

Data Protection Agreement for the Processing of Personal Data by Order

in accordance with article 28 para. 3 clause 1 GDPR

– hereafter referred to as the OP Contract –

between **the Controller** (Customer) and **the Processor** (KRATZER AUTOMATION AG)

The Controller and the Processor are also referred to hereafter as the **Contractual Parties**

Attachments

- Attachment A: Details of the order
- Attachment B: Security concept
- Attachment C: Sub-contracting

Preamble

This Agreement specifies the details of Contractual Parties obligations in terms of data protection that arise from order processing described in this Agreement and in **attachment A “Details of the Order”**. It applies to all activities that are associated with the service and in the course of which the Processor’s employees or third parties appointed by the Processor might come into contact with the Controller’s personal data.

The Parties are aware that the EU General Data Protection Regulation (GDPR: EU Regulation 2016/679) applies with effect from 25.05.2018 and that the requirements are basically governed by article 28 GDPR.

Individual agreements within this OP Contract have precedence over the Processors Standard Terms and Conditions (STC). The provisions of this OP Contract apply in precedence to the Main Contract.

§ 1 Definitions

1. Personal data

According to article 4 para. 1 GDPR “personal data” are 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.

2. Processor

According to article 4 para. 8 GDPR, **Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

3. Instruction

Instruction refers to a particular action in terms of data protection (for example, storage, pseudonymisation, deletion, return) by the Processor with personal data, as a rule, a written order by the Controller. The instructions are issued by the Controller and may be amended, complemented or replaced by individual instructions (individual instruction). Written instructions by the Controller may also be issued in electronic form (text form).

§ 2 Scope of application and responsibility

1. The Processor processes personal data on behalf of the Controller or it cannot be excluded in connection with the provision of the service that the Processor has access to or obtains knowledge of personal data. According to article 28 GDPR, the conclusion of an agreement for processing by order is required.
2. The Controller has selected the Processor in accordance with the duties of care described in article 28 GDPR. Authorisation for data processing by order is conditional on the Controller issuing the order to the Processor in writing (electronic in text form is sufficient). This contract contains the data processing order in accordance with the Parties’ intentions and in particular the Controller’s intention within the meaning of article 28 para. 3 GDPR and establishes the

Parties' rights and obligations with regard to data protection in connection with the provision of the service.

3. The Controller has sole title to the personal data as the "Responsible Party" within the meaning of the GDPR. Due to this responsibility, the Controller may demand that personal data be corrected, deleted, blocked or returned both, during the term of the Contract and after it has ended.

§ 3 Subject matter and duration of the order

1. The subject matter of the order is recorded in **attachment A "Details of the order"**.
2. This OP Contract only commits the Processor to the extent that this is required to fulfill its legal obligations, particularly in accordance with article 28 ff. GDPR and does not impose any additional obligations on the Processor.
3. This OP Contract comes into force as soon as it is signed by both Parties and will end as a rule with the termination of the underlying main contract in accordance with its general terms and conditions. The right to extraordinary termination is not affected.

§ 4 Description of the processing, data and the Data subjects

The scope, nature and purpose of processing as well as the nature of the data and the group of data subjects are described in **attachment A "Details of the order"**.

§ 5 Technical and organisational measures to ensure data protection

The Processor undertakes to the Controller that it will comply with technical and organisational measures that are appropriate and necessary in order to safeguard the data protection regulations that must be applied.

1. Since the Processor will also carry out services for the Controller outside the Controller's business premises, the Processor must document the technical and organisational measures that it takes within the meaning of article 28 para. 3.C GDPR, article 32 GDPR in conjunction with article 5 paras. 1 and 2 GDPR and submit this documentation to the Controller for examination if requested to do.
2. The purpose of these measures is data security and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, accessibility and robustness of the systems associated with this order. In this context, the state of technology, the costs of implementation and the nature, scope and purpose of the processing as well as the various probabilities of occurrence and gravity of the risks for the rights and freedoms of natural persons within the meaning of article 32 para. 1 GDPR must be considered.
3. The state of technical and organisational measures at the time the Contract is concluded is enclosed as **attachment B "Technical and organisational measures to ensure data protection"** of this agreement. The Parties are agreed that amendments to the technical and organisational measures might be necessary in order to adjust to the technical and legal circumstances. The

Processor will agree with the Controller major changes that might affect the integrity, confidentiality or accessibility of the personal data. The Processor may carry out measures that entail only minor technical and organisational changes and that do not negatively affect the integrity, confidentiality or accessibility of the personal data without consultation with the Controller. The Controller may demand at any time an up-to-date copy of the technical and organisational measures taken by the Processor.

§ 6 Correction, restriction and deletion of data

1. The Processor may not correct, delete or restrict processing of the data on its own initiative but only in accordance with instructions from the Controller. Should a data subject refer directly to the Processor with regard to these matters, the Processor will immediately forward this request to the Controller to be handled by the latter. The implementation of rights to deletion, correction and the transferability of data and information may only be taken by the Processor subject to instructions from the Controller.
2. Copies and duplicates of data may only be made with the Controller's knowledge. Excluded from this provision are backup copies, provided they are necessary in order to ensure proper processing of the data, as well as data that are required in order to comply with legal retention obligations or due to orders by courts of law or public authorities. The Processor is authorised to make interim, temporary or duplicate files of the personal data required for procedural and security reasons in order to provide the agreed service.
3. After the contractually agreed work has been completed or earlier at the Controller's request - but at latest at the end of the service contract - the On the Controller's request, the Processor is required to return to the Controller all documents that have come into the Processor's possession, processing and operating results produced as well as data stocks related to the assignment and to personal data. The Processor is required to ultimately destroy this data in accordance with data protection law. The same applies to test and wastage material. The report on the deletion must be submitted on request. The destruction of the data must be confirmed to the Controller, should this be demanded.
4. The Processor is required to retain documentation that serves to prove that data processing has been carried out according to the order and good practice beyond the end of the contract as required by the current rules on records retention. It may relieve itself of this responsibility at the end of the contract by transferring this material to the Controller.

§ 7 Processor's obligations

1. **Bound by instructions received.** The Processor is forbidden to carry out any processing of personal data that is not related to the provision of the service ordered, unless the Controller has given its consent in writing or should this be required by EU law or by the law of the EU member-states to which the Processor is subject.
2. The Processor confirms, to the extent this is required by law, that it has appointed a company data protection officer within the meaning of articles 38

and 39 GDPR. His contact data will be provided to the Controller on request in order that direct contact may be made.

3. **Obligation to provide advice.** The Processor will inform the Controller immediately should an instruction issued by the latter, in the Processor's opinion infringe provisions of the law. The Processor is entitled to suspend implementation of the instruction in question until it has been confirmed or amended by the Controller. The Processor has no obligation to check the legality of instructions.
4. **Obligation to report.** Should the Processor become aware that the protection of personal data within the meaning of article 4 no. 12 GDPR has been infringed in his area of responsibility and that this infringement affects the Controller's data, the Processor will report the infringement to the Controller immediately.
5. **Obligation to provide support.** On request, the Processor provides to the Controller the necessary information for the list of processing activities in accordance with article 30 para. 1 GDPR and will itself maintain a list of processing activities in accordance with article 30 para. 2 GDPR.
6. **Obligation to provide information.** Moreover, the Processor undertakes to support the Controller in accordance with article 28 para. 3.f GDPR in complying with the obligations referred to in articles 34 to 36 GDPR:
 - a) as part of its obligations towards the data subjects and the Controller to provide information, to supply all relevant information in this context immediately.
 - b) In carrying out its data protection impact assessment.
 - c) As part of prior consultations with the regulatory authority.
7. **Data secrecy.** The Processor will ensure that employees involved in processing the Controller's personal data are required to safeguard confidentiality in accordance with articles 28 para. 3 clause 2.b, 29, 32 para. 4 GDPR and have been acquainted with the provisions of data protection relevant to them. The Processor and every person subject to the Processor that have access to personal data may only process this data in accordance with the Controller's instructions, including the powers granted in this agreement, unless they are required to process the data by law. This obligation to secrecy will remain in force after the work has finished.
8. The Controller and the Processor will cooperate with the regulatory authority in fulfilling its obligations when requested to do so.
9. The Processor is required to inform the Controller immediately of inspections and measures carried out by the regulatory authorities should they relate to this order. This also applies should a responsible authority conduct investigation as part of administrative offence or criminal proceedings relating to the processing of personal data in connection with the order processing carried out by the Processor. No information will be provided should this be forbidden by a court of law or public authority.
10. Should the Controller itself be subject to an inspection by the regulatory authority, administrative offence or criminal proceedings, a liability claim by an affected person or a third party or some other in connection with order processing by the Processor, the Processor is required to do its best to provide assistance.

§ 8 Controller's rights and obligations

1. The Controller is entitled to issue additional instructions at any time to the Processor on the nature, scope and procedures in order processing. Instructions may be given
 - a) in writing
 - b) electronically in text form (e. g. by e-mail or ticket)
 - c) verbally

The Controller must confirm verbal instructions to the Processor in text form (e.g. by e-mail).

2. The Controller is required to inform the Processor immediately and comprehensively should it identify errors or irregularities with regard to data protection when checking the results of the work.
3. The Controller is subject to the reporting obligations resulting from article 33 para. 1 GDPR.
4. The Controller will establish by contract or by instructions measures for the return of data media provided and/or the deletion of personal data after the order has been completed.
5. Should the Controller issue individual instructions that exceed the range of services agreed in the Main Contract, the costs that arise as a result will be borne by the Controller.

§ 9 Safeguarding the rights of the data subject

1. The Controller is responsible for safeguarding the rights of those affected.
2. Should the Controller require the Processor's cooperation in safeguarding the rights of data subjects – particularly to information, correction, restriction, data transferability or deletion – the Processor will take the necessary measures having received instructions from the Controller.
3. Should a data subject approach the Processor directly for the purpose of correcting, deleting or restricting information or on the transferability of his data, the Processor will refer the data subject to the Controller should reference to the Controller be possible based on the information provided by the data subject.
4. The Processor will not be liable should the Controller not answer the data subject's request or answer it incorrectly or not on time.
5. Arrangements with respect to any remuneration for additional work/expenses incurred in connection with the assertion of data subjects' rights against the Controller involving the Processor are not affected.

§ 10 Control rights

1. The Controller is entitled to verify, at any time and to the extent required, that the Processor is in compliance with the requirements of the law and the provisions of this OP Contract, particularly the technical and organisational measures (article 28 para. 3.h GDPR).
2. The Processor is required to provide the Controller with information should this be necessary in order to carry out the check within the meaning of para. 1.
3. Subject to having given adequate notice beforehand (at least 14 days, apart from emergency cases), the Controller is entitled to carry out the checks referred to in para. 1 on the Processor's business premises during normal business hours. During such visits, the Controller will ensure that checks are only carried out to the extent necessary should the checks disturb the Processor's normal business operations.
4. Should the Processor's operating and business secrets possibly be disclosed as a result of these checks, the Processor's intellectual property possibly threatened or the Processor's interests similarly impinged, the Controller will have the checks carried out by a qualified and independent third party who is required to commit himself to confidentiality to the Processor beforehand.
5. In the event of measures carried out by the regulatory authority with respect to the Controller within the meaning of article 58 GDPR, particularly with regard to information and control obligations, the Processor is required to provide the Controller with the required information.
6. Proof of technical and organisational measures carried out by the Processor not relating solely to the specific order may also be established by:
 - a) Compliance with approved rules of conduct in accordance with article 40 GDPR.
 - b) Certification in accordance with an approved certification procedure pursuant to article 42 GDPR.
 - c) Current attestations, reports or extracts of reports by independent bodies (e.g. auditors, the internal audit department, data protection officer, IT security coordinator, data protection auditors).
 - d) Suitable certification through an IT security or data protection audit (e.g. in accordance with ISO 27001).
7. The Controller is required to reimburse the Processor the costs of such a control.

§ 11 Sub-processing

1. The Controller is in agreement that, in order to provide its contractually agreed services, the Processor uses companies to provide services and sub-contracts services.

This consent may apply to specific companies (individual consent) or be granted generally to a group or type of companies (general consent).
2. The Processor will inform the Controller of changes in the sub-contractors who play a major part in processing the order. The Controller will only exercise its right to object to changes or to new sub-processors subject to the principles of goodwill as well as of appropriateness and fairness.

3. The sub-processors used at the time this agreement was concluded are listed in **attachment C “Sub-processing relationships”** and are deemed to have been approved by the Controller.
4. The Processor is required to exercise the utmost care in selecting any sub-processors and before making an appointment to ensure that the sub-processor can comply with agreements made between the Controller and the Processor.
5. The Processor is required to ensure that the rules agreed in this Contract and any supplementary instructions issued by the Controller also apply to the sub-processor.
6. The Processor is particularly required to ensure by means of contractual agreements that the Controller’s control rights (section 10 of this agreement) and those of the regulatory authorities also apply to the sub-processor and that appropriate control rights are agreed with regard to the Controller and the regulatory authorities.

§ 12 Processing in third countries

1. The contractually agreed services will only be provided in a member-state of the European Union or in some other signatory-state to the agreement on the European Economic Area (EEA).
2. Data processing in a third country, even by a sub-processor, requires the Controller’s prior consent and may only take place provided the particular conditions of article 44 ff. GDPR are fulfilled, unless the Processor is required by EU law or the law of the member-states to which the Processor is subject to carry out processing in a third country; in such a case, the Processor will inform the Controller of these legal requirements prior to processing, unless the applicable law forbids such notification on account of an important public interest (article 28 para. 3 clause 2.a GDPR).
3. The Controller’s consent to processing in a third country is considered to have been given with respect to processing referred to in **attachment C “Sub-processing relationships”**.

§ 13 Data secrecy and obligations to secrecy

1. The Processor undertakes to comply with the same rules on secrecy as apply to the Controller. The Controller is required to inform the Processor of any special rules on the protection of secrecy.
2. The Processor gives an assurance that it is aware of the currently valid rules on data protection provided for in law and that it is acquainted with their application.
3. Both Parties undertake without any time limitation to treat all information that they receive in connection with the implementation of this agreement as confidential and only to use this information in order to implement the Contract. Neither of the Parties is entitled to use all or part of this information other than for the purposes referred to above or to disclose this information to third parties.
4. The above obligation does not apply to information that one of the Parties can prove that it has acquired from third parties who are not bound to secrecy or that is publicly known.

§ 14 Remuneration

1. The remuneration agreed in accordance with this OP Contract also includes any reimbursement of expenses incurred for working time of the Processor's staff involved as well as any out-of-pocket expenses (e.g. travel or material costs). As far as is possible, foreseeable and reasonable, the Processor will inform the Controller of the amount of remuneration by way of an appropriate estimate.
2. The amount of remuneration will be calculated in accordance with the Main Contract. Should no rules on remuneration or applicable rates for services provided relevant to the OP Contract have been agreed in the Main Contract, the Processor's standard rates will apply or, should it not be possible to determine these rates, the customary rates in the business.

§ 15 Liability

1. Reference is made to the rules on liability in article 82 GDPR.
2. Internally in relations with the Processor, the Controller alone is responsible for compensation for any damage incurred by those affected by unauthorised or incorrect data processing or use as part of order processing in accordance with the laws on data protection.
3. Should the Controller be called to account by an individual with regard to any claims for compensation in accordance with article 82 GDPR, the Processor undertakes to assist the Controller as far as possible in resisting claims.

§ 16 Information obligations, written form clause, choice of law

1. The Processor is required to notify the Controller immediately should the Controller's personal data be endangered by attachment or confiscation, by insolvency or settlement proceedings or by other events or measures whilst in the Processor's possession. The Processor will immediately inform all those responsible in this connection that the Controller has sole sovereignty over and ownership of the personal data as the "responsible party" within the meaning of the GDPR.
2. Amendments of and additions to this attachment and all its component parts – including any assurances by the Processor – require a written agreement and the explicit reference to the fact that it relates to an amendment of or addition to this agreement. This also applies to a waiver of this written form clause.
3. Should any provision in these contractual conditions be invalid, this will not affect the validity of the remaining provisions. The Parties undertake to replace in good faith an invalid provision or a provision omitted unintentionally by a provision that most closely approximates to the purpose pursued jointly by the Parties.