabile del trattamento durante i normali orari di apertura (9:00 - 18:00) una volta ogni tre anni o facendo effettuare tali controlli da un auditor esterno soggetto a obblighi di non divulgazione legali o contrattuali. Il Cliente deve fornire un preavviso scritto di due settimane per tali ispezioni. Tale restrizione nei confronti del Cliente non si applica nei casi di emergenza (ad esempio se sussiste un sospetto più che trascurabile di violazioni del presente Accordo da parte del Responsabile del trattamento); il Cliente non deve inviare un preavviso scritto al Responsabile del trattamento in tali casi.

11. Subappaltatori

11.1. Qualora e nella misura in cui tale Responsabile del trattamento abbia il diritto sulla base di un accordo esplicito concluso con il Cliente di ingaggiare ulteriori responsabili del trattamento (subappaltatori), e nel caso in cui la possibilità che tali subappaltatori abbiano accesso ai Dati personali del Cliente non possa essere esclusa, il Responsabile del trattamento ha la facoltà di ingaggiare esclusivamente tali subappaltatori e pertanto di consentire l'accesso ai Dati personali del Cliente purché abbia comunicato al Cliente per iscritto i dettagli descritti nel paragrafo seguente e abbia offerto al Cliente la possibilità di opporsi, e il Cliente non si sia opposto entro il periodo stipulato.

11.2. Le informazioni che il Responsabile del trattamento è tenuto a fornire come detto sopra devono almeno includere quanto indicato qui sotto in maniera specifica e dettagliata:

11.2.1. Identità del subappaltatore

11.2.2. Servizi specifici che il subappaltatore deve fornire al Responsabile del trattamento

11.2.3. L'esperienza, la capacità, l'affidabilità e le misure di sicurezza IT e protezione dei dati essenziali per la conformità agli obblighi in materia di protezione dei dati nel presente Accordo.

11.2.4. Le garanzie o assicurazioni del subappaltatore che si conformerà alle disposizioni del presente Accordo.

11.3. Il Cliente ha diritto, entro sette giorni dalla ricezione delle informazioni suddette, di opporsi per iscritto all'ingaggio di un subappaltatore, a condizione che abbia un motivo legittimo per farlo. In caso di opposizione, il Responsabile del trattamento è tenuto ad adempiere al presente Accordo, e a fornire i servizi e adempiere ai suoi obblighi senza avvalersi di tale subappaltatore, pur continuando ad avere la facoltà di risolvere il presente Accordo.

11.4. Qualora e nella misura in cui a un subappaltatore sia consentito l'accesso ai Dati personali del Cliente, il Responsabile del trattamento è tenuto a concludere un accordo per il trattamento dei dati con il subappaltatore che impone a quest'ultimo gli obblighi definiti nel presente Accordo. Tale accordo deve essere concluso prima che il subappaltatore abbia accesso ai Dati personali del Cliente.

12. Restituzione e cancellazione

12.1. Il Responsabile del trattamento è tenuto, dopo la risoluzione del presente Accordo o prima, se richiesto dal Cliente, a restituire o consegnare tutti i Dati personali del Cliente.

12.2. I dettagli degli obblighi di cancellazione dei dati possono essere aggiunti nell'Appendice del presente Accordo e, ove applicabile, mediante istruzioni esplicite da parte del Cliente. Il Responsabile del trattamento non è tenuto ad avere un piano di cancellazione. Il Responsabile del trattamento è tenuto a cancellare immediatamente dopo la risoluzione del presente Accordo o prima, se richiesto dal Cliente, tutti i Dati personali che non sono soggetti a un requisito di archiviazione o conservazione legale da parte del Responsabile del trattamento ai sensi della legge dell'UE o di uno Stato membro dell'UE, o a un accordo contrario esplicito che regoli l'archiviazione o la cancellazione dei Dati personali concluso con il Cliente. Il Responsabile del trattamento dovrà conservare documenti che attestino la cancellazione.

13. Costi sostenuti dal Responsabile del trattamento

Tutti i costi sostenuti dal Responsabile del trattamento o dai subappaltatori durante il trattamento dei Dati personali per conto del Cliente ai sensi del presente Accordo, e in particolare quelli sostenuti sulla base di

13.1. un obbligo a rispondere alle richieste dell'interessato secondo le istruzioni del Cliente, che in particolare implichino la correzione, cancellazione o limitazione dei Dati personali o la restituzione dei Dati personali al Cliente e, ove applicabile, la trasmissione dei dati (portabilità) o la fornitura di assistenza in tali misure,

13.2. un obbligo a fornire assistenza durante la valutazione dell'impatto della protezione dei dati,

13.3. la conformità o l'attuazione delle istruzioni del Cliente,

13.4. l'obbligo a fornire assistenza nell'adempimento alle disposizioni di divulgazione delle informazioni all'ente regolatore o agli interessati,

13.5. la produzione di un'auto-valutazione qualificata,

13.6. le ispezioni in loco effettuate dal Cliente o da auditor (esterni) ingaggiati dal Cliente, a condizione che tale ispezione abbia identificato criticità considerevoli; l'onere della prova in tal caso ricade sul Cliente,

13.7. costi aggiuntivi per misure tecniche e organizzative adottate al fine di garantire la sicurezza del trattamento, ove tali misure sono adottate come conseguenza ad analisi del rischio discordanti delle Parti,

13.8. conformità agli obblighi di restituzione o cancellazione dei Dati personali,

saranno rimborsati separatamente al Responsabile del trattamento sulla base di tariffe orarie applicate nel mercato. Il Responsabile del trattamento dovrà conservare documenti attestanti i costi e le spese sostenute.

14. Modifiche al presente Accordo

Qualora il Responsabile del trattamento sia tenuto per legge ad adottare modifiche ed emendamenti, il Cliente è tenuto a supportarli e approvarli.

15. Responsabilità

15.1. Nel caso in cui un interessato e/o un terzo intentino un'azione legale nei confronti del Responsabile del trattamento relativamente alle attività di trattamento dei dati condotte dal Responsabile del trattamento per conto del Cliente, il Cliente è tenuto a manlevare il Responsabile del trattamento e a farsi carico dei costi legali, dei danni e/o delle sanzioni associati ai sensi del diritto amministrativo o penale.

15.2. La disposizione soprastante non si applica nel caso in cui il Responsabile del trattamento non si sia conformato agli obblighi a lui spettanti ai sensi del Regolamento generale sulla protezione dei dati o non si sia conformato alle istruzioni legalmente fornite dal Cliente o abbia agito in maniera contraria a tali istruzioni.

15.3. I limiti alla responsabilità concordati tra il Cliente e il Responsabile del trattamento in favore del Responsabile del trattamento delineati nell'Accordo principale, si applicano anche alla responsabilità del Responsabile del trattamento per le attività di trattamento dei dati previste nel presente Accordo.

Linde Material Handling

Appendice

I. Categorie degli Interessati

- Clienti
- Altri: distributori, partner della rete

II. Tipi di dati

- Dati personali principali
- Dati sulla comunicazione principali
- Cronologia del cliente

III. Ambito del trattamento

I requisiti principali del Cliente sono indicati qui sotto:
Creazione ed elaborazione di notifiche e richieste di assistenza

IV. Luogo del trattamento dei Dati personali

SEE

V. Sistemi usati per il trattamento, tra cui importazione ed esportazione di dati personali da altri sistemi

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP e altri sistemi ERP dei nostri distributori, OneSignal Mobile Push Notifications

VI. Misure di sicurezza tecniche e organizzative adottate dal Responsabile del trattamento

Adozione di misure tecniche e organizzative

a. Riservatezza (Art. 32 (1) GDPR)

(1) Controllo dell'accesso (stabilimenti)

- Sistema di allarme
- Controllo automatico dell'accesso
- Blocchi di sicurezza
- Videosorveglianza degli ingressi
- Controllo chiavi/Elenco
- Reception/Portineria
- Elenco visitatori
- ID del collaboratore/visitatore
- Visitatori accompagnati da un collaboratore

(2) Controllo dell'accesso (sistemi)

- Login con nome utente e password
- Antivirus server
- Antivirus client
- Firewall
- Sistemi di rilevamento delle intrusioni
- Gestione dei dispositivi mobili
- Uso di VPN per l'accesso remoto
- Crittografia dei sistemi di storage dei dati
- Crittografia degli smartphone
- Protezione BIOS (password separata)

(3) Controllo dell'accesso (dati)

- Gestione dei diritti degli utenti
- Creazione di profili degli utenti
- Linee guida "Password sicure"
- Linee guida "Eliminazione/Distruzione"
- Linee guida generali per la protezione dei dati e/o la sicurezza dei dati
- Manuale "Blocco manuale del desktop"
- Corsi di formazione frequenti per i collaboratori
- Uso di uno schema di autorizzazione
- Gestione dei diritti degli utenti da parte degli amministratori

(4) Controllo della separazione

Separazione dell'ambiente di produzione e di prova

(5) Pseudonimizzazione (Art. 32 (1) GDPR; Art. 25 (1) GDPR)

n/d

b. Disponibilità e resilienza (Art. 32 (1) GDPR)

- Rilevatori di fiamme e fumo
- Estintori nella sala server
- Controllo della temperatura e dell'umidità nella sala server
- Sala server climatizzata
- Sistema UPS
- Multipresa di sicurezza nella sala server
- Sistema RAID/Mirroring del disco rigido
- Videosorveglianza nella sala server
- Segnale di allarme in caso di accesso non autorizzato nella sala server
- Concetto di backup e recupero (scritto)
- Controllo del backup
- Nessun apparecchio sanitario all'interno o sopra la sala server
- Esistenza di un piano di emergenza (iE BSI IT-Grundschutz 100-4)
- Partizioni separate per l'uso di sistemi e dati

c. Integrità (Art. 32 Par. 1 GDPR)

- I dati personali possono essere modificati solo dagli amministratori
- Fornitura di collegamenti crittografati come sftp e https
- Registrazione degli accessi e dei recuperi
- Panoramica dei processi regolari di recupero e trasmissione
- Personale selezionato accuratamente

d. Procedura per verifica, esame e valutazione regolari (Art. 32 (1) GDPR; Art. 25 (1) GDPR)

(1) Gestione della protezione dei dati

- Certificazione di sicurezza di ISO 27001
- L'efficacia delle misure di sicurezza tecniche è verificata almeno una volta all'anno
- I collaboratori sono formati e tenuti a mantenere la riservatezza

(2) Gestione della risposta agli incidenti

- Uso di un firewall e aggiornamento regolare
- Uso di filtri antispam e aggiornamento regolare
- Uso di scansioni antivirus e aggiornamento regolare
- Sistema di rilevamento delle intrusioni (IDS)
- Sistema di prevenzione delle intrusioni (IPS)

Protezione dei dati per impostazione predefinita (Art. 25 (2) GDPR)

- La quantità di dati personali è limitata a quanto necessario per i fini per cui sono trattati

Linde Material Handling

Umowa o przetwarzanie danych („Umowa") dotycząca aplikacji Linde Service Manager

Niniejsza umowa odnosi się do warunków aplikacji „Linde Service Manager" („**Warunki ogólne**"). Wszystkie terminy pisane wielkimi literami, ale niezdefiniowane w niniejszym dokumencie, będą miały znaczenie nadane im w Warunkach ogólnych.

Dystrybutor („**Klient**" lub „**Administrator**") reprezentowany przez Użytkownika i LMH („**Podmiot przetwarzający**" a razem z Administratorem „**Strony**") zawierają niniejszą Umowę o przetwarzanie danych osobowych w odniesieniu do Usługi. Umowa reguluje zobowiązania dotyczące przetwarzania danych Stron w odniesieniu do ochrony danych osobowych Klienta.

1. Definicje

W niniejszej Umowie poniższe terminy będą miały następujące znaczenia:

1.1. „**Podmiot przetwarzający**": Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

1.2. „**Osoba trzecia**": Osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

1.3. „**Dane osobowe**": Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („**Osobie, której dane dotyczą**"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

1.4. „**Pseudonimizacja**": Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej Osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

1.5. „**Administrator**": Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

1.6. „**Przetwarzanie**": Dowolna operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

1.7. „**Naruszenie ochrony danych osobowych**": Naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania,

nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

1.8. „**Umowa główna**": Umowa zawarta między LMH a Dystrybutorem w odniesieniu do Usług, zgodnie z Warunkami ogólnymi.

2. Przedmiot i okres obowiązywania Umowy

2.1. Niniejsza Umowa reguluje obowiązki Podmiotu przetwarzającego w zakresie Danych osobowych Klienta przetwarzanych przez Podmiot przetwarzający w imieniu Klienta.

2.2. Postanowienia niniejszej Umowy nie mają zastosowania, jeżeli i w zakresie w jakim, zgodnie ze zleceniem, Podmiot przetwarzający nie ma obowiązku prowadzenia działań związanych z przetwarzaniem w zakresie Danych osobowych Klienta. W takim przypadku Klient dopilnuje, by jego Dane osobowe były stosownie chronione przed Podmiotem przetwarzającym.

2.3. Jedynie Klient określa, czy Przetwarzanie danych jest zgodne z prawem i gwarantuje, że prawa osób, których dane dotyczą, są chronione.

2.4. Niniejsza Umowa wchodzi w życie w chwili wejścia w życie Umowy głównej, a przestaje obowiązywać w chwili, gdy przestaje obowiązywać Umowa główna. Jeżeli Podmiot przetwarzający przetwarza Dane osobowe na polecenie Klienta, nawet po zakończeniu obowiązywania Umowy głównej, niniejsza Umowa także będzie nadal obowiązywać do czasu zakończenia Przetwarzania realizowanego na polecenie Klienta.

2.5. **Niezależnie od postanowień pkt.** 2.4 **Strony mogą rozwiązać niniejszą Umowę z ważnej przyczyny.** Jeżeli przyczyna odnosi się do naruszenia obowiązku wynikającego z niniejszej Umowy, rozwiązanie jest dozwolone, dopiero kiedy okres wskazany do naprawienia naruszenia wygaśnie, a naruszenie nie zostanie naprawione lub kiedy ostrzeżenie nie przyniesie żadnego skutku. Ważna przyczyna dla Podmiotu przetwarzającego następuje, jeżeli:

2.5.1. Klient wielokrotnie wydaje niezgodne z prawem polecenia, Podmiot przetwarzający poinformował o tym Klienta bez zbędnej zwłoki, ale Klient nie odwołał polecenia;

2.5.2. Klient naruszył postanowienia niniejszej Umowy;

2.5.3. Klient wyraził sprzeciw wobec zaangażowania podwykonawcy zgodnie z niniejszą Umową.

Ponadto postanowienia Umowy głównej stosuje się odpowiednio do niniejszej Umowy.

3. Charakter, zakres i miejsce Przetwarzania

3.1. Podmiot przetwarzający jest uprawniony do uzyskania dostępu do Danych osobowych Klienta do celów świadczenia usług zgodnie z Umową główną, w zakresie opisanym w Załączniku 1. Postanowienia niniejszej Umowy nie rozszerzają obowiązków Podmiotu przetwarzającego, a jedynie je uszczegóławiają. Niniejsza Umowa reguluje także obowiązki Klienta.

3.2. Klient może wydawać polecenia, które uszczegóławiają obowiązki Podmiotu przetwarzającego.

3.3. Podmiot przetwarzający nie może korzystać z Danych osobowych do celów innych niż opisane w Umowie głównej i niniejszej Umowie, a w szczególności nie wolno mu, bez uprzedniego wyraźnego polecenia Klienta, przekazać Danych osobowych osobie trzeciej ani ujawnić ich innym odbiorcom, chyba że niniejsza Umowa stanowi inaczej.

3.4. Przetwarzanie dokonywane na podstawie niniejszej Umowy jest ograniczone do terytorium Unii Europejskiej i EOG, chyba że w Załączniku/Załącznikach do niniejszej Umowy określono inaczej.

4. Polecenia Klienta, prawa osób, których dane dotyczą, ocena skutków w zakresie ochrony danych

4.1. W drodze wydawanych poleceń Klient jest uprawniony do określania lub aktualizowania charakteru, zakresu i metody przetwarzania danych, środków ochrony, Danych osobowych, które mają być przetwarzane, oraz grup osób, których dane dotyczą. Ma to zastosowanie przede wszystkim do przypadków, kiedy organy regulacyjne lub zmiany w przepisach wymagają od Klienta wydania poleceń. Jeżeli Osoba, której dane dotyczą, skontaktuje się bezpośrednio z Podmiotem przetwarzającym, Podmiot przetwarzający niezwłocznie powiadomi o tym Klienta na piśmie i poprosi o polecenia dotyczące sposobu postępowania.

4.2. Jeżeli Klient będzie przeprowadzał ocenę skutków w zakresie ochrony danych, Podmiot przetwarzający wesprze go zgodnie z poleceniem w zakresie, w jakim jest to uzasadnione i konieczne, w tym w zakresie wcześniejszych konsultacji z właściwym organem regulacyjnym.

4.3. Polecenia Klienta są ograniczone do realizacji wymogów ustawowych lub regulacyjnych wynikających z przepisów o ochronie danych. Różnią się one od wniosków o zmianę. Wnioski o zmianę odnoszą się do zakresu usług, które nie są wymagane w celu realizacji wymogów ustawowych bądź regulacyjnych, lub które wykraczają poza środki niezbędne do realizacji takich wymogów. Nie stanowią one poleceń w znaczeniu niniejszej Umowy, a składane przez Klienta wnioski o zmianę usług. Podmiot przetwarzający ma prawo, ale nie obowiązek, zrealizować takie wnioski o zmianę. Realizacja wniosków o zmianę będzie wynagradzana odrębnie.

4.4. Klient będzie zawsze wydawał polecenia na piśmie, faksem lub pocztą elektroniczną. Klient będzie potwierdzał wszelkie polecenia w drodze wyjątku wydane ustnie bez zbędnej zwłoki, na piśmie lub w formie pisemnej lub tekstowej.

4.5. Podmiot przetwarzający będzie informował Klienta w formie tekstowej, jeżeli będzie uważał, że polecenie wydane przez Klienta narusza przepisy dotyczące ochrony danych lub jest, w sposób inny niż znikomy, błędne, niekompletne, sprzeczne bądź prawnie lub technicznie niewykonalne. Przekazując taką informację, Podmiot przetwarzający wyraźnie poprosi Klienta w formie tekstowej o niezwłoczne określenie, czy życzy sobie, by Podmiot przetwarzający zastosował się do tego polecenia, czy ma kontynuować przetwarzanie Danych osobowych bez zastosowania polecenia, do czasu gdy Klient zweryfikuje informacje i podejmie decyzję.

5. Obowiązki Podmiotu przetwarzającego w zakresie przekazywana informacji

5.1. W przypadku naruszenia ochrony danych osobowych Klient może mieć obowiązek zgłoszenia naruszenia. Podmiot przetwarzający powiadomi Klienta, jeżeli będzie podejrzewał lub będzie wiedział o (poważniejszym niż znikome) naruszeniu ochrony Danych osobowych Klienta przez Podmiot przetwarzający lub osoby pozostające pod kontrolą Podmiotu przetwarzającego.

5.2. Klient może wymagać od Podmiotu przetwarzającego podjęcia wszelkich zasadnych i niezbędnych kroków w celu wsparcia Klienta w wypełnianiu jego obowiązków w zakresie zgłaszania.

6. Obowiązki Klienta

6.1. Klient będzie niezwłocznie informował Podmiot przetwarzający, jeżeli stwierdzi błędy lub nieprawidłowości podczas sprawdzania wyniku świadczonej usługi.

6.2. Klient musi się upewnić, zarówno przed rozpoczęciem przetwarzania danych, jak i po jego zakończeniu, że środki techniczne i organizacyjne wdrożone przez Podmiot przetwarzający są przestrzegane. Wynik takiego sprawdzenia należy udokumentować.

6.3. Klient odpowiada za realizację obowiązków wynikających z art. 33 i 34 ogólnego rozporządzenia o ochronie danych UE wobec organu regulacyjnego lub wobec dowolnych osób, których dane dotyczą, dotkniętych Naruszeniem ochrony danych osobowych.

6.4. Klient powiadomi Podmiot przetwarzający o wymogach w zakresie usuwania i zachowywania Danych osobowych oraz o wdrożeniu tych wymogów.

7. Inspektor ochrony danych

7.1. Podmiot przetwarzający wyznaczył inspektora ochrony danych („**IOD**"). Dane kontaktowe: datenschutz@kiongroup.com. Podmiot przetwarzający powiadomi Klienta o zmianach lub nadchodzących zmianach w tym zakresie.

7.2. Klient wyznaczył inspektora ochrony danych lub – w zakresie, w jakim Klient nie ma obowiązku wyznaczania inspektora ochrony danych i tego nie zrobił – poda Podmiotowi przetwarzającemu nazwisko osoby ze strony Klienta, która przyjęła obowiązki i odpowiedzialność inspektora ochrony danych. Klient będzie powiadamiał Podmiot przetwarzający o zmianach lub nadchodzących zmianach w tym zakresie bez konieczności wystosowania specjalnego wniosku o to przez Podmiot przetwarzający.

7.3. Jeżeli Klient będzie miał obowiązek powołania przedstawiciela w znaczeniu art. 27 ogólnego rozporządzenia o ochronie danych UE, powiadomi Podmiot przetwarzający o tożsamości tego przedstawiciela. Klient będzie powiadamiał Podmiot przetwarzający o zmianach lub nadchodzących zmianach w tym zakresie bez konieczności wystosowania specjalnego wniosku o to przez Podmiot przetwarzający.

8. Osoby będące pod kontrolą Podmiotu przetwarzającego

8.1. Realizując przetwarzanie danych zgodnie z postanowieniami niniejszej Umowy, Podmiot przetwarzający będzie korzystał wyłącznie z osób, które podjęły udokumentowane zobowiązanie do zachowania poufności i które zapoznały się z wyprzedzeniem z przepisami ustawowymi o ochronie danych istotnymi dla nich oraz dla działań związanych z przetwarzaniem danych, które mają być prowadzone w imieniu Klienta.

8.2. Podmiot przetwarzający zagwarantuje, że wszystkie osoby znajdujące się pod jego kontrolą, które mają dostęp do Danych osobowych Klienta, przetwarzają takie Dane osobowe wyłącznie w zakresie poleceń Klienta i postanowień niniejszej Umowy oraz zgodnie z nimi. Jedyny wyjątek od powyższego postanowienia dotyczy indywidualnych przypadków działań związanych z

przetwarzaniem danych, w szczególności przekazywania danych, do których wykonania Podmiot przetwarzający lub osoby znajdujące się pod jego kontrolą są wyraźnie zobligowane przez sąd lub organ państwowy na podstawie przepisów ustawowych. W zakresie dozwolonym przepisami prawa Podmiot przetwarzający powiadomi Klienta o takich obowiązkach, najlepiej przed przekazaniem Danych osobowych.

9. Zasady bezpiecznego przetwarzania

9.1. Uwzględniając dostępną aktualnie technologię, koszty wdrażania oraz charakter, zakres, okoliczności i cele przetwarzania danych ustalone z Klientem, jak również prawdopodobieństwo i potencjalną wagę zagrożeń dla praw i wolności osób (analiza ryzyka), Podmiot przetwarzający wprowadzi środki techniczne i organizacyjne niezbędne do zapewnienia odpowiedniej ochrony Danych osobowych.

9.2. Oceniając stosowny poziom ochrony, Podmiot przetwarzający uwzględni ryzyko właściwe dla przetwarzania Danych osobowych Klienta, w tym w szczególności ryzyko niezamierzonego lub bezprawnego zniszczenia, a także utraty, zmiany, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych Klienta.

9.3. Podmiot przetwarzający zaktualizuje i dostosuje środki techniczne i organizacyjne w swoim planie bezpieczeństwa w celu uwzględnienia zmian w dostępnej technologii, chociaż środki te nie mogą spaść poniżej poziomu bezpieczeństwa i ochrony określonego w niniejszej Umowie.

9.4. Podmiot przetwarzający szczegółowo udokumentuje środki techniczne i organizacyjne zgodnie z niniejszą Umową w Załączniku do niniejszej Umowy. Podmiot przetwarzający musi prowadzić aktualną dokumentację i dokumentować wszelkie istotne zmiany.

9.5. Środki techniczne i organizacyjne zawarte w Załączniku do niniejszej Umowy uznaje się za zatwierdzone i niezbędne w chwili zawarcia umowy; stanowią one całość zobowiązań, które Podmiot przetwarzający winien spełnić.

9.6. Klient ma obowiązek weryfikacji środków technicznych i organizacyjnych w oparciu o własną analizę ryzyka. Klient odpowiada za dopilnowanie, by środki techniczne i organizacyjne zapewniały poziom ochrony danych proporcjonalny do zagrożeń dla przetwarzanych Danych osobowych. Jeżeli analiza ryzyka przeprowadzona przez Klienta da inne wyniki niż analiza ryzyka Podmiotu przetwarzającego, Klient ma prawo negocjować z Podmiotem przetwarzającym korektę środków bezpieczeństwa. Jeżeli Strony nie będą w stanie dojść do porozumienia, każda z nich będzie mieć prawo do rozwiązania Umowy za czternastodniowym wypowiedzeniem.

10. Kontrole

10.1. Klient jest uprawniony do sprawdzania realizacji usług przez Podmiot przetwarzający w zakresie Danych osobowych klienta oraz przestrzegania postanowień niniejszej Umowy, w tym w szczególności środków technicznych i organizacyjnych, w celu zapewnienia bezpieczeństwa przetwarzania.

10.2. Na żądanie Podmiot przetwarzający przekaże Klientowi dowody potwierdzające wdrożenie środków technicznych i organizacyjnych. Czyli

- dowód przestrzegania zatwierdzonych kodeksów postępowania zgodnie z art. 40 ogólnego rozporządzenia o ochronie danych lub

- certyfikat odpowiadający zatwierdzonej procedurze certyfikacji zgodnie z art. 42 ogólnego rozporządzenia o ochronie danych lub
- kwalifikowaną samoocenę niezależnej osoby trzeciej (takiej jak IOD, audytor, zewnętrzni audytorzy ochrony danych/bezpieczeństwa) w formie tekstowej lub
- stosowny certyfikat wydany w wyniku audytu bezpieczeństwa informatycznego lub ochrony danych (np. ISO 27001).

Takie dowody muszą zawierać wszystkie informacje niezbędne do wykazania realizacji obowiązków wdrożenia wynikających z niniejszej Umowy oraz stosownych środków technicznych i organizacyjnych, które są przeznaczone do zagwarantowania bezpieczeństwa przetwarzania. Klient może wymagać takich informacji raz w roku kalendarzowym oraz w krótszych okresach, wyłącznie w przypadku uzasadnionego podejrzenia naruszenia przez Podmiot przetwarzający niniejszej Umowy, o czym Klient winien powiadomić Podmiot przetwarzający w formie tekstowej.

10.3. Klient ma prawo sprawdzać przestrzeganie Umowy, w szczególności przestrzeganie bezpieczeństwa przetwarzania poprzez przeprowadzanie zapowiedzianych kontroli na miejscu, w siedzibie Podmiotu przetwarzającego, w czasie standardowych godzin pracy (09:00 - 18:00) raz na trzy lata lub zlecać przeprowadzanie takich kontroli zewnętrznemu audytorowi, który podlega ustawowym lub umownym zobowiązaniom do zachowania poufności. Klient musi zapowiadać takie kontrole w formie tekstowej z dwutygodniowym wyprzedzeniem. Powyższe ograniczenie Klienta nie obowiązuje w przypadkach pilnych (na przykład, jeżeli istnieje podejrzenie poważniejszych niż znikome naruszeń niniejszej Umowy przez Podmiot przetwarzający); w takich przypadkach Klient nie musi powiadamiać Podmiotu przetwarzającego w formie tekstowej z wyprzedzeniem.

11. Podwykonawcy

11.1. Jeżeli i w zakresie, w jakim Podmiot przetwarzający ma prawo, na mocy wyraźnego porozumienia z Klientem, do zaangażowania dodatkowych podmiotów przetwarzających (podwykonawców), i jeżeli nie można wykluczyć możliwości uzyskania dostępu do Danych osobowych Klienta przez takich podwykonawców, Podmiot przetwarzający może zaangażować takich podwykonawców, a tym samym potencjalnie udzielić dostępu do Danych osobowych Klienta, jedynie gdy przekazał Klientowi w formie tekstowej szczegóły wskazane w następnym podpunkcie i dał Klientowi możliwość wniesienia sprzeciwu, a Klient nie wniósł sprzeciwu we wskazanym terminie.

11.2. Informacje, jakie Podmiot przetwarzający winien przekazać zgodnie z powyższymi postanowieniami, obejmują co najmniej poniższe informacje w konkretnej i szczegółowej formie:

11.2.1. dane podwykonawcy,

11.2.2. konkretne usługi, jakie podwykonawca ma świadczyć na rzecz Podmiotu przetwarzającego,

11.2.3. doświadczenie, możliwości, niezawodność oraz informatyczne środki bezpieczeństwa i ochrony danych, które są niezbędne do przestrzegania zobowiązań w zakresie ochrony danych wynikających z niniejszej Umowy,

11.2.4. gwarancje lub zapewnienia podwykonawcy, że będzie przestrzegać postanowień niniejszej Umowy.

11.3. Klient jest uprawniony, w terminie siedmiu dni od daty otrzymania powyższych informacji, do wniesienia sprzeciwu w formie tekstowej wobec zaangażowania podwykonawcy, o ile ma ku temu uzasadniony powód. W przypadku takiego sprzeciwu Podmiot przetwarzający ma obowiązek zrealizować niniejszą Umowę, świadczyć usługi oraz wypełniać obowiązki bez korzystania z usług danego podwykonawcy, jednocześnie zachowując prawo do rozwiązania niniejszej Umowy.

11.4. Jeżeli i w zakresie w jakim podwykonawca uzyska dostęp do Danych osobowych Klienta, Podmiot przetwarzający ma obowiązek zawrzeć z podwykonawcą umowę o przetwarzaniu danych, która nakłada na podwykonawcę obowiązki określone w niniejszej Umowie. Taka umowa winna zostać zawarta zanim podwykonawca po raz pierwszy uzyska dostęp do Danych osobowych Klienta.

12. Zwrot i usunięcie

12.1. Na wniosek Klienta, po zakończeniu obowiązywania niniejszej Umowy lub wcześniej Podmiot przetwarzający ma obowiązek zwrócić lub przekazać wszystkie Dane osobowe Klienta.

12.2. Szczegóły dotyczące usuwania danych mogą być dodawane w Załączniku do niniejszej Umowy oraz, w stosownych przypadkach, na wyraźne polecenie Klienta. Podmiot przetwarzający nie ma obowiązku posiadania własnego planu usuwania. Podmiot przetwarzający ma obowiązek niezwłocznie po zakończeniu obowiązywania niniejszej Umowy lub wcześniej, na wniosek Klienta, usunąć wszystkie Dane osobowe, które nie podlegają ustawowemu obowiązkowi przechowywania lub zachowywania ze strony Podmiotu przetwarzającego na mocy prawa UE lub państwa członkowskiego UE ani wyraźnemu przeciwnemu porozumieniu regulującemu przechowywanie lub usuwanie Danych osobowych zawartemu z Klientem. Podmiot przetwarzający sporządzi i będzie przechowywać dokumentację dotyczącą usunięcia danych.

13. Koszty ponoszone przez Podmiot przetwarzający

Wszystkie koszty poniesione przez Podmiot przetwarzający lub podwykonawców w wyniku przetwarzania Danych osobowych w imieniu Klienta na mocy niniejszej Umowy, w szczególności koszty poniesione na podstawie

13.1. zobowiązania do odpowiadania na żądania składane przez osoby, których dane dotyczą, zwłaszcza żądania sprostowania, usunięcia lub ograniczenia przetwarzania Danych osobowych bądź zwrotu Danych osobowych Klientowi oraz, w stosownych przypadkach, przeniesienia danych (możliwość przenoszenia) lub pomocy w takich krokach,

13.2. zobowiązania do pomocy w ocenie skutków w zakresie ochrony danych,

13.3. przestrzegania poleceń Klienta lub ich realizacji,

13.4. zobowiązania do zapewnienia pomocy w realizacji zobowiązań do ujawnienia informacji organowi regulacyjnemu lub osobom, których dane dotyczą,

13.5. sporządzenia kwalifikowanej samooceny,

13.6. kontroli na miejscu przeprowadzanych przez Klienta lub (zewnętrznych) audytorów, wymaganych przez Klienta, chyba że w wyniku takiej kontroli stwierdzono znaczne braki; w tym przypadku ciężar dowodu spoczywa na Kliencie,

13.7. dodatkowych kosztów środków technicznych i organizacyjnych dla zagwarantowania bezpieczeństwa przetwarzania, jeżeli takie środki są wdrażane w wyniku różniących się analiz ryzyka przeprowadzonych przez Strony,

13.8. przestrzegania obowiązku zwrotu lub usunięcia Danych osobowych,

zostaną odrębnie zwrócone Podmiotowi przetwarzającemu na podstawie rynkowych stawek godzinowych. Podmiot przetwarzający będzie prowadził ewidencję poniesionych kosztów i wydatków.

14. Zmiany niniejszej Umowy

Jeżeli Podmiot przetwarzający jest zobowiązany z mocy prawa do wprowadzenia zmian, Klient ma obowiązek ich wspierania i zatwierdzenia.

15. Odpowiedzialność

15.1. Jeżeli osoba, której dane dotyczą, lub osoba trzecia wytoczy powództwo przeciwko Podmiotowi przetwarzającemu w związku z działaniami związanymi z przetwarzaniem danych prowadzonymi przez Podmiot przetwarzający w imieniu Klienta, Klient będzie zobowiązany do zwolnienia Podmiotu przetwarzającego z odpowiedzialności i opłacenia powiązanych z tym kosztów prawnych, odszkodowań lub grzywien wynikających z przepisów prawa administracyjnego lub karnego.

15.2. Powyższe postanowienie nie ma zastosowania, jeżeli Podmiot przetwarzający nie wywiązał się z obowiązków nałożonych na niego na podstawie ogólnego rozporządzenia o ochronie danych lub nie zastosował się do poleceń Klienta wydanych zgodnie z prawem, lub postąpił wbrew takim poleceniom.

15.3. Ograniczenia odpowiedzialności ustalone między Klientem a Podmiotem przetwarzającym dla Podmiotu przetwarzającego w Umowie głównej mają także zastosowanie do odpowiedzialności Podmiotu przetwarzającego w zakresie działań związanych z przetwarzaniem danych wynikających z niniejszej Umowy.

Linde Material Handling

Załącznik

I. Kategorie osób, których dane dotyczą

- Klienci
- Inne: dystrybutorzy, partnerzy w sieci

II. Rodzaje danych

- Dane podstawowe personelu
- Dane podstawowe do komunikacji
- Historia klientów

III. Zakres przetwarzania

Podstawowe wymogi Klienta:
Tworzenie i przetwarzanie powiadomień o usłudze i zamówień

IV. Miejsce, w którym mają być przetwarzane dane osobowe

EOG

V. System(y) przetwarzania, w tym import i eksport danych osobowych z innych systemów

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP i inne systemy ERP naszych dystrybutorów, Powiadomienia push OneSignal Mobile

VI. Techniczne i organizacyjne środki bezpieczeństwa Podmiotu przetwarzającego

Realizacja środków technicznych i organizacyjnych

a. Poufność (art. 32 ust. 1 RODO)

(1) Kontrola dostępu (siedziba)

- Alarm
- Automatyczna kontrola dostępu
- Zamki bezpieczeństwa
- Nadzór wideo wejść
- Kontrola klucza / lista
- Recepcja / portier
- List odwiedzających
- Identyfikator pracownika / odwiedzającego

Odwiedzający przebywają w towarzystwie pracownika

(2) Kontrola dostępu (systemy)

- Login z nazwą użytkownika + hasło
- Serwer oprogramowania antywirusowego
- Klienci oprogramowania antywirusowego
- Zapora sieciowa
- Systemy wykrywania nieautoryzowanego dostępu
- Zarządzanie urządzeniami mobilnymi
- Wykorzystanie VPN do zdalnego dostępu
- Szyfrowanie przechowywania danych
- Szyfrowanie smartfonów
- Ochrona BIOSU (odrębne hasło)

(3) Kontrola dostępu (dane)

- Zarządzanie prawami użytkowników
- Tworzenie profili użytkowników
- Wytyczne „Bezpieczne hasła"
- Wytyczne „Usuwanie / niszczenie"
- Ogólne wytyczne w sprawie ochrony danych lub bezpieczeństwa danych
- „Ręczna blokada komputera"
- Częste szkolenia pracowników
- Użycie schematu autoryzacji
- Zarządzanie prawami użytkowników przez administratorów

(4) Kontrola oddzielenia

Oddzielenie środowiska produkcyjnego i testowego

(5) Pseudonimizacja (art. 32 ust. 1 RODO; art. 25 ust. 1 RODO)

nie dot.

b. Dostępność i odporność (art. 32 ust. 1 RODO)

- Czujnik ognia i dymu
- Gaśnica w każdej serwerowni
- Kontrola temperatury i wilgotności w serwerowni
- Klimatyzowana serwerownia
- System zasilania awaryjnego
- Zabezpieczająca listwa zasilająca używana w serwerowni
- System RAID / lustrzane odbicie HD
- Serwerownia nadzoru wideo
- Sygnał alarmowy w przypadku nieuprawnionego dostępu do serwerowni
- Koncepcja kopii zapasowej i odzyskiwania (słownie)
- Kontrola kopii zapasowych
- Brak urządzeń sanitarnych w serwerowni lub ponad nią
- Istnienie planu awaryjnego (iE BSI IT-Grundschutz 100-4)
- Odrębne partycje dla systemów operacyjnych i danych

c. Integralność (art. 32 ust. 1 RODO)

- Dane osobowe mogą być zmieniane wyłącznie przez administratorów
- Dostarczanie połączeń szyfrowanych takich jak sftp, https
- Rejestrowanie dostępu i pobierania danych
- Przegląd regularnych procesów pobierania i transferu
- Starannie dobrany personel

d. Procedura regularnego testowania, uzyskiwania dostępu i oceniania (art. 32 ust. 1 RODO; art. 25 ust. 1 RODO)

(1) Zarządzanie ochroną danych

- Certyfikat bezpieczeństwa ISO 27001
- Skuteczność technicznych środków bezpieczeństwa jest weryfikowana co najmniej raz do roku
- Szkoleni pracownicy mają obowiązek zachowania poufności

(2) Zarządzanie reagowaniem na incydenty

- Korzystanie z zapory sieciowej i regularne aktualizacje
- Korzystanie z filtrów antyspamowych i regularne aktualizacje
- Korzystanie ze skanera antywirusowego i regularne aktualizacje
- System wykrywania nieautoryzowanego dostępu
- System zapobiegania nieautoryzowanemu dostępowi

Domyślna ochrona danych (art. 25 ust. 2 RODO)

- Ilość danych osobowych jest ograniczona do tego, co niezbędne do celów, dla których są one przetwarzane.

Linde Material Handling

Acordo de Tratamento de Dados («acordo») relativo ao Linde Service Manager

O presente acordo incide sobre os termos e condições gerais do «Linde Service Manager» («**TCG**»). Todos os termos utilizados e não definidos no presente acordo têm o significado que lhes é atribuído nos TCG.

O distribuidor («**cliente**» ou «**responsável pelo tratamento**»), representado pelo utilizador, e a LMH («**subcontratante**» designado em conjunto com o responsável pelo tratamento por «**partes**») celebram o presente acordo de tratamento de dados pessoais relativo ao Serviço. O presente acordo rege as obrigações das partes em matéria de proteção dos dados pessoais do cliente.

1. Definições

Para efeitos do presente acordo, entende-se por:

1.1. «**subcontratante**», uma pessoa singular ou coletiva, autoridade pública, agência ou outra entidade, que proceda ao tratamento de dados pessoais em nome do responsável pelo tratamento.

1.2. «**terceiro**», uma pessoa singular ou coletiva, autoridade pública, agência ou outra entidade que não o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas autorizadas a tratar dados pessoais sob a supervisão direta do responsável pelo tratamento ou do subcontratante.

1.3. «**dados pessoais**», quaisquer informações relativas a uma pessoa singular identificada ou identificável («**titular dos dados**»); uma pessoa singular identificável é uma pessoa que pode ser direta ou indiretamente identificada, nomeadamente por referência a um identificador, como o nome, um número de identificação, dados de localização, identificadores por via eletrónica ou um ou vários fatores específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa singular em causa.

1.4. «**pseudonimização**», o tratamento de dados pessoais de modo a que os mesmos não possam ser relacionados especificamente com um titular de dados específico sem recorrer a informação adicional, desde que essa informação adicional seja conservada em separado e seja objeto de medidas técnicas e organizativas que garantam que esses dados não sejam associados a uma pessoa singular identificada ou identificável.

1.5. «**responsável pelo tratamento**», a pessoa singular ou coletiva, autoridade pública, agência ou outra entidade, que, sozinha ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais; no caso de as finalidades e os meios do tratamento em questão serem determinados pela legislação da União ou de um Estado-Membro, a designação do responsável pelo tratamento ou os critérios específicos para a mesma podem reger-se pela legislação da União ou do Estado-Membro.

1.6. «**tratamento**», qualquer operação ou conjunto de operações executada com dados pessoais ou conjuntos de dados pessoais, por meios automatizados ou não, como a recolha, registo, organização, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, alinhamento ou combinação, restrição, apagamento ou destruição.

1.7. «**violação de dados pessoais**», uma violação da segurança que, de forma acidental ou ilegítima, conduza à destruição, perda, alteração, divulgação não autorizada ou acesso a dados pessoais transmitidos, armazenados ou submetidos a outro tipo de tratamento.

1.8. «**acordo principal**», o acordo celebrado entre a LMH e o distribuidor relativamente aos serviços, de acordo com os TCG.

2. Objeto e termo do presente acordo

2.1. O presente acordo rege os deveres do subcontratante relativamente aos dados pessoais do cliente tratados pelo subcontratante em nome do cliente.

2.2. As disposições do presente acordo não são aplicáveis, se e na medida em que, de acordo com o compromisso assumido, não forem necessárias atividades de tratamento dos dados pessoais do cliente por parte do subcontratante. Nesse caso, o cliente deverá assegurar-se de que os seus dados pessoais estão convenientemente protegidos pelo subcontratante.

2.3. Cabe exclusivamente ao cliente determinar se o tratamento é legítimo e assegurar a proteção dos direitos dos titulares dos dados.

2.4. O presente acordo tem início no momento em que tiver início o acordo principal e cessa após o termo do acordo principal. Se o subcontratante, a pedido do cliente, efetuar o tratamento de dados pessoais após o termo do acordo principal, o presente acordo mantém-se em vigor até estar concluído o tratamento de dados efetuado a pedido do cliente.

2.5. Não obstante o disposto no ponto 2.4, as partes podem rescindir o presente acordo por justa causa. Se a referida causa estiver relacionada com o incumprimento de um dever decorrente do acordo, a rescisão só é possível se, depois de decorrido um período definido para sanar o incumprimento, este não tiver sido sanado, ou se uma advertência não tiver produzido quaisquer efeitos. Considera-se haver especial justa causa na perspetiva do subcontratante, se

2.5.1. o cliente tiver emitido repetidamente instruções ilegítimas, o subcontratante tiver sem demora informado o cliente do facto e o cliente não tiver anulado as instruções em causa;

2.5.2. o cliente tiver violado as disposições do presente acordo;

2.5.3. o cliente tiver contestado um subadjudicatário contratado em conformidade com o presente acordo.

Aplicam-se, além disso, mutatis mutandis ao presente acordo os termos do acordo principal.

3. Natureza, âmbito e local do tratamento

3.1. O subcontratante está autorizado a aceder aos dados pessoais do cliente para fins de prestação de serviços em conformidade com o acordo principal, se tal for pertinente nos termos do anexo 1. As disposições do presente acordo não ampliam os deveres do subcontratante, limitando-se a especificá-los mais pormenorizadamente. O presente acordo rege igualmente os deveres do cliente.

3.2. O cliente pode emitir instruções que especifiquem mais pormenorizadamente os deveres do subcontratante.

3.3. Salvo disposição em contrário no presente acordo, o subcontratante não está autorizado a utilizar os dados pessoais para outros fins diferentes dos descritos no acordo principal e no presente acordo, não devendo nomeadamente transferir os dados pessoais para terceiros nem divulgá-los a outros destinatários sem instruções explícitas prévias do cliente nesse sentido.

3.4. No âmbito do presente acordo, o tratamento de dados restringe-se ao território da União Europeia e do EEE, salvo disposição em contrário constante no(s) anexo(s) do presente acordo.

4. Instruções do cliente, direitos dos titulares dos dados, avaliação do impacto na proteção dos dados

4.1. Através das suas instruções, o cliente está autorizado a especificar ou atualizar a natureza, âmbito e método do tratamento dos dados, as medidas de segurança, os dados pessoais a processar e os grupos de titulares de dados. Isto aplica-se nomeadamente quando uma autoridade de controlo ou uma alteração da legislação impuserem ou solicitarem ao cliente a emissão de instruções. No caso de um titular de dados contactar diretamente o subcontratante, este deve informar sem demora o cliente, sob a forma de texto, e solicitar instruções sobre o procedimento a adotar.

4.2. No caso de o cliente levar a cabo uma avaliação do impacto na proteção dos dados, o subcontratante deve, na medida do necessário e do razoável, prestar-lhe assistência de acordo com as instruções, nomeadamente no que diz respeito a uma eventual consulta prévia por parte da autoridade de controlo competente.

4.3. As instruções do cliente limitam-se à aplicação dos requisitos legais ou regulamentares da legislação em matéria de proteção de dados. Essas instruções não devem ser confundidas com pedidos de alteração. Os pedidos de alteração referem-se a alterações do âmbito dos serviços que não são solicitadas para fins de aplicação dos requisitos legais ou regulamentares ou que ultrapassam as medidas necessárias à aplicação desses requisitos. Não constituem instruções na aceção do presente acordo, mas pedidos do cliente para alteração dos serviços. O subcontratante está autorizado, mas não obrigado, a aplicar as alterações pedidas. A aplicação das alterações pedidas é remunerada separadamente.

4.4. O cliente deve emitir sempre as suas instruções por escrito, via fax ou correio eletrónico. O cliente deve confirmar sem demora, por escrito ou sob a forma de texto, quaisquer instruções emitidas oralmente a título excecional.

4.5. Caso o subcontratante considere que uma instrução do cliente viola as disposições em matéria de proteção de dados ou está, para lá do negligenciável, errada, incompleta, contraditória ou é legal ou tecnicamente inexequível, o subcontratante deve informar sem demora o cliente sob a forma de texto. Ao fornecer estas informações, o subcontratante deve solicitar explicitamente ao cliente, sob a forma de texto, que declare sem demora se pretende que o subcontratante cumpra as instruções ou continue o tratamento de dados pessoais sem seguir as instruções, até que o cliente analise as informações e tome uma decisão.

5. Deveres de prestação de informações do subcontratante

5.1. Em caso de violação de dados pessoais, o cliente pode ter o dever de notificar essa violação. Caso suspeite ou tenha conhecimento de uma violação (para lá do negligenciável) da proteção de dados pessoais do cliente por parte do subcontratante ou de pessoas sob o seu controlo, o subcontratante deve informar o cliente.

5.2. O cliente pode solicitar ao subcontratante que tome todas as medidas razoáveis e necessárias para lhe prestar assistência no cumprimento dos seus deveres de notificação.

6. Deveres do cliente

6.1. O cliente deve informar sem demora o subcontratante, caso detete erros ou irregularidades, ao verificar o resultado dos serviços prestados.

6.2. O cliente deve certificar-se, tanto antes como depois do início do tratamento dos dados, de que estão a ser cumpridas pelo subcontratante as medidas técnicas e organizativas adotadas. O resultado destas verificações deve ficar registado.

6.3. O cliente é responsável pelo cumprimento das obrigações para com a autoridade de controlo e para com todos os titulares de dados afetados pela violação de dados pessoais, definidas nos artigos 33.º e 34.º do Regulamento Geral de Proteção de Dados da UE.

6.4. O cliente deve informar o subcontratante de todos os pedidos de apagamento e retenção de dados pessoais e da resposta a esses pedidos.

7. Responsável pela proteção de dados

7.1. O subcontratante nomeou um responsável pela proteção de dados («**RPD**»). Os seus dados de contacto são os seguintes: datenschutz@kiongroup.com. O subcontratante deve notificar ao cliente qualquer alteração introduzida ou iminente nesta matéria.

7.2. O cliente designou um responsável pela proteção de dados ou, caso o não tenha feito por não lhe ser exigida a designação de um responsável pela proteção de dados, comunica ao subcontratante o nome de um colaborador do cliente que aceite os deveres e responsabilidades de um responsável pela proteção de dados. O cliente deve notificar ao subcontratante qualquer alteração introduzida ou iminente nesta matéria, sem que o subcontratante tenha de o solicitar especificamente.

7.3. Se for solicitada ao cliente a designação de um representante na aceção do artigo 27.º do Regulamento Geral de Proteção de Dados da UE, o cliente deve notificar ao subcontratante a identidade desse representante. O cliente deve notificar ao subcontratante qualquer alteração introduzida ou iminente nesta matéria, sem que o subcontratante tenha de o solicitar especificamente.

8. Pessoas sob o controlo do subcontratante

8.1. O subcontratante deve apenas confiar o tratamento de dados nos termos do presente acordo a pessoas que tenham assinado um termo de confidencialidade e sido antecipadamente familiarizadas com as disposições legais em matéria de proteção de dados pertinentes para elas próprias e para as atividades de tratamento a executar em nome do cliente.

8.2. O subcontratante deve garantir que todas as pessoas sob o seu controlo com acesso aos dados pessoais do cliente tratam exclusivamente esses dados no âmbito das instruções do cliente e de acordo com essas instruções e com as disposições do presente acordo. A única exceção à disposição supra diz respeito a casos pontuais de atividades de tratamento, nomeadamente transferências de dados, a que o subcontratante ou as pessoas sob o seu controlo se vejam obrigados por ordem de um tribunal ou autoridade governamental, com base numa disposição legal. Na medida em que a lei o permita, o subcontratante deve informar o cliente de tais ordens antes da transferência de quaisquer dados pessoais.

9. Princípios de tratamento seguro

9.1. Tendo em conta a tecnologia atualmente disponível, os custos de aplicação, a natureza, âmbito, circunstâncias e finalidades do tratamento de dados estipulado com o cliente, assim como a probabilidade e potencial gravidade do risco para os direitos e liberdades individuais (análise de risco), o subcontratante deve adotar as medidas técnicas e organizativas necessárias para garantir uma proteção adequada dos dados pessoais.

9.2. Ao avaliar o nível de segurança adequado, o subcontratante deve ter em consideração os riscos inerentes ao tratamento dos dados pessoais do cliente, nomeadamente o risco de destruição inadvertida ou ilícita, e a perda, modificação, divulgação não autorizada ou acesso não autorizado aos dados pessoais do cliente.

9.3. No seu plano de segurança, o subcontratante deve atualizar e ajustar as medidas técnicas e organizativas de acordo com as alterações na tecnologia disponível, não devendo, porém, essas medidas ficar abaixo dos níveis de segurança e proteção especificados no presente acordo.

9.4. O subcontratante deve registar todas as medidas técnicas e organizativas adotadas ao abrigo do presente acordo, detalhadas no anexo do presente acordo. O subcontratante deve manter esta documentação atualizada e registar qualquer alteração substancial.

9.5. As medidas técnicas e organizativas constantes do anexo do presente acordo são consideradas aprovadas e necessárias a partir do momento de celebração do contrato e representam a totalidade dos requisitos que o subcontratante é obrigado a satisfazer.

9.6. O cliente é obrigado a rever as referidas medidas técnicas e organizativas com base na sua própria análise de risco. O cliente é responsável por garantir que as referidas medidas técnicas e organizativas proporcionem um nível de proteção de dados proporcional aos riscos dos dados pessoais a tratar. Se a análise de risco do cliente produzir resultados diferentes dos da análise de risco do subcontratante, o cliente tem direito a negociar com o subcontratante um ajustamento das medidas de segurança. Caso não seja possível um acordo entre as partes, qualquer uma delas tem direito a rescindir o acordo com um aviso prévio de 14 dias.

10. Controlos

10.1. O cliente tem direito a verificar o desempenho dos serviços prestados pelo subcontratante relativamente aos dados pessoais do cliente e o cumprimento das disposições do presente acordo, nomeadamente as medidas técnicas e organizativas para garantia da segurança do tratamento.

10.2. Se tal lhe for solicitado, o subcontratante deve apresentar ao cliente provas da implementação das medidas técnicas e organizativas de segurança, designadamente

- provas do cumprimento dos códigos de conduta definidos no artigo 40.º do Regulamento Geral de Proteção de Dados ou
- certificação de acordo com um procedimento de certificação aprovado, nos termos do artigo 42.º do Regulamento Geral de Proteção de Dados ou
- autoavaliação idónea por meio de terceiro independente (por exemplo, um RPD, auditor ou auditor externo de proteção/segurança dos dados) sob a forma de texto ou
- certificação adequada por meio de uma auditoria de cibersegurança ou de proteção de dados (por exemplo, nos termos da ISO 27001).

As provas em questão devem conter todas as informações necessárias para provar o cumprimento e aplicação das obrigações decorrentes do presente acordo e de todas as medidas técnicas e organizativas, destinadas a garantir a segurança do tratamento. O cliente pode solicitar estas informações uma vez por ano civil e a intervalos mais curtos apenas em caso de suspeita legítima de violação do presente acordo pelo subcontratante, a qual deve ser notificada ao subcontratante sob a forma de texto.

10.3. O cliente tem direito a verificar o cumprimento do acordo, em particular o cumprimento em matéria de segurança do tratamento, levando a cabo inspeções in situ, previamente anunciadas, nas instalações comerciais do subcontratante, durante o horário normal de funcionamento (das 9h00 às 18h00), de três em três anos ou de confiar as referidas verificações a um auditor externo, sujeito a um obrigação legal ou contratual de confidencialidade. O cliente deve notificar as inspeções em causa com duas semanas de antecedência. Esta restrição não se aplica ao cliente em casos urgentes (por exemplo, se houver suspeita de violações não negligenciáveis do presente acordo por parte do subcontratante); nesses casos, o cliente não é obrigado a notificar o subcontratante sob a forma de texto.

11. Subadjudicatários

11.1. Se e na medida em que um acordo explícito com o cliente permita ao subcontratante contratar subcontratantes adicionais (subadjudicatários) e não puder ser excluída a possibilidade de acesso desses subadjudicatários aos dados pessoais do cliente, o subcontratante pode contratar os referidos subadjudicatários e possibilitar, por conseguinte, o seu potencial acesso aos dados pessoais do cliente, se tiver informado previamente o cliente, sob a forma de texto, acerca dos elementos enunciados no parágrafo seguinte e concedido ao cliente a possibilidade de contestação, sem que este tenha contestado no prazo estipulado.

11.2. As informações a serem fornecidas pelo subcontratante nos termos supra devem incluir, pelo menos, os seguintes elementos, de forma específica e detalhada:

11.2.1. identidade do subcontratante,

11.2.2. serviços específicos a prestar pelo subadjudicatário ao subcontratante,

11.2.3. experiência, capacidade, fiabilidade e medidas de cibersegurança e proteção dos dados essenciais para cumprimento das obrigações estipuladas no presente acordo em matéria de proteção dos dados.

11.2.4. garantias e compromissos apresentadas pelo subadjudicatário de que irá cumprir as disposições do presente acordo.

11.3. Até sete dias após ter recebido as informações supra, o cliente tem o direito de apresentar, sob a forma de texto, uma contestação da contratação do subadjudicatário, se para isso dispuser de motivos legítimos. Na eventualidade de uma tal contestação, o subcontratante é obrigado a agir em conformidade com o presente acordo, prestando os seus serviços e cumprindo as suas obrigações sem recorrer ao subadjudicatário em questão, assistindo-lhe, no entanto, o direito de rescindir o presente acordo.

11.4. Se e na medida em que seja concedido ao subadjudicatário acesso aos dados pessoais do cliente, o subcontratante é obrigado a celebrar com o subadjudicatário um acordo de tratamento de dados, que imponha ao subadjudicatário as obrigações definidas no presente acordo. O acordo em causa tem de ser celebrado antes de o subadjudicatário aceder pela primeira vez aos dados pessoais do cliente.

12. Devolução e apagamento

12.1. Após o termo do presente acordo ou antes disso, se o cliente o solicitar, o subcontratante é obrigado a devolver ou entregar todos os dados pessoais do cliente.

12.2. Podem ser acrescentados pormenores das obrigações de apagamento de dados no anexo do presente acordo e, se for o caso, por instruções explícitas do cliente. O subcontratante não é obrigado a dispor de um plano de apagamento próprio. Após o termo do presente acordo ou antes disso, se o cliente o solicitar, o subcontratante é obrigado a apagar todos os dados pessoais que não estejam sujeitos a um requisito legal de conservação ou de retenção pelo subcontratante ao abrigo da legislação da UE ou de um Estado-Membro da UE ou a disposição em contrário relativamente à conservação e apagamento de dados pessoais, constante de um acordo explícito celebrado com o cliente. O subcontratante deve registar os apagamentos e conservar esses registos.

13. Custos a cargo do subcontratante

Todos os custos incorridos pelo subcontratante ou pelos subadjudicatários para fins de tratamento de dados em nome do cliente ao abrigo do presente acordo, especialmente aqueles que decorram

13.1. de uma obrigação de resposta a pedidos dos titulares dos dados relativamente a instruções do cliente, nomeadamente no sentido de corrigir, apagar ou restringir dados pessoais ou de devolver dados pessoais ao cliente e, se for o caso, de transferir dados (portabilidade), ou de prestar ajuda nessas atividades,

13.2. de uma obrigação de ajuda na avaliação do impacto na proteção dos dados,

13.3. do cumprimento ou aplicação de instruções do cliente,

13.4. da obrigação de prestar ajuda no cumprimento de pedidos de fornecimento de informações à autoridade de controlo ou a titulares dos dados,

13.5. da realização de uma autoavaliação idónea,

13.6. de inspeções in situ por parte do cliente ou de auditores (externos) requeridas pelo cliente, a menos que a inspeção em questão tenha detetado deficiências graves; o ónus da prova cabe, neste caso, ao cliente,

13.7. de custos adicionais relativos a medidas técnicas e organizativas para garantia da segurança do tratamento, caso as referidas medidas sejam aplicadas devido a diferenças nas análises de risco das partes,

13.8. do cumprimento de obrigações de devolução ou apagamento de dados pessoais,

devem ser reembolsados ao subcontratante com base nas tarifas horárias do mercado. O subcontratante deve conservar um registo de todos os custos e despesas incorridos.

14. Emendas ao presente acordo

Se, por força da lei, o subcontratante for obrigado a introduzir alterações e emendas, o cliente é obrigado a apoiá-las e a aprová-las.

15. Responsabilidade

15.1. Caso um titular de dados e/ou terceiro intentar uma ação contra o subcontratante relativamente a atividades de tratamento de dados lavadas a cabo pelo subcontratante em nome do cliente, o cliente é obrigado a indemnizar o subcontratante e a assumir os custos legais, danos e/ou sanções administrativas e multas de direito penal.

15.2. A disposição supra não se aplica no caso de o subcontratante estar em situação de incumprimento das obrigações que lhe são impostas por força do Regulamento Geral de Proteção de Dados ou de instruções legitimamente emitidas pelo cliente ou ter atuado em sentido contrário a essas instruções.

15.3. Os limites de responsabilidade acordados entre o cliente e o subcontratante a favor do subcontratante aplicam-se igualmente à responsabilidade do subcontratante pelas atividades de tratamento de dados ao abrigo do presente acordo.

Linde Material Handling

Anexo

I. Categorias de titulares de dados

- Clientes
- Outros: distribuidores, parceiros de rede

II. Tipos de dados

- Dados mestre do pessoal
- Dados mestre de comunicação
- Histórico do cliente

III. Âmbito do tratamento

Os principais requisitos do cliente são os seguintes:
Criação e processamento de notificações e ordens de serviço

IV. Local onde os dados pessoais devem ser tratados

EEE

V. Sistema(s) de tratamento, nomeadamente de importação e exportação de dados pessoais de outros sistemas

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP e outros sistemas ERP dos nossos distribuidores,
OneSignal Mobile Push Notifications

VI. Medidas técnicas e organizativas de segurança do subcontratante

Aplicação das medidas técnicas e organizativas

a. Confidencialidade (artigo 32.º, n.º 1, do RGPD)

(1) Controlo do acesso (instalações)

- Alarme
- Controlo automático do acesso
- Fechaduras de segurança
- Videovigilância nas entradas
- Controlo de chaves/lista
- Receção/porteiro
- Lista de visitantes
- Identificação de funcionários/visitantes
- Visitantes acompanhados por funcionários

(2) Controlo do acesso (sistemas)

- Login / utilizador + palavra-passe
- Software antivírus do servidor
- Software antivírus dos clientes
- Firewall
- Sistemas de deteção de intrusão
- Gestão de dispositivos móveis
- Utilização da rede VPN para acesso remoto
- Cifragem da conservação de dados
- Cifragem de smartphones
- Proteção da BIOS (palavra-passe própria)

(3) Controlo do acesso (dados)

- Administração dos direitos do utilizador
- Criação de perfis de utilizador
- Guia de «palavras-passe seguras»
- Guia de «apagamento / destruição»
- Guia geral de proteção dos dados e/ou segurança dos dados
- Manual de «bloqueio manual do ambiente de trabalho»
- Treino frequente dos funcionários
- Utilização do regime de autorizações
- Administração dos direitos do utilizador pelos administradores

(4) Controlo da separação

Separação dos ambientes de produção e de ensaio

(5) Pseudonimização (artigo 32.º, n.º 1, do RGPD; artigo 25.º, n.º 1, do RGPD)

n/a

b. Disponibilidade e resiliência (artigo 32.º, n.º 1, do RGPD)

- Detetores de incêndio e de fumo
- Extintores de incêndio na sala do servidor
- Controlo da temperatura e da humidade na sala do servidor
- Ar-condicionado na sala do servidor
- Sistema UPS
- Barra de tomadas de segurança utilizada na sala do servidor
- Sistema RAID / imagem do HD
- Videovigilância na sala do servidor
- Sinal de alarme em caso de acesso não autorizado à sala do servidor
- Sistema de backup e recuperação (formulado)
- Controlo do backup
- Sem equipamento sanitário na sala do servidor nem por cima da mesma
- Existência de um plano de emergência (iE BSI IT-Grundschutz 100-4)
- Partições separadas para os sistemas operativos e para os dados

c. Integridade (artigo 32.º, n.º 1, do RGPD)

- Os dados pessoais só podem ser modificados por um administrador
- Fornecimento de ligações cifradas, como sftp ou http
- Registo do acesso e recuperação
- Supervisão dos processos regulares de recuperação e transferência
- Seleção criteriosa do pessoal

d. Processo para testar, apreciar e avaliar regularmente (artigo 32.º, n.º 1, do RGPD; artigo 25.º, n.º 1, do RGPD)

(1) Gestão da proteção de dados

- Certificação da segurança nos termos da ISO 27001
- Eficiência das medidas técnicas de segurança verificada, pelo menos, uma vez por ano
- Funcionários treinados e obrigados a manter a confidencialidade

(2) Gestão da resposta a incidentes

- Utilização e atualização frequente de uma firewall
- Utilização e atualização frequente de filtros de spam
- Utilização e atualização frequente de um verificador de vírus
- Sistema de deteção de intrusão (SDI)
- Sistema de prevenção de intrusão (SPI)

Proteção de dados por defeito (artigo 25.º, n.º 2, do RGPD)

- A quantidade de dados pessoais deve ser limitada ao necessário para as finalidades do respetivo tratamento.

Linde Material Handling

Personuppgiftsbiträdesavtal (”Avtal”) gällande Linde Service Manager

Detta Avtal avser de allmänna villkoren för Linde Service Manager (”Allmänna villkor”). Termer med inledande versal som inte definieras här ska ha den betydelse som anges i Allmänna villkor.

Distributören (”**Klient**” eller “**Personuppgiftsansvarig**”), som representeras av användaren, och LMH (“**Personuppgiftsbiträde**”, tillsammans med personuppgiftsansvarig ”**Parterna**”) ingår detta avtal för behandling av personuppgifter med avseende på tjänsten. Avtalet styr Parternas dataskyddsförpliktelser med avseende på skydd av Klientens personuppgifter.

1. Definitioner

I detta Avtal har följande termer nedanstående betydelse:

1.1. ”**Personuppgiftsbiträde**”: En fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ som behandlar personuppgifter för Personuppgiftsansvariga.

1.2. ”**Tredje part**”: En fysisk eller juridisk person, offentlig myndighet, byrå eller organ, som inte är den registrerade, personuppgiftsansvariga, personuppgiftsbiträde och personer som med direkt fullmakt från personuppgiftsansvariga eller personuppgiftsbiträde, har befogenhet att behandla personuppgifter.

1.3. ”**Personuppgifter**”: All information gällande en identifierad eller identifierbar fysisk person (”**Registrerad**”). En identifierbar fysisk person är en person som kan identifieras, direkt eller indirekt, i synnerhet genom referens till en identifierare, däribland ett namn, ett id-nummer, platsdata, en webbidentifierare eller genom en eller fler faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identitet.

1.4. ”**Pseudonymisering**”: Behandling av personuppgifter på ett sådant sätt att personuppgifterna inte längre kan hänföras till en specifik Registrerad utan ytterligare information, förutsatt att sådan ytterligare information hålls separat och omfattas av tekniska och organisatoriska åtgärder som säkerställer att personuppgifter inte kan hänföras till en identifierad eller identifierbar fysisk person.

1.5. ”**Personuppgiftsansvarig**”: En fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ som ensamt eller tillsammans med andra fastställer syftet och innebörden i personuppgiftsbehandlingen. ///Om detta fastställs i EU- eller medlemsstatslagstiftning kan utnämnandet ske antingen av Personuppgiftsansvariga eller genom specifika kriterier för utnämnande i EU- eller medlemsstatslagstiftning.

1.6. ”**Behandling**”: All behandling av personuppgifter, oavsett om denna sker automatiskt eller inte, däribland insamling, registrering, organisering, strukturering, lagring, anpassning eller ändring, hämtning, konsultation, användning, utlämnande genom överföring, spridning eller annat tillgängliggörande, samordning eller sammanslagning, begränsning, radering eller förstörelse.

1.7. ”**Personuppgiftsincident**”: En säkerhetsincident som leder till en oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt utlämnande av eller åtkomst till personuppgifter som överförts, lagrats eller behandlats på annat sätt.

1.8. ”**Huvudavtal**”: Det avtal som ingås mellan LMH och distributören med avseende på Tjänsterna, så som beskrivs i Allmänna villkor.

2. Avtalets ämne och löptid

2.1. Avtalet reglerna Personuppgiftsbiträdets skyldigheter när det gäller de Personuppgifter som tillhörande Klienten, och som behandlas av Personuppgiftsbiträdet för Klienten.

2.2. Bestämmelserna i Avtalet gäller inte om Personuppgiftsbiträdet, i enlighet med uppdraget, inte ska utföra behandlingsaktiviteter avseende Klientens personuppgifter. I så fall ska Klienten se till att Personuppgifterna är skyddade från Personuppgiftsbiträdet.

2.3. Det är endast Klienten som har rätt att bedöma om Behandlingen är laglig och att Registrerades rättigheter är skyddade.

2.4. Avtalet träder i kraft när Huvudavtalet träder i kraft och upphör samtidigt som Huvudavtalet. Om Personuppgiftsbiträdet fortsätter att behandla Personuppgifterna enligt Klientens instruktioner efter det att Huvudavtalet upphört ska Avtalet gälla till dess att Behandling som utförs enligt Klientens instruktioner upphört.

2.5. Oaktat bestämmelsen i 2.4 kan Parterna säga upp Avtalet på saklig grund. Om orsaken är ett brott mot en skyldighet enligt Avtalet är uppsägning endast tillåtet efter det att den period som angetts för att rätta till brottet har löpt ut utan att rättelse skett eller en varning inte gett något resultat. Exempel på saklig grund för Personuppgiftsbiträdet:

2.5.1. Klienten utfärdar olagliga instruktioner upprepade gånger, och Personuppgiftsbiträdet har informerat Klienten om detta utan dröjsmål, men Klienten har inte återkallat instruktionerna.

2.5.2. Klienten har brutit mot bestämmelserna i Avtalet.

2.5.3. Klienten har invänt mot anlitande av en underentreprenör enligt Avtalet.

Dessutom ska villkoren i Huvudavtalet gälla mutatis mutandis med Avtalet.

3. Behandlingens beskaffenhet, omfattning och plats

3.1. Personuppgiftsbiträdet är godkänd för åtkomst till Klientens Personuppgifter i syfte att tillhandahålla tjänsterna enligt Huvudavtalet, så som beskrivs i bilaga 1. Bestämmelserna i Avtalet utökar inte Personuppgiftsbiträdets skyldigheter, utan beskriver dem mer detaljerat. Avtalet styr också Klientens skyldigheter.

3.2. Klienten kan utfärda instruktioner som specificerar Personuppgiftsbiträdets skyldigheter ännu mer detaljerat.

3.3. Personuppgiftsbiträdet får inte använda Personuppgifterna för andra skäl än de som beskrivs i Huvudavtalet och detta Avtal, och får i synnerhet inte, utan Klientens uttryckliga instruktioner, överföra Personuppgifter till en tredje part eller lämna ut dem till andra mottagare, om inte detta anges i Avtalet.

3.4. Behandling enligt Avtalet begränsas till EU och EES, om inte annat anges i bilagorna i Avtalet.

4. Klientens instruktioner, Registrerades rättigheter, konsekvensbedömning avseende dataskydd

4.1. Klienten kan genom sina instruktioner specificera eller uppdatera beskaffenheten hos, omfattningen av och metoden för databehandling, säkerhetsåtgärder, Personuppgifter som ska behandlas och grupper av Registrerade. Detta gäller främst i de fall då en tillsynsmyndighet eller förändringar i lagstiftningen orsakat eller kräver att Klienten utfärdar instruktioner. Om en Registrerad kontaktar Personuppgiftsbiträdet direkt ska denna kontakta Klienten omedelbart och be om vidare instruktioner.

4.2. Om Klienten genomför en konsekvensbedömning avseende dataskydd ska Personuppgiftsbiträdet i den mån det är möjligt och nödvändigt följa instruktionerna, däribland gällande förhandskonsultation med behörig tillsynsmyndighet.

4.3. Klientens instruktioner begränsas till implementering av kraven i dataskyddslagstiftningen. Dessa ska hållas åtskilda från ändringsbegäranden. Med ändringsbegäranden avses ändringar i tjänsteomfattningen som inte krävs enligt lagstiftning eller som överstiger de åtgärder som krävs för att implementera sådana krav. De utgör inte instruktioner enligt detta Avtal, utan betraktas som begäranden från Klienten att ändra tjänsterna. Personuppgiftsbiträdet har rätt, men är inte tvungen att implementera sådana ändringsbegäranden. Ändringsbegäranden debiteras separat.

4.4. Klientens instruktioner ska vara skriftliga och skickas via fax eller e-post. Klienten ska utan dröjsmål bekräfta eventuella muntliga instruktioner (i undantagsfall) skriftligen.

4.5. Personuppgiftsbiträdet ska utan dröjsmål skriftligen informera Klienten om Personuppgiftsbiträdet anser att Klientens instruktion bryter mot dataskyddsbestämmelserna eller på annat väsentligt sätt är felaktig, ofullständig, motsägelsefull eller juridiskt eller tekniskt ogenomförbar. Personuppgiftsbiträdet ska fråga Klienten om instruktionen ska följas eller om Behandlingen ska fortsätta som tidigare, fram till dess att Klienten hunnit granskat informationen och komma fram till en slutsats.

5. Personuppgiftsbiträdets skyldighet att tillhandahålla information

5.1. Vid en Personuppgiftsincident kan Klienten ha en skyldighet att rapportera detta. Personuppgiftsbiträdet ska informera Klienten vid misstanke eller kännedom om ett väsentligt brott mot skyddet av Klientens Personuppgifter begåtts av Personuppgiftsbiträdet eller personer under Personupppgiftsbiträdets kontroll.

5.2. Klienten kan kräva att Personuppgiftsbiträdet vidtar alla rimliga och nödvändiga åtgärder för att hjälpa Klienten att uppfylla rapporteringskraven.

6. Klientens skyldigheter

6.1. Klienten ska utan dröjsmål informera Personuppgiftsbiträdet om det framkommer fel eller oegentligheter vid kontroll av resultatet av den utförda tjänsten.

6.2. Klienten måste själv kontrollera, både innan databehandlingen inleds och därefter, att de tekniska och organisatoriska åtgärder som införts hos Personuppgiftsbiträdet följs. Resultatet av sådana kontroller måste dokumenteras.

6.3. Klienten är ansvarig för efterlevnad av skyldigheterna enligt artikel 33 och 34 i GDPR gentemot tillsynsmyndigheten eller en Registrerad som påverkas av sådan Personuppgiftsincident.

6.4. Klienten ska informera Personuppgiftsbiträdet om kraven för radering och lagring av Personuppgifter, samt för implementering av dessa krav.

7. Dataskyddsombud

7.1. Personuppgiftsbiträdet har utsett ett dataskyddsombud (DSO). Kontaktuppgifter enligt följande: datenschutz@kiongroup.com. Personuppgiftsbiträdet ska meddela Klienten om eventuella ändringar eller förestående ändringar.

7.2. För det fall Klienten är skyldig att utse ett DSO (vilket inte alltid är fallet) ska namnet på denna lämnas till Personuppgiftsbiträdet. Klienten ska meddela Personuppgiftsbiträdet om eventuella ändringar eller förestående ändringar, utan uppmaning från Personuppgiftsbiträdet.

7.3. Om Klienten måste utse en företrädare i enlighet med artikel 27 i GDPR ska Klienten meddela Personuppgiftsbiträdet namnet på denna. Klienten ska meddela Personuppgiftsbiträdet om eventuella ändringar eller förestående ändringar, utan uppmaning från Personuppgiftsbiträdet.

8. Personer som lyder under Personuppgiftsbiträdets kontroll

8.1. För att utföra databehandlingen enligt Avtalets villkor ska Personuppgiftsbiträdet utse endast personer som har ett dokumenterat sekretessåtagande och som i förväg känner till de dataskyddsbestämmelser som är relevanta för dem och för behandlingsaktiviteterna som ska utföras för Klienten.

8.2. Personuppgiftsbiträdet ska se till att alla personer under dess kontroll som har åtkomst till Klientens Personuppgifter endast behandlar dessa inom omfattningen för och i enlighet med Klientens instruktioner och Avtalsbestämmelserna. Enda undantaget till ovanstående bestämmelse rör enskilda fall av behandlingsaktiviteter, i synnerhet dataöverföring, som Personuppgiftsbiträdet eller personer som lyder under dess kontroll är skyldiga att utföra enligt beslut av en domstol eller myndighet som grundar sig på lagstiftning. I den utsträckning som är tillåtet i lag ska Personuppgiftsbiträdet informera Klienten om sådana beslut, helst innan Personuppgifterna överförs.

9. Säkra behandlingsprinciper

9.1. Med hänsyn till den tillgängliga tekniken, implementeringskostnader och beskaffenheten, omfattningen, omständigheterna och syftena med Personuppgiftsbehandlingen som Klienten begär, samt sannolikheten och allvarsgraden hos risken för enskildas rättigheter och friheter (riskanalys) ska Personuppgiftsbiträdet införa de tekniska och organisatoriska åtgärder som krävs för att säkerställa att Personuppgifterna är skyddade.

9.2. Vid bedömning av den lämpliga säkerhetsnivån ska Personuppgiftsbiträdet ta hänsyn till de inneboende riskerna med behandling av Klientens Personuppgifter, däribland men inte begränsat till risken för oavsiktlig eller olaglig förstörelse, och förlust, ändring, eller obehörigt utlämnande av eller obehörig åtkomst till Klientens Personuppgifter.

9.3. Personuppgiftsbiträdet ska uppdatera och justera de tekniska och organisatoriska åtgärderna i sin säkerhetsplan i enlighet med ändringar i den tillgängliga tekniken. Dock får sådana åtgärder inte underskrida den säkerhets- och skyddsnivå som anges i detta Avtal.

9.4. Personuppgiftsbiträdet ska i detalj dokumentera de tekniska och organisatoriska åtgärderna i samband med Avtalet i tillhörande bilaga. Personuppgiftsbiträdet måste hålla dokumentationen uppdaterad och dokumentera alla väsentliga ändringar.

9.5. De tekniska och organisatoriska åtgärderna i bilagan till Avtalet bedöms vara godkända och nödvändiga när kontraktet tecknas. De representerar alla krav som Personuppgiftsbiträdet måste uppfylla.

9.6. Klienten är skyldig att granska de tekniska och organisatoriska åtgärderna baserat på sin egen riskanalys. Klienten är ansvarig för att säkerställa att de tekniska och organisatoriska åtgärderna erbjuder en nivå av dataskydd som överensstämmer med riskerna för de Personuppgifter som ska behandlas. Om Klientens riskanalys ger ett resultat som avviker från Personuppgiftsbiträdets riskanalys har Klienten rätt att förhandla med Personuppgiftsbiträdet om justeringar av säkerhetsåtgärderna. Om Parterna inte kan nå en överenskommelse har de var och en rätt att säga upp Avtalet med 14 dagars varsel.

10. Kontroller

10.1. Klienten har rätt att kontrollera Personuppgiftsbiträdets utförande av tjänsterna med avseende på Klientens Personuppgifter och efterlevnaden av bestämmelserna i Avtalet, däribland men inte begränsat till de tekniska och organisatoriska åtgärderna för att säkerställa behandlingssäkerhet.

10.2. På begäran ska Personuppgiftsbiträdet tillhandahålla Klienten bevis för att de tekniska och organisatoriska säkerhetsåtgärderna har implementerats. Exempel:

- bevis för efterlevnad av godkända uppförandekoder enligt artikel 40 i GDPR
- Intyg i enlighet med ett godkänt certifieringsförfarande enligt artikel 42 i GDPR
- en kvalificerad skriftlig bedömning från en oberoende tredje part (däribland DSO, revisor, externa dataskydds-/säkerhetsrevisorer) eller
- lämplig certifiering genom en IT-säkerhets- eller dataskyddsrevision (t.ex. ISO 27001).

Sådana bevis måste innehålla all nödvändig information för att bevisa efterlevnad och implementering av skyldigheterna enligt Avtalet och relevanta tekniska och organisatoriska åtgärder som är avsedda att garantera behandlingssäkerheten. Klienten kan begära denna information en gång per kalenderår och med kortare intervall endast i händelse av en berättigad misstanke om att Personuppgiftsbiträdet brutit mot Avtalet, vilket Klienten måste informera Personuppgiftsbiträdet om skriftligen.

10.3. Klienten har rätt att kontrollera efterlevnad av Avtalet, i synnerhet efterlevnad av behandlingssäkerheten, genom att utföra förannonserade inspektioner i Personuppgiftsbiträdets lokaler under ordinarie arbetstid (9–18) en gång vart tredje år, eller låta sådana kontroller utföras av en extern revisor som omfattas av tystnadsplikt. Klienten måste lämna två veckors skriftlig varsel före sådan inspektion. Detta gäller dock inte i akuta fall (t.ex. om det finns misstanke om att Personuppgiftsbiträdet brutit mot Avtalet i ett mer väsentligt avseende). Klienten måste i sådana fall meddela Personuppgiftsbiträdet skriftligen i förväg.

11. Underentreprenör

11.1. Om Personuppgiftsbiträdet enligt överenskommelse med Klienten har rätt att anlita underentreprenörer för behandlingen och det inte kan uteslutas att dessa underentreprenörer kommer att ha åtkomst till Klientens Personuppgifter får Personuppgiftsbiträdet endast anlita underentreprenörer, och därigenom möjliggöra för åtkomst till Klientens Personuppgifter, om

Klienten informerats skriftligen om uppgifterna i nästa stycke. Klienten ska ha fått möjlighet att invända, men inte gjort det inom den föreskrivna tiden.

11.2. Informationen som ska tillhandahållas av Personuppgiftsbiträdet enligt ovan måste minst innehålla följande:

11.2.1. Underentreprenörens identitet

11.2.2. De specifika tjänster som underentreprenören ska tillhandahålla Personuppgiftsbiträdet

11.2.3. Den erfarenhet, kapacitet, pålitlighet samt de IT-säkerhets- och dataskyddsåtgärder som krävs för att efterleva dataskyddsförpliktelserna i Avtalet

11.2.4. Underentreprenörens garantier eller försäkring om att man kommer att efterleva bestämmelserna i Avtalet.

11.3. Klienten har rätt att inom sju dagar efter att ha fått ovanstående information invända skriftligen mot anlitandet av underentreprenör, förutsatt att det finns ett berättigat skäl att göra det. Om Klienten invänder är Personuppgiftsbiträdet skyldig att genomföra Avtalet, utföra tjänsterna och fullgöra skyldigheterna utan underentreprenören, men har samtidigt rätt att säga upp Avtalet.

11.4. Om en underentreprenör får åtkomst till Klientens Personuppgifter är Personuppgiftsbiträdet skyldig att ingå ett Personuppgiftsbiträdesavtal med underentreprenören som innebär att denna ska ha samma skyldigheter som anges i Avtalet. Sådant avtal ska upprättas innan underentreprenören får åtkomst till Klientens Personuppgifter för första gången.

12. Retur och radering

12.1. Personuppgiftsbiträdet är skyldigt att när Avtalet löpt ut, eller tidigare om Klienten så begär, returnera eller lämna över alla Personuppgifter tillhörande Klienten.

12.2. I bilagan till Avtalet kan detaljer om radering av uppgifter läggas till, i förekommande fall efter Klientens instruktioner. Personuppgiftsbiträdet behöver inte ha en egen plan för radering. Personuppgiftsbiträdet är skyldigt att utan dröjsmål efter Avtalet har löpt ut, eller tidigare om Klienten så begär, radera alla Personuppgifter som inte måste lagras eller behållas av Personuppgiftsbiträdet enligt EU-lagstiftning eller lagstiftning i medlemsstaten i fråga, eller ett uttryckligt avtal med Klienten som anger det motsatta och som styr lagring eller radering av Personuppgifter. Personuppgiftsbiträdet ska föra register över raderade uppgifter.

13. Kostnader som ska bäras av Personuppgiftsbiträdet

Alla kostnader som uppkommer för Personuppgiftsbiträdet eller underentreprenörer genom behandling av Personuppgifter för Klienten enligt villkoren i Avtalet, i synnerhet sådana som uppkommit på grund av

13.1. en skyldighet att tillmötesgå Registrerades begäranden för Klientens räkning, i synnerhet att rätta, radera eller begränsa Personuppgifter eller lämna tillbaka Personuppgifter till Klienten, samt i förekommande fall överföra uppgifter (portabilitet) eller bistå med sådana åtgärder

13.2. en skyldighet att bistå med konsekvensbedömning avseende dataskydd

13.3. efterlevnad av eller implementering av Klientens instruktioner

13.4. skyldigheten att bistå med fullgörande av kraven att lämna upplysningar till tillsynsmyndighet eller till Registrerade

13.5. utarbetande av en kvalificerad egenbedömning

13.6. inspektioner av Klienten eller (externa) revisorer som Klienten kräver, om inte sådan inspektion identifierat väsentliga brister, som dock måste bevisas av Klienten,

13.7. ytterligare kostnader för tekniska och organisatoriska åtgärder för att garantera behandlingssäkerheten, om sådana åtgärder införs som ett resultat av Parternas olika riskanalyser

13.8. efterlevnad av skyldigheter att returnera eller radera Personuppgifter

kommer att ersättas Personuppgiftsbiträdet enligt normal timtaxa. Personuppgiftsbiträdet ska dokumentera alla kostnader och utgifter.

14. Tillägg till Avtalet

Om Personuppgiftsbiträdet enligt lag är skyldigt att implementera ändringar och tillägg ska Klienten stötta och godkänna dem.

15. Ansvar

15.1. Om en Registrerad och/eller tredje part väcker talan mot Personuppgiftsbiträdet i samband med behandlingsaktiviteter som utförs av Personuppgiftsbiträdet för Klienten är Klienten skyldig att hålla Personuppgiftsbiträdet skadeslöst och betala tillhörande rättsliga kostnader, skadestånd och/eller böter som beslutas av en domstol.

15.2. Ovanstående bestämmelse gäller inte om Personuppgiftsbiträdet inte fullgjort sina skyldigheter enligt GDPR eller inte efterlevt lagenliga instruktioner som utfärdats av Klienten eller agerat i strid med sådana instruktioner.

15.3. Ansvarsbegränsningar som överenskommits mellan Klienten och Personuppgiftsbiträdet till förmån för Personuppgiftsbiträdet i Huvudavtalet gäller även för Personuppgiftsbiträdets behandlingsaktiviteter enligt Avtalet.

Linde Material Handling

Bilaga

I. Kategorier av registrerade

- Kunder
- Övriga: distributörer, nätverkspartner

II. Typer av uppgifter

- Masterdata personal
- Masterdata kommunikation
- Kundhistorik

III. Behandlingsomfattning

Klientens kärnkrav enligt följande:
Skapa och behandla tjänsteaviseringar och order

IV. Platsen där personuppgifterna behandlas

EES

V. Behandlingssystem, däribland import och export av personuppgifter från andra system

Linde Global Extranet, SAP Netweaver Gateway, SAP ERP och andra ERP-system tillhörande våra distributörer,
OneSignal Mobile Push Notifications

VI. Personuppgiftsbiträdets tekniska och organisatoriska säkerhetsåtgärder

Implementering av tekniska och organisatoriska åtgärder

a. Konfidentialitet (artikel 32.1 GDPR)

(1) Tillträdeskontroll (lokaler)

- Larm
- Automatisk tillträdeskontroll
- Säkerhetslås
- Videoövervakning av entréer
- Nyckelkontroll/lista
- Reception/vakt
- Besökslista
- Medarbetar-/besöks-id
- Besökare i medarbetares sällskap

(2) Åtkomstkontroll (system)

- Inloggning med användarnamn + lösenord
- Antivirusprogram server
- Antivirusprogram klienter
- Brandvägg
- Intrångsdetekteringssystem
- Hantering av mobilenheter
- Användning av VPN för fjärråtkomst
- Kryptering av datalagring
- Kryptering av smarttelefoner
- BIOS-skydd (separat lösenord)

(3) Åtkomstkontroll (data)

- Administration av användarrättigheter
- Skapande av användarprofiler
- Riktlinjer för säkra lösenord
- Riktlinjer för radering/förstörelse
- Allmänna riktlinjer för dataskydd och/eller datasäkerhet
- Manual för manuellt skrivbordlås
- Frekvent medarbetarutbildning
- Användning av behörighetsplaner
- Användarrättigheter administreras av administratörer

(4) Separeringskontroll

Separation av produktions- och testmiljöer

(5) Pseudonymisering (artikel 32.1 GDPR, artikel 25.1 GDPR)

n/a

b. Tillgänglighet och motståndskraft (artikel 32.1 GDPR)

- Brand- och rökdetektorer
- Brandsläckare i serverrum
- Kontroll av temperatur och fuktighet i serverrum
- Luftkonditionering i serverrum
- UPS-system
- Säkerhetsströmuttag används i serverrum
- RAID-system/spegling av HD
- Videoövervakning serverrum
- Larmsignal för obehörigt tillträde till serverrum
- Backup- och återställningsplan (skriftlig)
- Kontroll av backup
- Ingen sanitetsutrustning i eller över serverrum
- Nödplan (iE BSI IT-Grundschutz 100-4)
- Separata partitioner för operativsystem och data

c. Integritet (artikel 32.1.b GDPR)

- Personuppgifter kan endast ändras av administratör
- Tillgång till krypterade anslutningar, t.ex. sftp, https
- Loggning av åtkomst och hämtning
- Översikt över ordinarie processer för hämtning och överföring
- Noggrant utvald personal

d. Process för regelbunden testning, bedömning och utvärdering (artikel 32.1 GDPR, artikel 25.1 GDPR)

(1) Dataskyddshantering

- Säkerhetscertifiering enligt ISO 27001
- Effektiviteten i de tekniska säkerhetsåtgärderna revideras minst en gång per år
- Medarbetare får utbildning i och är skyldiga att upprätthålla konfidentialiteten

(2) Incidenthantering

- Användning av brandvägg och regelbundna uppdateringar
- Användning av spamfilter och regelbundna uppdateringar
- Användning av virusskanner och regelbundna uppdateringar
- Intrångsdetekteringssystem (IDS)
- Intrångspreventionssystem (IPS)

Dataskydd som standard (artikel 25.2 GDPR)

- Mängden personuppgifter begränsas till det som krävs för det syfte för vilket de behandlas.