Data processing contract

Contract for the processing of personal data on behalf of a controller in accordance with Art. 28 GDPR

between

.....

as the controller (hereinafter referred to as the **"customer"**)

and
Aliaxis Deutschland GmbH. Steinzeugstr. 50, D-68299 Mannheim

as the processor (hereinafter referred to as the **"contractor"**)

- The customer and contractor shall each be referred to individually as a "party" and collectively as the "parties" -

Preamble

The contractor shall provide services for the customer by storing data on the customer's welding and installation processes and job processing, more specifically in relation to the equipment and resources required for such jobs, in accordance with a separate contract for mobile applications (apps) and digital services, including via the customer portal provided by the contractor (hereinafter referred to as the **"main contract"**). Part of the main contract shall include the processing of personal data, as described in the General Data Protection Regulation (**"GDPR"**). In order to meet the requirements of the GDPR for such processing activities, the parties wish to conclude the following agreement; unless explicitly agreed otherwise, the contractor shall not be entitled to separate remuneration for performing this agreement.

§ 1 Subject / Scope of the Assignment

(1) As part of the cooperation between the parties under the main contract, the contractor shall gain access to personal data belonging to the customer (hereinafter referred to as **"customer data"**) and the contractor shall process such data exclusively on behalf of the customer and according to the customer's instructions as stipulated in Art. 4 No. 8 and Art. 28 GDPR.
(2) The contractor shall process customer data exclusively in the manner specified in **Annex 1** 1 and to the extent and for the purpose specified in the same document. The relevant data subjects are presented in **Annex 2** to this agreement. The duration of the processing shall depend on the term of the main contract.
(3) The contractor shall be prohibited from processing customer data in any way that deviates from or goes beyond the specifications of **Annex 1** and **2**. This also applies to the processing of anonymised data.
(4) The customer data shall be processed exclusively within the Federal Republic of Germany, a member state of the European Union or another country within the European Economic Area. The data may only be transferred to a third country with the customer's written permission; this may only occur if the special requirements stipulated in Art. 44 to 49 GDPR are met.
(5) The provisions of this agreement shall apply to all activities related to the main contract where the contractor and the contractor's employees or subcontractors may come into contact with personal data that is provided by the customer or collected on behalf of the customer.

§ 2 Authority of the Customer

(1) The contractor shall only process the customer data within the scope of the assignment and exclusively on behalf of the customer and according to the instructions issued by the customer, as stipulated in Art. 28 GDPR (commissioned processing), particularly with regard to the transfer of personal data to third countries or international organisations. In this respect, the customer shall be solely entitled to issue instructions on the nature, scope and method of the processing activities (hereinafter referred to as a **"right to issue instructions"**). If the contractor is obliged to perform further processing under the laws of the European Union or other member states, the customer must be notified of the legal requirements prior to processing.

Data processing contract

(2) The customer shall generally issue instructions in writing; any verbal instructions must be confirmed by the contractor in writing. The persons authorised to issue and receive instructions are detailed in **Annex 3**. If the persons indicated in **Annex 3** are changed or become unavailable on a long-term basis, their replacements or representatives must be immediately indicated to the other party in text form. The contractor shall promptly notify the customer if there is a change in the persons authorised to receive instructions. Until the customer has received such a notification, the persons previously indicated to the customer shall still be deemed authorised to receive instructions.
(3) If the contractor believes an instruction issued by the customer constitutes a violation of data protection regulations, the customer must be immediately informed. The contractor shall be entitled to refrain from executing the instruction in question until it has been confirmed or changed by the customer.

§ 3 Protective Measures to be Implemented by the Contractor

(1) The contractor must comply with the statutory data protection regulations and refrain from disclosing any information obtained from the customer or making it available to third parties. All documents and data must be secured against unauthorised access using state-of-the-art technology.
(2) Furthermore, the contractor shall oblige all persons entrusted with the task of processing and performing this agreement (hereinafter referred to as **"employees"**) to maintain confidentiality by means of a written agreement (obligation of confidentiality, point (b) of Art. 28 (3) GDPR) and the contractor shall take due care to ensure that such employees fulfil their obligation. If so requested by the customer, the contractor shall present written or electronic evidence to prove that the employees are subject to such an obligation.
(3) The contractor shall structure all internal affairs in a way that ensures compliance with the specific requirements of data protection law. The contractor agrees to take and maintain all the technical and organisational measures required to adequately protect customer data in accordance with Art. 32 GDPR, particularly the measures listed in **Annex 4** to this agreement, for the duration of the data processing assignment.
(4) The contractor reserves the right to change such technical and organisational measures, but the contractor must always ensure the contractually agreed level of protection. The contractor must immediately inform the customer in writing if there is reason to believe that the measures described in **Annex 4** are no longer sufficient; in such cases, the contractor shall discuss further technical and organisational measures with the customer.
(5) If so requested by the customer, the contractor shall present appropriate evidence to prove that the technical and organisational measures specified in **Annex 4** are being taken.

§ 4 Information and Assistance to be Provided by the Contractor

(1) In the event of any faults, suspected data breaches, violations of the contractor's contractual duties, suspected security incidents or other irregularities that might arise when customer data is being processed by the contractor, employees or third parties, the contractor shall inform the customer immediately and within 48 hours at the latest in writing or text form. The same shall apply if the contractor is audited by the data protection supervisory authority. The reports described in the first sentence of § 4 (1) must contain at least the information specified in Art. 33 (3) GDPR.
(2) In the cases described in § 4 (1) above, the contractor shall provide the customer with a reasonable degree of assistance in clarifying the facts of the matter, rectifying the situation and informing third parties. In particular, the contractor shall immediately take the necessary measures to secure the data and mitigate any adverse effects for the data subjects; the contractor shall inform the customer and await further instructions.
(3) The contractor agrees to provide the customer with any information and evidence requested verbally or in writing within a reasonable period to allow the customer to inspect the contractor's technical and organisational measures in accordance with § 7 (1) of this agreement. Furthermore, the contractor shall provide the customer with a comprehensive, up-to-date data protection and security plan for the data processing and authorised persons upon request.

§ 5 Other Obligations of the Contractor

(1) The contractor shall be obliged to keep a record of all categories of data processing activities performed on behalf of the customer, as stipulated in Art. 30 (2) GDPR. The record must be provided to the customer upon request.
(2) The contractor must help the customer carry out a data protection impact assessment in accordance with Art. 35 GDPR and provide assistance during any prior consultations with the supervisory authority in accordance with Art. 36 GDPR.
(3) Insofar as the contractor is legally obliged to appoint a data protection officer, the contractor hereby confirms that this has been done. The

data protection officer may be contacted as follows: Aliaxis Deutschland GmbH, FAO Jörn Menzel, Steinzeugstr. 50, D-68299 Mannheim, datenschutz@aliaxis.com, Tel.: +49 621 486-1325, Fax: +49 621 486-25 1325.
The customer must be immediately informed in writing if the contractor appoints a new data protection officer or a new contact for data protection issues.
(4) If customer data is jeopardised in the hands of the contractor through seizure, confiscation, insolvency or settlement proceedings, or any other events or third-party measures, the contractor must immediately inform the customer unless this is prevented by a judicial or official order. In such cases, the contractor shall immediately inform all responsible parties that the customer is solely entitled to make decisions concerning the data as the "controller" (as defined in the GDPR).

§ 6 Subcontracting Relationships

(1)) The contractor shall not be authorised to hire subcontractors to fulfil the obligations assumed under this agreement (**"subcontracting relationships"**). Any exceptions to this rule shall only be made in specific cases with the prior express consent of the customer, which must be given in writing. In such cases, the contractor must ensure that the subcontractors are also subject to the provisions of this agreement and the customer must be granted all rights to inspect the subcontractors in accordance with § 7 of this agreement. The contractor shall not be permitted to establish subcontracting relationships with third parties outside the European Economic Area.
The subcontracting relationships that had been established prior to this agreement, as detailed in **Annex 5**, shall be permitted.
(2) For the purposes of this agreement, "subcontracting relationships" shall not include any purely ancillary services provided by third parties for the contractor. This may include postal, transport and shipping services, cleaning services, security services, telecommunications services with no specific relation to the services provided by the contractor for the customer, and any other measures taken to ensure the confidentiality, availability, integrity and resilience of data processing hardware and software. The contractor shall remain obliged to ensure data protection and data security in such cases.

§ 7 Inspection Rights

(1) The customer shall be entitled to regularly check whether the contractor is complying with the provisions of this agreement, and particularly to check whether the contractor is taking the technical and organisational measures referred to in § 3 (3) of this agreement. For this purpose, the customer may obtain information from the contractor or request expert reports, certifications or internal audits; furthermore, the customer may inspect the technical and organisational measures during the contractor's regular business hours or have such inspections carried out by a qualified third party, who must not be one of the contractor's competitors.
(2) The customer shall only carry out inspections to the necessary extent and shall take reasonable account of the contractor's business interests. The parties shall arrange the date and nature of such inspections in good time.
(3) The customer shall document the inspection results and share them with the contractor. If the customer notices any errors or irregularities (e.g. when checking deliverables within the scope of the order), the contractor must be immediately informed. If an inspection reveals circumstances that can only be avoided in the future by restructuring processing activities, the customer shall immediately notify the contractor of the necessary changes.

§ 8 Rights of Data Subjects

(1) The contractor shall take suitable technical and organisational measures where possible to help the customer meet the requirements of Art. 12 to 22 GDPR and Art. 32 to 36 GDPR. In cases where information requested by the customer is not held directly by the contractor, the contractor shall obtain such information immediately but within 10 working days at the latest.
(2) If data subjects exercise their rights under Art. 16 to 18 GDPR, the contractor shall be obliged to rectify, erase or restrict the relevant customer data immediately but within 10 working days at the latest according to the instructions issued by the customer. If so requested by the customer, the contractor shall present written evidence to prove that the data has been deleted, rectified or restricted.
(3) If data subjects assert their rights directly against the contractor (e.g. right of access, rectification or erasure), the contractor shall immediately forward the request to the customer and await further instructions. The contractor shall not communicate with data subjects unless instructed to do so.

§ 9 Term and Termination

Data processing contract

(1) The term of this agreement shall correspond to the term of the main contract. If the main contract can be terminated ordinarily, the provisions for its ordinary termination shall apply accordingly to this agreement. In case of doubt, the termination of the main contract shall be deemed to result in the termination of this agreement and vice versa.
(2) The customer shall be entitled to extraordinarily terminate this agreement for good reason at any time. The customer shall have a particularly good reason for doing so if the contractor fails to fulfil the obligations assumed under this agreement, violates the provisions of the GDPR through intent or gross negligence, or is unable or unwilling to execute an instruction issued by the customer. In the event of simple violations (i.e. neither intentional nor grossly negligent), the customer shall first allow the contractor to rectify the violation within a reasonable deadline. If this deadline expires without bringing about the desired effect, the customer shall be entitled to extraordinarily terminate this agreement.

§ 10 Deletion and Return of Customer Data

(1) Once the main contract has been terminated, the contractor shall return all documents, data and storage media to the customer or, if so requested by the customer, such material shall be completely and irrevocably deleted, unless it has to be retained for a certain period by law. This also applies to any copies of the customer data held by the contractor (e.g. back-ups), but not to any documentation that serves to prove that the customer data has been properly and professionally processed in accordance with the assignment. The contractor must keep such documentation for 6 years and present it to the customer upon request.
(2) The contractor shall provide the customer with written confirmation to state that the data has been deleted. The customer shall be entitled to check whether the contractor has fully and suitably returned or deleted the data in accordance with this agreement; § 7 (2) of this agreement applies accordingly.
(3) The contractor must continue to maintain confidentiality with regard to any data that has become known in connection with the main contract, even after the main contract has come to an end.

§ 11 Liability

(1) The liability of the parties shall be based on Art. 82 GDPR. Notwithstanding the above, the contractor shall remain liable to the customer for the violation of any obligations assumed under this agreement or the main agreement.
(2) The parties may exempt themselves from liability by proving that they are in no way responsible for the circumstances that have resulted in the damage incurred by a data subject. The first sentence of § 11 (2) shall apply accordingly if a fine is imposed on a party; an exemption shall be granted to the extent that the other party takes responsibility for the violation sanctioned by the fine.

§ 12 Final Provisions

(1) The parties hereby agree that the contractor shall not be entitled to claim a right of retention, as stipulated in Section 273 of the German Civil Code (BGB), with regard to the data to be processed and the associated storage media.
(2) Any additions and amendments to this agreement must be made in writing. This also applies to the waiver of this written form requirement.
(3) In case of doubt, the provisions of this agreement shall take precedence over those of the main contract. If individual provisions of this agreement prove to be fully or partially ineffective or unenforceable, or if they become ineffective or unenforceable due to changes in legislation after this agreement has been concluded, this shall have no bearing on the effectiveness of the remaining provisions. In such cases, the ineffective or unenforceable provision shall be replaced by an effective and enforceable provision that best reflects the objective and purpose of the invalid provision.
(4) This agreement is subject to German law. Mannheim shall be the exclusive place of jurisdiction.

23.09.2021

Customer:	Contractor:
	Aliaxis Deutschland GmbH
	Steinzeugstrasse 50
	D-68229 Mannheim

Data processing contract

Data processing contract

Annexes

Annex 1 Nature, Scope and Purpose of Data Processing

We will process the data you give us to provide essential services.
The aim of such services is to improve the traceability and documentation of work processes involving our equipment and resources (or the resources of our competitors). We will record the location in which our equipment and resources are used, as well as the usage parameters. The stored data records may contain the personal data of your employees / customers in some cases. We will also store your billing and contract documents and make them available for you to download at any time.

Annex 2 Types of Data and Categories of Data Subjects

Types of data:

- Personal master data
- Communication data (e.g. telephone, email)
- Contract master data (contractual relationship, interest in products / contracts)
- Customer history
- Contract billing and payment data
- Planning and control data
- Geodata

Categories of data subjects

- Existing customers
- Prospective customers
- Employees
- Suppliers
- Commercial agents
- Contacts

Annex 3 Persons Authorised to Issue and Receive Instructions

Customer: the user registered as the "administrator" in the customer portal
Contractor: our portal customer service team (portal.de@aliaxis.com or +49 621 / 486-1533)

Annex 4 Technical and Organisational Measures of the Contractor (Art. 32 GDPR)

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

1.1 Controlling physical access to facilities

- All external doors are fitted with a cylinder locking system.
- The company premises are fenced off and can be accessed via an entrance manned by external staff.
- The company premises are under video surveillance.
- The office doors are fitted with cylinder locks. Access is only granted by authorised personnel. Access is restricted using a key authorisation concept.
- The server room doors are equipped with cylinder locks. Access is only granted by authorised personnel. Access is restricted using a key authorisation concept.

Data processing contract

1.2 Controlling digital access to systems

- Secure passwords are used for all data processing systems in accordance with the BSI standard “IT-Grundschutz M2.11: Rules for Password Use”.
- OTPs are used for two-factor authentication to ensure a secure VPN dial-in (hardware token and domain authentication).
- A VPN tunnel is used for all external communication with the company network.
- Hard disk encryption is used on the storage media of all mobile devices (notebooks) in accordance with the BSI standard “IT-Grundschutz M 4.337: Use of BitLocker Drive Encryption”.
- There is an administration concept (separate administration accounts) based on the “privacy by design” approach.

1.3 Controlling access to data

- The authorisation structure of the Microsoft domain environment is based on the “need to know” principle, whereby users only gain access to the folders and network drives needed for their daily work.
- The role authorisation concept of the ERP systems is also based on the “need to know” principle.

1.4 Controlling the separation of data

- The ERP systems and the CRM system are served by separate databases.
- Applications for certain uses are managed in separate directories / databases and sometimes even on different servers.
- The company network has various VLANs, where the network segments are virtually separated.

1.5 Pseudonymisation

- Aliaxis Deutschland GmbH observes the principle of data minimisation. If there is no specific purpose for processing a personal data record, the data record is pseudonymised.

2. Integrity (Art. 32 (1) GDPR)

2.1 Controlling the transfer of data

- Transport encryption is used for all outgoing emails.
- A VPN tunnel (SSL-VPN) is used for external access to the company network.
- A data processing agreement is concluded with every processor.
- All employees have to sign a written confidentiality and data secrecy agreement before starting their work for the company.

2.2 Controlling data entries

- In the case of remote maintenance, each remote session is logged.

3. Availability and resilience (rt. 32 (1) GDPR)

3.1 Controlling the availability of systems

- The storage environment has a redundant controller, power supply and network connection.
- There is an HA virtualisation cluster.
- There is a back-up concept, whereby data is transferred to a separate NAS system and also stored on removable media.
- All business-critical systems are backed up on a daily basis; non-critical systems are backed up once a week.
- All server systems are secured with a UPS.
- All servers and clients have anti-virus protection with integrated malware protection.

Data processing contract

- All client systems have a software firewall.
- The company network is protected by a firewall with a content filter.
- All incoming and outgoing emails are processed separately by Microsoft 365 using an integrated virus scanner and spam filter.
- All incoming and outgoing emails are legally archived in an email archive.

3.2 Recoverability (Art. 32 (1) GDPR)

- The back-ups allow data records to be restored immediately and at any time.

4. Regular inspection, assessment and evaluation (Art. 32 (1) GDPR; Art. 25 (1) GDPR)

- In the interest of complying with the relevant data protection regulations, a data protection management system is used to ensure the regular review, assessment, evaluation and documentation of all processes related to data protection.

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

- Data protection by default is ensured by the company's technical and organisational measures, which are checked and evaluated at regular intervals. The technical measures are constantly optimised in line with the latest developments.

4.2 Controlling the assignment of orders

- No data is processed without corresponding instructions from the customer, as stipulated in Art. 28 GDPR.
- All processors are selected according to strict criteria (subject to prior checks).
- All commissioned processing is performed on the basis of a separate data processing agreement.

Annex 5 Subcontractors

Quellwerke GmbH
Friedrichsdorfer Landstraße 6/7
69412 Eberbach
Website support / Internet services / app development
Data protection officers: Timo Grüber and Christian Hildenbrand, Tel.: +49 6271 / 960 90 00
E-Mail: info@quellwerke.de

No data is transferred to third countries.