

General Data Processing Addendum

– hereinafter referred to as the GDPR –

Annex to an existing contract – hereinafter referred to as “Agreement” - between KRONES - hereinafter referred to as “Processor” - and the CUSTOMER - hereinafter referred to as “Controller” – hereinafter referred to individually and collectively as the “Party”/”Parties”.

1. Definition of terms

For the purposes of this GDPR, the following definitions apply:

- (a) The “**Processor**” is a natural or legal person, authority, organization or other agency that processes Personal Data on behalf of the Controller;

The “Processor” means the contractual party who processes Personal Data on behalf of the Controller.

- (b) “**Third Party**” means 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.

- (c) “**Agreement**” refers to the agreement between KRONES and CUSTOMER – such as purchase order, contract, service level agreement or cooperation agreement - which this GDPR is incorporated by reference.

- (d) “**Special Conditions**” refers to an appendix to the Agreement that provides specifications and conditions of the respective services/products along with specific data processing specifications.

- (e) The “**Controller**” is the natural or legal person, authority, organization or other agency that makes decisions individually or together with other parties regarding the purposes and means for Processing Personal Data;

The “Controller” is the contractual Party referred to above as the “Controller” that bears the sole responsibility under this GDPR for making decisions regarding the purposes and means for Processing Personal Data.

- (f) “**Processing**” refers to every procedure performed with or without the aid of automated processes or any series of such procedures relating to Personal Data such as acquisition, recording, organization, filing, storage, adaptation or modification, reading out, querying, using, disclosing through communication, dissemination or any other form of provision, comparison or linking, applying restrictions, deletion or destruction;

- (g) “**Personal Data**” means any information relating to an identified or identifiable natural person (hereinafter “Data Subject”); an identifiable 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 such a natural person.

- (h) “**Additional Processor or Subprocessor**” is the contractual partner of the Processor, engaged to carry out specific Processing activities on behalf of the Controller;

- (i) “**Sub-subprocessor**” refers to the agreement partner of the Additional Processor or Subprocessor, who is commissioned by the latter to perform specific Processing activities under the regulatory scope of this GDPR.

2. Subject matter of this GDPR, legal foundations

- (1) **[Legal Foundations]** This GDPR is subject to the provisions of the EU General Data Protection Regulation (GDPR) as from its date of validity.
- (2) **[Subject of the GDPR]** This GDPR governs the Processing of Personal Data by the Processor for and on behalf of the Controller, according to the Controller's instructions, in connection with the Agreement.
- (3) **[Specification of the Processing]** The Agreement in combination with the Special Conditions for the services or products covered by the Agreement define the subject and duration of the commission, the nature and purpose of the Processing, the type of Personal Data involved and the categories of the Data Subjects.
- (4) **[Maintenance, inspection]** If the Processor provides services for the Controller in the area of maintenance/remote maintenance/IT fault analysis where access to the Controller's Personal Data is not intended but cannot be excluded, this GDPR shall apply accordingly.

3. Rights and obligations of the Controller

- (1) **[Lawfulness of the Data Processing]** The Controller shall be solely responsible for assessing whether data can be processed lawfully and for safeguarding the rights of the Data Subjects. The Controller shall ensure in its area of responsibility that the necessary legal requirements are met (e.g., by collecting declarations of consent) so that the Processor can provide the agreed services in a way that does not violate any legal regulations.
- (2) **[Instructions]** The Processor shall process Personal Data only upon the documented instructions of the Controller – including the transfer of Personal Data to a non-EU country or an international organization – unless the Processor is obliged to do so by the law of the European Union or of the Member States, to which the Processor is subjected. In such a case, the Processor shall notify the Controller of such legal requirements prior to the Processing, insofar as the relevant law does not prohibit such a notification due to significant public interest.
- (3) **[Proof from the Processor]** The Processor is entitled to document the adequate implementation of the obligations arising from this GDPR, in particular the technical and organizational measures (section 5) and measures that do not only affect the specific commission, with the following proofs:
 - Current certificates, reports or excerpts from reports from independent instances (e.g., auditors, audit department);
 - A suitable certification from an IT security or data protection audit;
 - Certification in accordance with an approved certification procedure;
 - Compliance with the approved code of conduct.
- (4) **[Checks, inspections]** The Controller can audit at its own expense the compliance with the regulations for data protection and the obligations stipulated in this GDPR by obtaining information and requesting the proofs listed under section 3 (3) from the Processor with regard to the Processing in which it is involved. The Controller will primarily check whether the possibility for inspection granted in Sentence 1 of this paragraph is sufficient. Moreover, the Controller may, at its own expense, inspect on site the compliance with the data protection regulations. The Controller may perform the checks itself or have them performed by a Third Party it has commissioned at its own expense. Persons or Third Parties entrusted with such checks by the Controller must be obliged in a documented form at the time of commissioning to maintain confidentiality. The persons or Third Parties entrusted with the checks by the Controller are announced to the Processor in an appropriate form and are enabled to prove their legitimation for carrying out the checks. Third Parties in the meaning of

this paragraph may not be representatives of the Processor's competitors. The Controller shall announce checks within a reasonable period of time and shall take due care during their performance not to disturb business operations.

- (5) **[Support from the Controller]** In terms of the Processing relating to the Controller, the latter shall inform the Processor immediately and in full about any suspicion of data protection infringements and/or other irregularities in the Processing of the Personal Data. In terms of the Processing relating to the Controller, the latter shall support the Processor promptly and in full in the inspection of possible infringements and in a defense against any claims of affected parties or Third Parties and in a defense against any sanctions imposed by regulatory authorities.

4. Rights and obligations of the Processor

- (1) **[Data Processing]** The Processor processes the Personal Data exclusively in the context of the concluded Agreement in combination with the Special Conditions and under the instructions of the Controller in accordance with the provisions in section 3 (2). The Processor shall not use the Personal Data for any other purposes and shall not pass on the Personal Data submitted to it to unauthorized Third Parties. Copies and duplicates must not be created without the prior consent of the Controller. This excludes backups required to assure proper Data Processing.

The Processor guarantees that the employees involved in the Processing of the Personal Data of the Controller and other persons operating on behalf of the Processor shall process such Personal Data only on the basis of the instructions of the Controller, unless they are obliged to process the data in accordance with the law of the European Union or the member states.

- (2) **[Data Protection Officer]** The Processor undertakes to appoint an independent, expert and reliable Data Protection Officer, insofar as this is required by the applicable law of the European Union or the member state to which Processor is subject.
- (3) **[Space restrictions; power of attorney]** The location of the Data Processing is defined in the Special Conditions for every product or service.

Any Data Processing in so-called non-EU countries (i.e. countries that are not member states of the European Union and do not possess an appropriate level of data protection) shall be carried out with due consideration of the relevant, applicable legal provisions of the European Union.

- (4) **[Support for obligations of the Controller]** The Processor shall – to the contractually agreed extent, taking into account the nature of the Processing and the information available to the Processor – support the Controller in complying with its obligations imposed on the Controller by the applicable, legal provisions.
- (5) **[Support for checks and requests for information]** Should the Controller be obliged to provide state agencies or persons with information about the Processing of Personal Data, the Processor shall support the Controller in providing such information, insofar as this information relates to Data Processing in accordance with this GDPR.

The Processor shall also notify the Controller – insofar as legally permissible – of any communications from the supervisory authorities (e.g., inquiries, notification of measures or requirements) to the Processor in connection with the Processing of Personal Data under this GDPR. Insofar as legally permissible, the Processor shall provide information to third parties, including supervisory authorities, only with the prior written consent of and in coordination with the Controller.

- (6) **[Incident reporting]** The Processor shall inform the Controller immediately of any incidents of serious disruption to operations, any suspicion of data protection violations, and/or other irregularities in relation to the Processing of the Personal Data.
- (7) **[Proof and documentation]** The Parties shall support each other mutually in providing proof and documentation of their due accountability in terms of the principles of proper Data Processing.
- (8) **[Directory of Processing activities performed by commission]** In accordance with the relevant, applicable legal provisions, to which the Processor is subject, the Processor shall maintain a directory of all categories of activities performed by commission of the Controller. The Processor shall support the Controller on request and shall provide the Controller with any details necessary for maintaining its directory of Processing activities, insofar as such information lies within the contractually defined scope of responsibility and service as the Processor and insofar as the Controller has no other access to this information.
- (9) **[Privacy impact assessment]** If the Controller carries out a privacy impact assessment and/or a consultation with the supervisory authority leads to the prospect of a privacy impact assessment, the contractual Parties shall coordinate the content and scope of any possible support services provided by the Processor, if necessary.
- (10) **[Assertion of rights of Data Subjects]** Depending on the type of Processing, the Processor shall support the Controller with its obligation to respond to request for the assertion of the rights of Data Subjects, if possible with suitable technical and organizational measures. If necessary, the contractual Parties shall coordinate the content and scope of any possible support services provided by the Processor.

Insofar as a Data Subject consults the Processor directly with regard to the assertion of a Data Subject right, the Processor shall forward the requests of the Data Subject promptly to the Controller.

- (11) **[Conclusion of the contractual work]** Any documents that contain Personal Data and other files that are no longer required, with the exception of Personal Data that must be retained due to the legal obligation of the Processor, must be returned to the Controller or destroyed or deleted at the expense of the Controller, unless provisions are already stipulated in the Agreement or its Annexes and Appendices and unless agreed otherwise. The same shall apply to test and waste material.
- (12) **[Return or deletion of Personal Data]** Insofar as the contractual Parties have concluded an explicit agreement for the return and deletion of Personal Data and/or data carriers, such an agreement shall take precedence over the provisions in this paragraph.

Insofar as the contractual Parties have not concluded an explicit agreement for the return of Personal Data and/or data carriers of the Controller, the Processor may return Personal Data and/or data carriers of the Controller at the expense of the Controller. If the Controller should fail to fulfil its obligation to accept returns, the Processor shall be entitled to delete/destroy the Personal Data and/or data carriers at the expense of the Controller.

During the term of the contractual relationship or upon expiry on the Agreement, the Controller may demand in writing any Personal Data that has not been destroyed or deleted in accordance with section 4 (12) at its own expense and may specify to the Processor a date (at the latest by the expiry of the Agreement) for such a transfer. Following such a request for a return, the contractual Parties shall reach an agreement on the further modalities for the transfer (such as the format). A request for a return must be received by the Processor one month prior to the return date specified by the Controller and/or one month prior to expiry of the Agreement.

5. Technical and organizational security measures

- (1) **[Technical and organizational measures]** The Processor shall implement suitable technical and organizational measures (“TOMs”) in order to guarantee a level of protection appropriate for the risk inherent with the Processing.

The Processor’s measures that are currently deemed to be appropriate are described in KRONES General technical and organizational security measures (“GTOMs”) and in the service or product specific technical and organizational security measures (“STOMS”) – available under <https://shop.krones.com/shop/KronesDocuments>. The Controller has assessed the technical and organizational measures in connection with any other potential measures with regard to an appropriate level of protection. These measures have been agreed as suitable measures. Any further developments shall be implemented in accordance with section 5 (2).

- (2) **[Further developments]** The technical and organizational measures may be adjusted to the further technical and organizational developments during the course of the contractual relationship.

The Controller shall check the security of the Processing and the appropriateness of the level of protection on a regular basis and shall inform the Processor immediately about any possible need for adjustments. The Controller shall provide the Processor with all necessary information in this respect. For its part, the Processor checks the internal processes and the technical and organizational measures on a regular basis, in order to guarantee that the Processing in its area of responsibility complies with the requirements of the EU GDPR and that the protection of the rights of the Data Subjects is guaranteed.

- (3) **[Audits and proofs]** With regard to the audit and proof possibilities, section 3 (3) and section 3 (4) shall apply.

6. Confidentiality

- (1) **[Confidentiality]** The Processor shall maintain the confidentiality of the Personal Data in relation to the Processing agreed in this document. It shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality, insofar as they are not already subject to an appropriate statutory obligation of confidentiality.
- (2) **[Obligations of persons involved]** The Processor shall familiarize any persons who have access to Personal Data with the data protection regulations and the provisions of this GDPR that are relevant for them.

7. Subprocessors

- (1) **[Authorisation]** The Processor is entitled to deploy Additional Processors (Subprocessors) in order to perform the tasks described in this GDPR. Information about Additional Processors (Subprocessors) will be made available at <https://shop.krones.com/shop/KronesDocuments>.

Commissions that the Processor places with Third Parties as ancillary services to support the execution of the work assigned to it and that do not involve Commissioned Processing for the Controller shall not be regarded as a subcontractual relationship within the meaning of this provision.

- (2) **[Authorisation]** The Controller consents to the above mentioned deployment of Additional Processors (Subprocessors). This authorization will constitute Controller’s prior written consent to the subcontracting by

the Processor of the processing of Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR terms.

- (3) **[Information of intended changes]** From time to time, the Processor may deploy new Additional Processors (Subprocessors). The Processor will give Controller notice (by updating the above mentioned website and providing Controller with a mechanism to obtain notice of that update) of any new Additional Processor (Subprocessor) at a sufficient time before providing that Additional Processor (Subprocessor) with access to Personal Data.

The notification of a new Additional Processor (Subprocessor) permits the Controller to raise an objection to any such changes within a period of 14 days after receipt. If necessary, the contracting parties will agree on the manner, additional or alternative possibilities of providing information on future use or changes in the use of other Subprocessors. This can include, for example, provision and call-up a list of Additional Processors (Subprocessors). The Controller shall not refuse its approval of the involvement of Additional Processors (Subprocessors) without a significant reason.

- (4) **[Selection, back-to-back agreement]** The Processor shall select Additional Processors (Subprocessors) who provide sufficient guarantees that suitable technical and organizational measures will be implemented in such a way that the Processing is carried out in accordance with the requirements of the relevant, applicable legal provisions. The Processor shall make contractual agreements with Additional Processors (Subprocessors) which correspond to the contractual arrangements of this GDPR. The Processor shall define the technical and organizational measures together with the Additional Processor (Subprocessor) and shall monitor the compliance with the agreed technical and organizational measures both before the beginning of Data Processing and then on a regular basis.

8. Term and termination of the GDPR

This GDPR shall be valid for the duration of the actual provision of services by the Processor. This shall apply regardless of the term of any other agreements (in particular, the Agreement) that the Parties have also concluded regarding the provision of the agreed services.

9. Liability and Indemnity

- (1) **[Area of responsibility of the Controller]** Within its area of responsibility, the Controller guarantees the implementation of the obligations arising from the relevant, applicable statutory provisions with regard to the Processing of Personal Data.
- (2) **[Liability]** The liability clause in the Agreement shall apply to this GDPR, unless a restriction of liability in accordance with the relevant, applicable statutory provisions applies in favor of the Processor.

10. Miscellaneous

- (1) **[Contact information]** The contact information of the Processor and the Controller are described in the Agreement.
- (2) **[Validity of the GDPR]** The invalidity of a provision of this GDPR shall not affect the validity of the remaining provisions. If a provision proves to be invalid, the Parties shall replace it with a new provision which approximates the intentions of the Parties as closely as possible.

- (3) **[Changes to GDPR]** Any changes to this GDPR and any side agreements shall be made in writing (including in electronic form), unless otherwise agreed in this GDPR. This shall also apply to the waiver of this written form clause itself.
- (4) **[New Features or Supplements]** Notwithstanding the foregoing limits on changes, when the Processor introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), the Processor may provide terms or make updates to the GDPR that apply to Controller's use of those new features, supplements or related software.
- (5) **[Government Regulation and Requirements]** Notwithstanding the foregoing limits on changes, the Processor may modify or terminate a service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects the Processor to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for the Processor to continue operating the service without modification, and/or (3) causes the Processor to believe the DPA Terms or the Online Service may conflict with any such requirement or obligation.
- (6) **[Precedence]** In the event of any contradictions between the provisions of this GDPR and provisions of any other agreements, and in particular of the Agreement, the provisions of this GDPR shall take precedence. In all other respects, the provisions of the Agreement shall remain unaffected and shall apply accordingly to this GDPR.

11. Annexes

The following Annexes are integral parts of this GDPR:

- [Technical and Organizational Security Measures at Krones \("TOMs" including "GTOMs" and "STOMs"\)](#)
- [List of approved sub-processors for the provision of KRONES services](#)

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

