# Data processing agreement according to FADP or, analogously, GDPR

between ALSO Schweiz AG

- Controller / Processor - hereinafter referred to as the Client -

and

Suppliers

- Processor - hereinafter referred to as the Contractor -

## 1. Subject and term of the contract

(1) Subject

The subject of the data processing agreement is the Contractor completing the tasks in accordance with the Individual Contract, in particular:

- Technical support and maintenance
- Order processing
- IT services
- Customer service such as repair and any warranty services
- Cloud services, in each case under the relevant product, service, purchase and/or work contract.

(2) Duration

The duration of this data processing agreement (term) corresponds to the term of the individual contract (hereinafter Individual Contract).

(3) Conclusion

This data processing agreement shall enter into force upon signing, with retroactive effect from 1 September 2023.

(4) Scope

This data processing agreement is exclusively applicable in the event that the Contractor processes personal data on behalf of the Client as a processor. This is exclusively the case in connection with the tasks mentioned under item 1 (1).

For the remaining processing operations, where there is no commissioned processing, the Contractor shall publish its principles for the processing personal data and any updates on the internet at Insert URL (Contractor privacy policy).

The Contractor and the Client shall comply with the applicable Swiss data protection law (Swiss Federal Act on Data Protection, FADP and its implementing ordinances) when processing the personal data (as defined in FADP). Where European data protection law (Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR)) is applicable to the Client's end customers, the Contractor shall comply with the GDPR by analogously.

## 2. Clarifying the content of the contract

(1) Nature and purpose of the intended data processing

The nature and purpose of the processing of personal data by the processor for the Client specifically arise from the Individual Contract entered into and its appendices.

| Nature of the processing | Purpose of the data processing |
|---|---|
| Technical support, order processing, IT services, customer service, cloud services | Order processing, technical support, IT services, customer service and cloud services |

The contractually agreed data processing is only carried out in Switzerland or in a member state of the European Union, in another contractual state of the Agreement on the European Economic Area or in a country for which there is a decision of adequacy by the European Commission or the Swiss Federal Council in accordance with Annex 1 of FADP.

(2) Nature of the data

The following types/categories of data (list/description of data categories) are the subject of processing personal data:

☒ Personal master data

☒ Communication data (e.g. telephone, e-mail)

☒ Contract master data (contractual relationship, product or contractual interest)

☒ Client history

☒ Contract settlement and payment information

☒ Planning and management data

☒ Disclosure information (from third parties, e.g. credit agencies or public directories)

(3) Categories of data subjects

☒ Categories of data processing subjects include:

- ☒ The Client’s employees
- ☐ The Client's suppliers
- ☒ The Client's customers
- ☐ Commercial agents/resellers

☐ Contact persons

☐ ……………………………………….

## 3. Obligations of the Client

(1) The Client shall be responsible for making appropriate data protection arrangements in the contractual relationships with third parties and with its end customers and for informing the third parties concerned about the processing, storage and transfer of data and, where applicable, about data processing by the Contractor. The Client shall be responsible for obtaining the necessary consents for this from the third parties concerned, insofar as this is required by law, and for submitting these to the Contractor on request.

(2) The Client authorises the Contractor to process the personal data of the Client and/or its end customers that are processed in connection with the Individual Agreement, regardless of whether they originate from the Client or from third parties, within the meaning of the data protection laws.

(3) The Client acknowledges that the Contractor may pass on detailed information on products, quantities, sales as well as name and address data of the Client and its end customers to its suppliers (sell-out reporting) in order to fulfil its contractual obligations.

## 4. Technical and organisational measures

(1) The Client and the Contractor shall ensure data security appropriate to the risk by means of suitable technical and organisational measures. This is based on Appendix 1, which corresponds to the requirements pursuant to Art. 3 FADP or, analogously, Art. 28(3)(c), 32 GDPR, in particular in conjunction with Art. 1- 4 FADP or, analogously, Art. 5(1)(2) GDPR.

(2) In order to ensure adequate data security, the Client and the Contractor must determine the need for protection of the personal data and specify the appropriate technical and organisational measures in view of the risk (Art. 1 FADP and, analogously, Art. 32(1)  GDPR). The Client and the Contractor must implement technical and organisational measures to ensure that the processed data are only accessible to authorised persons in accordance with their need for protection (confidentiality), are available when they are needed (availability), are not changed without authorisation or unintentionally (integrity), and are processed in a traceable manner (traceability). Details can be found in Appendix 1.

(3) Technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative suitable or better measures. In doing so, the Contractor may not fall short of the security level of the established measures. Significant changes shall be documented.

4. Correction, restriction and deletion of personal data

(1) The Contractor may not, without authorisation, correct or delete personal data processed as part of the contract or restrict its processing, but only with documented instruction from the Client. If a data subject directly contacts the Contractor in this regard, the Contractor shall immediately forward this request to the Client if the Contractor knows that the end customer is to be assigned to the Client.

## 5. Quality assurance and other obligations of the Contractor

The Contractor shall, in particular, ensure compliance with the following requirements (analogous to Art. 28 to 33 GDPR):

a) The Contractor has appointed a data protection advisor. Their current contact information can be easily found on the Contractor's website.

b) The Contractor shall ensure confidentiality is maintained between the parties in accordance with Art. 3(1) FADP or analogously Art. 28(3)(2)(b), 29, 32(4) GDPR. When executing the contract, the Contractor shall only employ people who are obliged to maintain confidentiality and that have previously familiarised themselves with the data protection provisions relevant to them. The Contractor and every subordinate person who has access to personal data may only process this data in accordance with the Client's instructions, including the authorisations granted in this agreement, unless they are legally obliged to process the data.

c) The Client and Contractor shall work together to comply with their respective duties at the request of the supervisory authorities.

d) Immediately informing the Client of control activities and measures from the supervisory authorities if they relate to this contract, to the extent permitted by law. This shall also apply if a competent authority investigates the processing of personal data with regard to the Contractor's execution of the contract in the course of administrative or criminal proceedings.

e) If the Client is exposed to an audit by the supervisory authorities, administrative or criminal proceedings, a liability claim from a data subject or a third party or another claim in connection with the Contractor executing the contract, the Contractor must support the Client to the best of its abilities.

f) The Contractor shall review internal processes and technical and organisational measures in order to ensure that the processing for which it is responsible complies with the requirements of the applicable data protection law and the protection of the rights of data subjects is ensured according to the risk.

## 6. Sub-contractual relationships

(1) Pursuant to this regulation, sub-contractual relationships are services that directly concern the rendering of the principal service. This does not include ancillary services provided by the Contractor, e.g. as telecommunication services, postal/transport services. In contrast, this includes other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Contractor is, however, obliged to enter into suitable and lawful contractual agreements and to implement control measures in order to ensure data protection and secure the Client's data, including with outsourced ancillary services.

(2) The Client hereby grants a general authorisation that the Contractor may also transfer data to a third party, provided that the third party processes the personal data in Switzerland or in a member state of the European Union, in another contractual state of the Agreement on the European Economic Area or in a country for which there is a decision of adequacy by the European Commission or the Swiss Federal Council in accordance with Annex 1 of FADP. If there is no adequacy decision, the Contractor shall take

the appropriate and necessary measures in accordance with Art. 16(2) FADP and Art. 46 GDPR. The Contractor shall inform the Client who the third party is and where the data processing takes place and what measures it has taken if it bases the data transfer on Art. 16(2) FADP or Art. 46 GDPR.

(3) The Contractor shall inform the Client of any planned change with regard to the addition or replacement of other processors, as a result of which the Client shall be able to object to such changes within 14 days of notification, with justification, otherwise the sub-contracting shall be deemed approved. The information shall be provided to the Client by e-mail. If the Client objects and selecting another processor is not possible, the Client may terminate the data processing agreement and the Individual Contract extraordinarily without right to any claim for reimbursement.

(4) The Contractor shall carefully select and regularly review sub-contractors according to their suitability, in particular with regard to FADP requirements. Forwarding the Client's personal data to sub-contractors and their initial employment is only permitted if all of the requirements for sub-contracting have been met. All contractual regulations in the contract chain must also be enforced upon the further sub-contractor.

(5) This does not affect the transfer of data to independent controllers (such as licensors) within the meaning of FADP, in particular if they conclude their own contract with end customers.

## 7. Client control rights

(1) The Client is entitled to verify the services according to the scope of the principal agreement in agreement with the Contractor, or to have such verified by an auditor sworn to professional confidentiality or appointed in individual cases once per calendar year for a maximum of two days during normal business hours by means of an audit. The Client is entitled to feel reassured that the Contractor is complying with this agreement by visiting their business premises by carrying out random inspections, which must be announced at least ten days in advance.

(2) Compliance with the technical and organisational measures that do not only relate to the specific contract can be demonstrated through certification according to an approved certification procedure, current attestations, reports or report excerpts, audits by independent bodies (e.g. auditors, data protection officers, the IT security department, data protection auditors, quality auditors) or suitable certification as a result of an IT security or data protection audit.

(3) The Contractor may raise a claim for remuneration for allowing the Client to carry out inspections. If an examination/an audit by the Client shows need for adaptation, this must be implemented by mutual agreement. The costs shall be borne by the Contractor if the specifications are not industry-specific.

## 8. Notification in the event of infringements

(1) Both parties shall support each other in complying with the legal obligations regarding the security of data protection, reporting obligations in the case of data breaches and loss, data protection impact assessments and prior consultations. Inter alia, this includes:

a) The obligation to report personal data breaches to the other party without undue delay, as soon as possible after discovery, using the notification form in Appendix 2;
b) The obligation to support the other party in its obligation to inform data subjects and to provide all relevant information in this context without delay;
c) Supporting the Client with regard to its data protection impact assessment; and
d) Supporting the Client in its prior consultations with the supervisory authority.

(2) The Contractor may claim compensation for support services that are not included in the service description for the Individual Contract or that cannot be attributed to misconduct by the Contractor.

## 9. Client's authority to issue instructions

(1) The Client shall issue instructions in writing. The Contractor must inform the Client immediately if it believes that an instruction violated data protection regulations. The Contractor is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the Client.

## 10. Deleting and returning personal data

(1) No copies or duplicates of data shall be created without the knowledge of the Client. Excluded from this are security copies if required and commissioned in order to ensure proper data processing that are required with regard to compliance with statutory storage obligations.

(2) After completing the contractually agreed work or at an earlier point in time at the request of the Client – at the latest at the end of the Individual Contract – the Contractual must hand over all of the documents, results from processing or use and all data in connection with the contractual relationship it possesses to the Client or irrevocably destroy them after prior approval. The same applies for test and waste material. The deletion protocol must be submitted to the Client.

(3) Business-relevant documentation and correspondence used to prove proper data processing in accordance with the contract must be stored by the Contractor after the end of the agreement in accordance with the relevant statutory archiving or storage periods.

## 11. Concluding provisions

(1) The Contractor's liability shall be governed exclusively by the service agreement within the framework of the respective Individual Contract.

(2) Offsetting is excluded.

(3) Applicable law is exclusively Swiss substantive law to the exclusion of private international law (IPRG, SR 291) and multinational conflict of laws.

(4) The exclusive place of jurisdiction is Emmen.

____________, on ____________________ ____________, on ____________________

**Client:** **Contractor:**

____________________________________ ____________________________________

(Signature / company stamp) (Signature/ company stamp)

____________________________________ ____________________________________

(Role of the signatory) (Role of the signatory)

____________________________________ ____________________________________

(Name of the signatory in block capitals ) (Name of the signatory in block capitals)

## Appendix 1– Technical and organisational measures

### 1. Confidentiality (Art. 2(a) FADP, analogously Art. 32(1)(b) GDPR)

**Physical access controls**

No unauthorised access to data processing systems.

Purpose: These measures are designed to ensure that unauthorised persons are denied "physical" access to data processing facilities used to process personal data.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Access control system (badge reader, locking system) |
| X | Property security measures |
| X | Security doors, security windows |
| X | Logging of visitors |
| X | Monitoring |
| X | Light barriers, motion detectors |
| X | Door security (locking system, code lock, biometric access lock, security locks) |
| X | Key management / documentation of key assignment |
| X | Security also outside working hours through alarm system and/or plant security |
| X | Regulations for guests / visitors / persons outside the company |
| X | Visitor passes |
| X | Special protective measures for the server room (water alarm system) |
| X | Employee and authorisation cards (must be worn) |
| X | Restricted areas for external visitors and internal employees |
| X | Careful selection of cleaning staff |
| X | Documentation of access control measures |
| X | Access monitoring |

**Physical access control:** No unauthorised system access.
Purpose: These measures are intended to ensure that only authorised persons can access the data processing systems and that they can only be used by them.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Personal and individual user login when logging on to the system or company network |
| X | Password procedure (password policy) |
| X | Multi-factor authentication |
| X | BIOS password protection |
| X | Additional system login for specific applications |
| X | Assignment of individual clients and identifiers only for specific functions |
| X | Automatic locking of the client after a certain time without user activity (also password-protected screen saver or automatic pause switching) |

| | |
|---|---|
| X | Electronic documentation of all passwords (no user passwords) and encryption of this documentation to protect against unauthorised access |
| X | Personalised smart cards |
| X | Housing lock |
| X | Use of intrusion detection systems |
| X | Use of antivirus/anti-malware software |
| X | Use of firewall systems |
| X | Network access control |
| X | Assignment of user profiles to IT systems |
| X | Use of VPN technology |
| X | Use of encryption mechanisms for files |
| X | Encryption of mobile hard disks<br>Data carriers in mobile devices (notebooks, smartphones, etc.)<br>External storage media (USB sticks, memory cards, etc.) |
| X | No device without password or lock code with access to company data |
| X | Obligation to maintain data secrecy in accordance with nFADP |
| X | Proper destruction of hard disks |
| X | Guideline on the private use of IT devices |
| X | BYOD (bring your own device) policy |
| X | Guideline for mobile workstations (e.g. notebook) |
| X | Background check of employees with privileged access to information |
| X | Access to external websites is monitored |
| X | Restricted access to archive information |
| X | Access control for software source code |
| X | Documented access controls |

## Access control

No unauthorised reading, copying, changing or removing within the system.
E.g. authorisation concepts and needs-based access rights, logging of accesses.

Purpose:
These measures are intended to ensure that only persons subject to this access authorisation have access to the data processing system and that access is restricted exclusively to this personal data, so that data cannot be read, copied, modified or removed without authorisation during processing, use and after storage.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Management of authorisations |
| X | Finely graded authorisations |
| X | Profiles |
| X | Roles |
| X | Documentation of authorisations |
| X | Approval procedure for the allocation of authorisations |
| X | Evaluations/logging |

| | |
|---|---|
| X | Auditing/auditing |
| X | Encryption of CD/DVD-ROM, external hard disks and/or laptops (e.g. via operating system, Safeguard, PGP, Veracrypt, etc.) |
| X | Dual control principle |
| X | Separation of responsibilities |
| X | Task-related authorisation profiles |
| X | Reduction of persons with administrator rights to a minimum |
| X | Deletion of data carriers before recycling |
| X | Use of document shredders or service providers for document destruction |
| X | Secure storage of data media |
| X | Proper destruction of hard disks |
| X | Logging of the destruction |
| X | Regular review of authorisations |
| X | Recording, evaluation and monitoring of logs (unsuccessful and successful authentication attempts) |
| X | Documented onboarding and offboarding of employees |
| X | Absence control (access to the data of the absent person) |
| X | Documented access controls |

**Separation control:**
Separate processing of data collected for different purposes. (e.g. sandboxing, multi-client capability)

Purpose:
The purpose-related processing of personal data should be technically ensured. This means that data collected for different purposes should be processed separately.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Separate systems |
| X | Separate databases |
| X | Permissions |
| X | Separation through access regulations |
| X | Separation of test, production, development and archive systems |

Other:
Personal data shall be processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and appropriate technical and organisational measures have been taken.

**2. Integrity** (Art. 2(b) FADP, analogously Art. 32(1)(b) GDPR)
**Release control**

No unauthorised reading, copying, modification or removal during transport or electronic transmission. (e.g. encryption, VPN, signature, etc.)

Purpose:
These measures are intended to ensure that the data carrier cannot be read, copied, altered or removed without authorisation during transport or electronic transmission, or to verify and identify where the transmission of personal data by means of data transmission facilities is envisaged. In this respect, the transport and data carrier controls are combined by the transfer control.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Classification of information |
| X | Encryption of e-mails |
| X | Encryption of CD/DVD-ROM, external hard disks and/or laptops (e.g. via operating system, Safeguard, PGP, Veracrypt, etc.) |
| X | Encrypted data connections (VPN) |
| X | Logging (audit logging) |
| X | Secured Wi-Fi |
| X | SSL encryption for web access |
| X | Regulation on the destruction of data carriers |
| X | Proper destruction of hard disks |
| X | Careful selection of the transport personnel for manual transport |
| X | Overview of regular retrieval and delivery processes |
| X | Malware detection and protection procedures |
| X | Secured data centre input |
| X | Data carrier management |
| X | Separate locking of confidential data carriers |
| X | Controlled destruction of data carriers (e.g. printing errors) |
| X | Deletion of data carriers before replacement |
| X | Secured printouts |
| X | Maintenance of software, hardware + appliances |

**Input control:**
Determining if personal data has been entered into the data processing systems, amended or removed, and by whom, e.g. logging, document management

Purpose:
These measures are intended to ensure the verifiability of a processing operation (input, modification, deletion) concerning personal data. This means that the author, content and time of data storage should be identified.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Access rights / authorisation concept |
| X | System logging |
| X | Security/logging software |
| X | Functional responsibilities |

| | |
|---|---|
| X | Multi-eye principle |
| X | Commitment to information and data protection as well as the protection of business and professional secrets. |

## 3. Availability and resilience

### Availability check

Protection against accidental or deliberate destruction or loss, e.g.: backup concept (online/offline, onsite/offsite), uninterrupted power supply, virus protection, firewall, reporting channels, emergency plans.

Purpose:
It must be ensured that personal data is not accidentally destroyed and is protected against loss. It must be ensured that the systems used can be restored in the event of a malfunction.

Measures taken within the company:

| Present | Measure |
|---|---|
| X | Backup strategy |
| X | Backup retention concept |
| X | Server rooms that are not located under water-bearing systems/facilities |
| X | Uninterrupted power supply (battery, diesel) |
| X | Temperature and humidity monitoring in server rooms |
| X | Virus/threat protection, firewall |
| X | Air conditioning in computer rooms |
| X | Fire and extinguishing protection (fire alarm systems, fire extinguishers) |
| X | Alarm |
| X | Suitable archiving options |
| X | Alternative plan |
| X | Emergency exercise |
| X | Disaster plans, BCM |
| X | Fault and recovery plans, etc. |
| X | Redundant data centre (in-house/external) |
| X | Redundant data connection of the data centres to the corporate network |
| X | Redundant hardware |
| X | Mirroring data |
| X | Maintenance of software, hardware + appliances |

## 4. Procedures for regular review, assessment and evaluation

### Job control:

No commissioned data processing without corresponding instructions from the client, e.g. clear contract design, formalised order management, strict selection of the service provider, obligation to pay in advance, verifications.

Purpose:
The Contractor shall ensure that the data to be processed under the contract are only processed in accordance with the Client's instructions. Indirectly connected to this is the Client’s duty to issue instructions to Contractors.

The following measures apply in the company:

| Present | Measure |
|---|---|
| X | Written contract for commissioned data processing with subcontractors with provisions on the rights and obligations of the Contractor and Client. |
| X | Regular monitoring of subcontractors' compliance with their obligations under data processing agreements. |
| X | Training of all authorised employees |
| X | Regular retraining |
| X | Secrecy and data confidentiality of employees |
| X | Regular data protection audits by the company data protection officer |
| X | Identification of contact persons and responsible project managers for the specific assignment. |
| X | Careful selection of the Contractor |

# Appendix 2 - to the Data Processing Agreement: Notification form

Notification to: the data protection or information protection officer of the Client / CONTRACTOR

| | |
|---|---|
| CONTRACTOR / CLIENT | |
| Time period/date of the incident | |
| Date of detection | |
| Description of the incident | |
| Categories of data concerned | |
| Number of data subjects | |
| IT systems affected | |
| Responsible department at the CONTRACTOR | |
| Name and contact details of the data protection officer or advisor | |
| Author + date of the message | |
| Who was informed by whom (data protection authorities, data subjects, supervisory authorities) and if so, what was communicated | |
| Source of information about the data breach | |
| Description of the consequences of the incident | |
| Description of any measures already taken by the CLIENT (taking into account that no evidence is destroyed) | |
| If criminal proceedings have been initiated | |
| Description of further technical and organisational measures to be taken in the future | |
| Measures to mitigate the damage of the incident | |
| Overall risk assessment | |