Agreement on order data processing (Maintenance and Audit according to §11 para. 5 BDSG) – August 2015

1 SUBJECT MATTER AND TERM OF THE ORDER
The subject matter and duration of the contract arise from the other documents (main contract or offer and order).
2 SPECIFICATION OF THE CONTENTS OF THE ORDER
2.1 The Supplier shall be granted access to automated processes or data processing facilities within the meaning of § 11.5 of the German Federal Data Protection Act (BDSG) during the implementation of the order. In that context, access to personal data cannot be excluded.
2.2 The Supplier may have access to the following types and categories of data: Personal master data, communication data (e.g. telephone, e-mail), master contract data (con-tractual relationship, product or contractual interests), customer history, contract in-voicing and payment data, planning and control data, and information entries (from third parties, e.g. information offices or from public directories). In principle, other types of data may be added.
2.3 The set of people whose personal data is processed under this order consists of customers, prospective customers, and employees within the meaning of § 3 para. 11 of the German Federal Data Protection Act (BDSG) and the contact persons of suppliers and business partners.
2.4 The data shall be processed and used exclusively in the territory of the Federal Republic of Germany or in another EU member state or EEA member state. Any outsourcing to a country other than those specified in the foregoing sentence is subject to the Customer's prior consent and permissible only if the special prerequisites
of §§ 4b, 4c of the German Federal Data Protection Act (BDSG) are satisfied.
3 TECHNICAL/ORGANISATIONAL MEASURES
3.1 In the course of implementing the order, the Supplier shall use exclusively the Customer's automated processes (IT systems, data storage media) except those mentioned in 3.4.
3.2 The Customer is therefore responsible for the technical and organisational measures for those automated processes. The Supplier hereby undertakes to comply with said measures.
3.3 Insofar as the Supplier also uses a computer made available by Knorr-Bremse outside the premises of Knorr-Bremse and personal data is contained therein, the Supplier shall ensure that unauthorised parties are prevented from approaching said computer (physical access control) either through personnel monitoring or by safekeeping in a cabinet/room under lock and key whenever unattended.
3.4 Insofar as the Supplier also uses its own workstation in the course of implementing the order (e.g. by remote access to the Customer's systems or to store documents) or a file server (e.g. to store documents), the Supplier shall ensure that the technical and organisational measures stipulated in § 9 of the German Federal Data Protection Act (BDSG) and its Annex are implemented for said IT system. The foregoing means, in particular, that:
3.4.1 Unauthorised parties are prevented from approaching said IT systems (physical access control), i.e. for workstations either through personnel monitoring or by safekeeping in a cabinet/room under lock and key whenever unattended.
3.4.2 Through authentication (e.g. user name/password) to ensure that the IT systems cannot be used by unauthorised parties (admission control)
3.4.3 Only the Customer's authorised employees can access the data stored on said IT systems in the course of performing the order (access control)
3.4.4 Personal data, when communicated, shall be transmitted electronically encrypted or an encrypted data storage medium shall be used (communication control)
3.4.5 Personal data shall be protected against inadvertent destruction or loss (availability control), in particular by means of functioning anti-virus and patch management services on the IT systems.
3.4.6 Appropriate access control shall ensure that the collected data can be processed separately for different purposes (separation requirement)
3.5 The technical and organisational measures shall be adapted to the state of the art and further developments. To that extent, it is permissible for the Supplier to implement suitable alternative measures, provided that they do not fall below the security level of the specified measures. Substantial changes shall be documented. On request, the Supplier shall provide the Customer with information in accordance with § 4g para. 2 no. 1 of the German Federal Data Protection Act (BDSG).
4 DATA CORRECTION, BLOCKING AND DELETION
The Supplier shall not correct, delete or block the data processed in the order unless so instructed by the Customer. Whenever a data subject directly asks the Supplier to correct or delete the data subject's personal data, the Supplier shall inform the Customer of that request without delay.
5 AUDITS AND OTHER OBLIGATIONS OF THE SUPPLIER
In addition to complying with the provisions of this order, the Supplier is subject to the following obligations under § 11 para. 4 of the German Federal Data Protection Act (BDSG):

- Written appointment – to the extent prescribed by law – of a data protection officer ("Datenschutzbeauftragter") capable of exercising his activities in accordance with §§ 4f, 4g of the German Federal Data Protection Act (BDSG). The Customer shall be informed of the contact data of said data protection officer for the purpose of entering into contact directly.
- Maintaining data secrecy in accordance with § 5 of the German Federal Data Pro-tection Act (BDSG). All persons who may access the personal data assigned by the Customer in accordance with the order shall be required to maintain data secrecy and, in addition, be instructed of any order-specific data protection obligations and instructions or dedication to a specific purpose.
- Implementing and complying with all the technical and organisational measures necessary for this order in accordance with § 9 of the German Federal Data Protec-tion Act (BDSG) and the corresponding Annex.
- Promptly informing the Customer of any audits or measures by the supervisory authorities in accordance with § 38 of the German Federal Data Protection Act (BDSG). The foregoing shall also apply whenever a relevant authority audits the Supplier in accordance with §§ 43, 44 of the German Federal Data Protection Act (BDSG).
- Implementation of order monitoring by means of regular inspections by the Customer with respect to the implementation/performance of the contract, particularly compliance with or any necessary adjustments of the provisions and measures for implementation of the order.
- Ability to provide the Customer with proof of all the technical and organisational measures taken. To that purpose, the Supplier may present current attestations, re-ports or excepts from reports by independent entities (e.g. chartered accountants, auditors, data protection officer, IT security department, data protection auditors, quality auditors) or appropriate certification from an IT security or data protection audit (e.g. according to the basic protection standards of the BSI (German Federal IT Security Authority)).

6 SUBCONTRACTING
6.1 Subcontractors may be called upon to process or use the personal data confided by the Customer provided that the following requirements are satisfied:

- Use of subcontractors is generally permissible only with the Customer's written approval. Subject to complying with the order monitoring obligations explained in section 5, the Supplier may utilise affiliated companies or, in certain cases, other subcontractors, with the degree of care required by law, for performance of the con-tract, without the Customer's written consent, provided that the Supplier informs the Customer thereof before the start of the processing or utilisation.
- The Supplier shall draft the contractual agreements with the subcontractor(s) in such a way as to incorporate the same data protection provisions as in the contract between the Customer and Supplier.
- In the case of subcontracting, the subcontractor shall grant the Customer the same rights of auditing and inspection as those granted in this agreement and stipulated in § 11 of the German Federal Data Protection Act (BDSG) in conjunction with section 6 of the Annex to § 9 BDSG. The foregoing shall include the Customer's right to obtain from the Supplier, if so requested in writing, information about the basic contractual content and implementation of the data protection obligations in the contractual relationship between the Supplier and the sub-suppliers thereof, if necessary through inspection of the relevant contract documents.

6.2 Services that the Supplier procures from third parties as an ancillary service to assist with order execution shall not be considered subcontracting for the purposes of this provision. Such ancillary services include, for example, services of telecommunication, maintenance and user support, cleaning, auditing or data storage medium disposal. Even if cases of outsourced ancillary services, however, it is the obligation of the Sup-plier to ensure the protection and security of the data entrusted by the Customer, to enter into appropriate contractual agreements as required by law and to implement auditing and inspection measures.
7 CUSTOMER'S MONITORING AND AUDITING RIGHTS
7.1 The Customer has the right to monitor orders as stipulated by section 6 of the Annex to § 9 of the German Federal Data Protection Act (BDSG), in agreement with the Supplier or, in certain cases, by means of designated auditors. The Customer is entitled to check for compliance with this agreement in the Supplier's business operations by means of spot checks, subject to giving sufficient advance notice. The Supplier hereby agrees to provide the Customer, upon request, with such information as is required to ensure proper performance of its order-monitoring obligations, accompanied by the corresponding proof thereof.
7.2 Regarding the Customer's auditing and inspection obligations under § 11 para. 2 no. 4 of the German Federal Data Protection Act (BDSG), before the start of the data processing and throughout the effective

period of the order, the Supplier shall ensure that the Customer is able to verify the technical and organisational measures implemented. To that purpose, the Supplier shall demonstrate to the Customer, upon request, the implementation of the technical and organisational measures according to § 9 of the German Federal Data Protection Act (BDSG). In so doing, verification that measures have been implemented not just specifically for an individual order may be provided by presenting a current attestation, reports or excepts from reports by independent entities (e.g. chartered accountants, auditors, data protection officers, IT security department, data protection auditors, quality auditors) or appropriate certification from an IT security or data protection audit (e.g. according to the basic protection standards of the BSI (German Federal IT Security Authority)).

8 REPORTING OF THE SUPPLIER'S VIOLATIONS

8.1 In every instance, the Supplier shall inform the Customer whenever the Supplier or the persons in the Supplier's employ violate the Customer's personal data protection pro-visions or the stipulations of the order.

8.2 The parties are aware that, according to § 42a of the German Federal Data Protection Act (BDSG), it is obligatory to report any loss or unlawful disclosure of personal data or any unauthorised access thereto. Any such events, irrespective of the cause, shall therefore be reported immediately to the Customer. The foregoing also applies to any serious disruptions of business operations in case of suspicion of other violations of personal data protection provisions or other irregularities in dealing with the personal data entrusted by the Customer. The Supplier shall, in agreement with the Customer, take appropriate measures to secure the data and reduce any potential adverse effects on the data subjects. The Supplier shall assist the Customer with any obligations to which the Customer is subject under § 42a of the German Federal Data Protection Act (BDSG).

9 CUSTOMER'S AUTHORITY TO INSTRUCT

9.1 The data shall be dealt with exclusively within the limits of the signed agreements and in accordance with the Customer's instructions (see § 11 para. 3 no. 1 of the German Federal Data Protection Act (BDSG)). Within the limits of the order specification agreed to under this contract, the Customer has a comprehensive right to give instructions regarding the type, extent and method of data processing, which the Customer may further specify through individual instructions. Any changes in the subject matter or method of processing shall be coordinated between the parties and documented. The Supplier shall not give any information to third parties or to the data subjects without the Customer's prior written consent.

9.2 Verbal instruction shall be promptly confirmed by the Customer in writing or by e-mail (in text format). The Supplier shall not use the data for any other purposes and, in particular, is not authorised to disclose the data to third parties. No copies or duplicates shall be made without the Customer's knowledge. The foregoing rule shall not apply to backup copies, to the extent necessary to ensure proper data processing, or to data required for compliance with legal record-keeping obligations.

9.3 The Supplier shall inform the Customer without delay in accordance with § 11 para. 3 no. 2 of the German Federal Data Protection Act (BDSG) if it believes that an instruction represents an infringement of data protection legislation. The Supplier is entitled to refrain from carrying out the corresponding instruction pending confirmation or modification by the Customer's employees responsible for data processing.

10 DELETION OF DATA AND RESTITUTION OF DATA STORAGE MEDIA

10.1 Upon completion of the contractual work or earlier, if so requested by the Customer – at the latest upon termination of the relevant agreement – the Supplier shall hand over to the Customer all documents and results of data processing or use, as well as databases generated in connection with the order, or destroy same in accordance with the data protection provisions, with the Customer's prior consent. The foregoing also applies to any test materials or discarded materials. The record of deletion shall be presented upon request. Alternatively, data can also be blocked by the Supplier, if the requirements of §35 para. 3 of the German Federal Data Protection Act (BDSG) are met. In this case, it has to be proven on demand that the blocking was adequately implemented.

10.2 Documentation used to prove proper data processing in accordance with the order shall be retained by the Supplier after termination of the contract in accordance with the relevant record-keeping periods. The Supplier may be discharged of the foregoing obligation by handing over such documentation to the Customer upon termination of the contract.