Data protection purchasing conditions in the sense of commissioned processing pursuant to Art. 28 DSGVO

0. preamble

These Data Protection Purchasing Terms and Conditions are an integral part of the contracts between Mitutoyo Deutschland GmbH / Mitutoyo Europe GmbH (hereinafter "Principal") and the service provider (hereinafter "Processor"). Unless otherwise agreed, all data processing operations are subject to these Data Protection Terms and Conditions of Purchase accepted upon commissioning.

In order to ensure data protection-compliant handling of personal data, you provide us with the following declaration of commitment for commissioned processing pursuant to Art. 28 DSGVO.

This Data Protection Purchasing Terms and Conditions specifies the data protection obligations of the contracting parties arising from the commissioned processing described in detail in the main contract. It shall apply to all activities that are related to the main contract and in which employees of the Processor or third parties commissioned by the Processor may come into contact with personal data of the Customer. The term of this Annex shall be based on the term of the Main Contract.

1. definitions

(1) Personal data (see Art. 4 lit. 1 DSGVO "Definitions").

"Personal data" means any information relating to an identified or identifiable natural person (hereinafter "data subject");

(2) Processor (see Art. 28 GDPR "Processor").

"Processor" - here the service provider - is a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

(3) Instruction (see Art. 28 lit 3 a DSGVO "Processor").

The processor processes the personal data only on the documented instructions of the controller - also with regard to the transfer of personal data to a third country or an international organization.

2. subject matter and duration of the order

2.1 Subject of the order

The Processor shall process Personal Data on behalf of the Customer resulting from individual orders or from other contractual agreements.

2.2 Duration of the order

The duration of the order (term) results from individual orders or from other contractual works. The Customer may terminate this Agreement at any time without notice in the event of a data protection breach by the Processor of the provisions of these Data Protection Purchase Conditions, if the Processor is unable or unwilling to carry out an instruction of the Customer or if the Processor refuses access by the Customer or the competent supervisory authority in breach of the Agreement.

3. concretization of the order content

3.1 Scope, type and purpose of the intended collection, processing or use of data

(1) The type and purpose of the processing of personal data by the Processor for the Customer shall be derived from the contract.

(2) The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client and may only take place if the special requirements of Art. 44 et seq. DSGVO are fulfilled.

3.2 Type of data

The type of personal data processed are described in individual orders or in other contractual agreements.

3.3 Categories of data subjects

The categories of data subjects affected by the processing result from the order.

4. technical and organizational measures

(1) The Processor shall ensure the implementation of the specified technical and organizational measures prior to the start of the Processing, in particular with regard to the specific execution of the order and to the Client for testing.

(2) Insofar as the examination/audit of the technical and organizational measures of the Principal reveals a need for adaptation, the necessary measures shall be implemented without undue delay. Insofar as these do not seriously exceed the state of the art, the Processor shall bear the implementation costs.

(3) The Processor shall comply with the security requirements pursuant to Art. 28 Para. 3 lit. c, 32 DSGVO, in particular in connection with Art. 5 Para. Art. 5 (1), (2) DSGVO in full. Overall, the measures to be taken are data security measures and measures to ensure the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, and the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be fully guaranteed.

(4) The technical and organizational measures are subject to technical progress and further development. In this respect, the Processor shall be obliged to further develop them. However, an improvement in the security level of the specified measures must be achieved in the process. Changes must be documented. The Processor shall inform the Customer of any changes.

5 Correction, restriction and deletion of data

(1) The Processor may not correct, delete or restrict (block) the processing of data processed on its own authority but only in accordance with documented instructions from the Customer. Insofar as a data subject contacts the Processor directly in this regard, the Processor shall forward this request to the Customer without delay.

(2) At the request of the Customer, the deletion concept, right to be forgotten, correction, data portability and information shall be implemented, documented and presented to the Customer.

(6) Quality assurance and other obligations of the Processor

In addition to compliance with the provisions of this Order, the Processor shall have statutory obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Processor shall in particular ensure compliance with the following requirements:

- If required by law, the Processor has appointed a data protection officer who may carry out his activities in accordance with Art. 38 and 39 DSGVO in conjunction with. § Section 38 BDSG. The contact details shall be provided to the Client upon request.

- The maintenance of confidentiality in accordance with Art. 28 para. 3 p. 2 lit. b, 29, 32 para. 4 DSGVO. When carrying out the work, the Processor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarized with the data protection provisions relevant to them. The Processor and any person subordinate to the Processor who has access to personal data may process such data exclusively in accordance with the Client's instructions, including the powers granted in these Data Protection Terms and Conditions, unless they are required by law to process it.

- The implementation of and compliance with all technical and organizational measures required for this order shall be carried out in accordance with Art. 28 (3) p. 2 lit. c, 32 DSGVO [details in Annex 1].

- The Principal and the Processor shall cooperate with the supervisory authority in the performance of their duties upon request.

- The Processor shall fully support the Principal in its cooperation with the supervisory authority.

- The Principal shall be informed immediately about control actions and measures taken by the supervisory authority. This shall also apply insofar as a competent authority is investigating the Processor in the context of administrative offence or criminal

proceedings with regard to the processing of personal data in the course of the Order Processing.

- Insofar as the Client is exposed to an inspection by the supervisory authority, an administrative offense or criminal proceedings, the liability claim of a data subject or a third party or another claim in connection with the commissioned processing at the Processor, the Processor shall fully support the Client.

- The Processor shall control the internal processes as well as the technical and organizational measures to ensure that the Processing in its area of responsibility is carried out in compliance with the requirements of applicable data protection law and that the protection of the rights of the Data Subject is fully ensured.

- Processor shall ensure the verifiability of the technical and organizational measures taken vis-à-vis Customer within the scope of its control powers pursuant to Section 8 of these Data Protection Terms and Conditions.

7 Subcontracting Relationships

(1) Pursuant to Article 28 (2) of the GDPR, the Customer shall be notified of subcontracting relationships prior to commissioning and approval shall be obtained from the Customer. Subcontracting relationships within the meaning of this provision are all services, including those directly related to the provision of the main service. This includes ancillary services which the Processor uses, for example, as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems.

2) The Processor shall be obliged to enter into appropriate and legally compliant contractual agreements with its subcontractors in order to ensure the same level of data protection at the subcontractor as results from these data protection purchasing conditions.

(3) If a subcontractor approved by the Customer provides the agreed service outside the EU/EEA, the Processor shall ensure the admissibility under data protection law pursuant to Art. 44 et seq. DSGVO by taking appropriate measures.

(8) Control rights and other obligations of the Customer

(4) The Customer shall have the right to carry out inspections or have them carried out by inspectors to be named. It shall have the right to convince itself of the Processor's compliance with these Data Protection Purchase Conditions in its business operations by means of spot checks. The Customer shall endeavor not to disproportionately impede the business operations of the Processor.

(5) The Processor shall ensure that the Customer can satisfy itself of the Processor's compliance with its obligations pursuant to Art. 28 GDPR. The Processor undertakes to provide the Customer with the necessary information without being requested to do so and, in particular, to provide evidence of the implementation of the technical and organizational measures.

(6) The Processor may provide evidence of such measures relating to the specific order by means of

- certification in accordance with an approved certification procedure pursuant to Art. 42 DSGVO;

- current attestations by independent bodies (e.g. auditors, data protection officers, data protection auditors);

- a suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).

(7) The enabling of controls by the Customer has been calculated into the order in advance by the Processor.

(8) The contact details of the data protection officer at the Client are:

Stefan Kleinermann, +49 (0) 2401 60 540, dsb@das-datenschutz-team.de

(9) The Processor shall ensure via its data protection contracts with the subcontractors that the Customer shall also be granted all control rights from the Data Protection Terms and Conditions 8 (1) to (4) here.

(9) Notification of violations by the Processor

(1) The Processor shall support the Principal in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. These include, but are not limited to.

(a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for immediate detection of relevant breach events

(b) the obligation to notify personal data breaches to the contracting authority without undue delay

(c) the obligation to assist the contracting authority in its duty to inform the data subject and to provide it with all relevant information in this context

d) the support of the client for its data protection impact assessment

e) the support of the client in the context of prior consultations with the supervisory authority.

(2) The fulfillment of these ancillary contractual obligations shall not entail any claim for compensation of expenses.

(10) Authority of the Principal to issue instructions

(1) The Processor shall immediately confirm verbal instructions in writing.

(2) The Processor shall ensure that verbal instructions are only implemented if they comply with the standards of data protection. Any concerns shall be expressed in writing without undue delay.

(3) The Processor shall inform the Customer without delay if it is of the opinion that an instruction violates data protection regulations.

11 Confidentiality Obligations

(1) Both parties undertake to treat all information received in connection with the execution of the order as confidential for an unlimited period of time and to use it only for the execution of the order. Neither party shall be entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to unauthorized third parties.

(2) The above obligation shall not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain secrecy or which is publicly known.

12. deletion and return of personal data

(1) Copies or duplicates of the data, including data backup or data archiving, outside the assignment shall not be made without the knowledge of the Customer.

(2) Upon completion of the contractually agreed work or earlier upon request by the Customer - at the latest upon termination of the cooperation - the Processor shall hand over to the Customer upon request all documents, created processing and utilization results as well as data files related to the contractual relationship that have come into its possession or, upon prior consent, destroy them in accordance with data protection laws. The deletion shall also include any data backups. The record of the deletion shall be submitted without request.

(3) Documentation that serves as evidence of data processing in accordance with the order and the rules shall be retained by the Processor in accordance with the respective retention periods beyond the end of the cooperation. He may hand them over to the Customer at the end of the cooperation to relieve himself.

(4) If subcontractors are used, the above provisions shall also apply to them.

13 Liability

(1) If there is any suspicion that a data protection incident may have occurred, this must be reported to the Customer in writing without delay. The cause, course of events, possible damage and consequential damage shall be reported. Countermeasures and further steps shall be proposed and approved by the Customer.

(2) The Processor shall be liable to the statutory extent within the meaning of Article 82 of the GDPR for incidents, damage and consequential damage that lie within its area of responsibility and that of its subcontractors.

(3) The Processor shall also be liable for consequential damages that were not foreseeable at the time of the incident.

(4) The Processor shall accept orders only on condition that it maintains sufficient insurance cover to the statutory extent as defined in Art. 83 of the GDPR. Evidence of such insurance coverage shall be provided upon request.

14. final provisions

(1) If the Customer's property with the Processor is endangered by measures of third parties (such as by attachment or seizure), by insolvency proceedings or by other events, the Processor shall inform the Customer. The Processor shall inform the creditors of the fact that data processed on behalf is involved.

(2) The written form shall be required for ancillary agreements.

(3) German law shall apply.

(4) Should individual parts of these data protection purchasing conditions be invalid, this shall not affect the validity of the remaining provisions of the data protection purchasing conditions.

Annex 1 - Minimum requirements for the technical and organizational measures of the processor.

1. confidentiality and integrity (Art. 32 para. 1 lit. b DSGVO)

- Access control

Denial of access to processing equipment with which the processing is carried out to unauthorized persons e.g.: Magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;

- data carrier control

Prevention of unauthorized reading, copying, modification or deletion of data carriers,

- memory control

Prevention of unauthorized entry of personal data and unauthorized access to, modification or deletion of stored personal data,

- user control

Prevention of the use of automated processing systems with the aid of devices for data transmission by unauthorized persons, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data carriers;

- Access control

Ensuring that those authorized to use an automated processing system have access only to the personal data covered by their access authorization, e.g.: Authorization concepts and needs-based access rights, logging of accesses;

- Transmission control

Ensuring that it is possible to check and determine to which entities personal data have been or can be transmitted or made available using data transmission equipment;

- Input control

Ensuring that it is possible to check and establish retrospectively which personal data have been entered or modified in automated processing systems, at what time and by whom, e.g.: Logging, document management;

- transport control

Ensuring that the confidentiality and integrity of personal data is protected during the transmission of personal data as well as during the transport of data media, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- Transport control

Ensuring that confidentiality and integrity of data are protected during transmission of personal data as well as during transport of data media, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature;

- Data integrity

Ensuring that stored personal data cannot be damaged by system malfunctions;

- Separability

Ensuring that personal data collected for different purposes can be processed separately, e.g., multi-client capability, sandboxing;

- Pseudonymization (Art. 32 para. 1 lit. a DSGVO; Art. 25 para. 1 DSGVO).

Processing of personal data in such a way that the data can no longer be attributed to a specific data subject without recourse to additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures;

2. availability and resilience (Art. 32(1)(b) GDPR).

- Rapid recoverability, Art. 32 (1) (c) DSGVO

Ensuring that deployed systems can be restored in the event of a failure;

- Reliability

Ensuring that all system functions are available and that any malfunctions that occur are reported;

- Availability control

Protection against accidental or deliberate destruction or loss, e.g.: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels, and contingency plans;

3. procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR).

- Data protection management;

- Incident response management;

- Data protection-friendly default settings (Art. 25(2) GDPR);

- Order control

Ensuring that personal data processed on behalf of the client can only be processed in accordance with the client's instructions, e.g.: Clear contract design, formalized order management, strict selection of the service provider, prior conviction obligation, follow-up checks.

Status: Okt 2022

Translated with www.DeepL.com/Translator (free version)