# Contract for order processing in accordance with Art. 28 GDPR

[As of: 01/2023]

# Agreement

between you, as the "controller" within the meaning of the GDPR – hereinafter referred to as the client –

and

**ICARO Software GmbH, Industriestrasse 27E, 63834 Sulzbach, Germany**

- data processor - also referred to below as the contractor

## Preamble

The contractor provides the client with its ICARO SaaS cloud platform for processing and data transfer to third-party systems.
Within the scope of the Contractor's activities, it cannot be ruled out that the Contractor may gain access to the Client's personal data. Appropriate provisions are made in this contract to ensure the security and proper use of personal data.

## 1. Subject matter and duration of the contract

(1) Subject

Provision of various services related to ICARO SaaS, in particular hosting, customizing, and fulfillment of service requests.

(2) Duration

This agreement is linked to the term of the subscription and ends at the latest as soon as and to the extent that the contractor no longer has access in accordance with Section 1. (1) of this agreement and, as a result, no longer processes orders.

## 2. Specification of the content of the order

(1) Type and purpose of the intended processing of data

The ICARO SaaS software is operated on the contractor's servers. Within the scope of the support services/maintenance services/hosting services provided by the contractor, the contractor has the possibility to access the data (type of data/categories of data subjects).

The contractually agreed data processing is carried out exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 ff. GDPR are met.

(2) Type of data

The personal data to be processed is essentially data imported by users of the aforementioned ICARO SaaS platform. This data generally includes name and organizational affiliation, billing information where applicable, and special categories of personal data in accordance with Art. 9 GDPR, insofar as this is relevant to the professional context.

(3) Categories of data subjects

The group of data subjects affected by the handling of their personal data within the scope of this order includes employees of the client and other groups of persons, such as external consultants and service providers.

## 3. Technical and organizational measures

(1) The contractor has put the necessary technical and organizational measures in place before starting processing.

(2) The contractor has established security in accordance with Art. 28 (3) (c), 32 GDPR, in particular in conjunction with Art. 5 (1), (2) GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability, and resilience of the systems. The state of the art, the implementation costs, and the nature, scope, and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR, were taken into account (see Appendix 1: Technical/Organizational Measures).

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. However, the security level of the specified measures must not be compromised. Significant changes must be documented.

## 4. Correction, restriction, and deletion of data

(1) The contractor may not correct, delete, or restrict the processing of the data processed on behalf of the client on its own authority, but only in accordance with the client's documented instructions. If a data subject contacts the contractor directly in this regard, the contractor shall forward this request to the client without delay.

(2) Insofar as covered by the scope of services, the deletion concept, right to be forgotten, correction, and data portability must be ensured directly by the contractor. The contractor shall support the client in providing these services in return for compensation.

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

In addition to complying with the provisions of this contract, the contractor has legal obligations in accordance with Articles 28 to 33 of the GDPR; in this respect, it shall ensure compliance with the following requirements in particular:

a) The contractor is not obliged to appoint a data protection officer in accordance with the GDPR. The following person is named as the contact person: Andreas Fritz, ICARO Software GmbH, Industriestrasse 27E, 63834 Sulzbach, Germany. He can be reached atinfo@icaro.com .

b) Maintenance of confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the contractor shall only employ staff who are bound to confidentiality and who have been familiarized with the relevant data protection provisions. The contractor and any person subordinate to the contractor who has access to personal data may only process this data in accordance with the client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

c) The implementation of and compliance with all technical and organizational measures necessary for this order in accordance with Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in Annex 1].

d) Insofar as the client is subject to supervision by the supervisory authority, administrative or criminal proceedings, liability claims by a data subject or a third party, or other claims in connection with the processing of orders by the contractor, the contractor shall support the client to the best of its ability. The contractor is entitled to expense-based compensation for this support.

**e)** The contractor shall regularly monitor internal processes and technical and organizational measures to ensure that processing within its area of responsibility complies with the requirements of applicable data protection law and that the rights of the data subject are protected.

**f)** Verifiability of the technical and organizational measures taken vis-à-vis the client within the scope of its control powers under Section 7 of this contract.

## 6. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision are understood to be those services that are directly related to the provision of the main service. This does not include ancillary services that the contractor uses to fulfill its business tasks. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and data security of the client's data, even in the case of outsourced ancillary services.

(2) The subcontractors listed in Appendix 2: Subcontracting relationships are involved in the provision of services.

(3) The subcontractors provide the ancillary services necessary in connection with the main service, which are necessary for the correct and contractual functioning of the solution. The client acknowledges this and expressly agrees to the assignment of the tasks described.

(4) If the subcontractor provides the agreed service outside the EU, the EEA, or Switzerland, the contractor shall ensure compliance with data protection laws by taking appropriate measures. The same applies if service providers within the meaning of paragraph 1, sentence 2, are to be used.

(5) Outsourcing to subcontractors or changing the existing subcontractor is permissible provided that:

- the contractor notifies the client of such outsourcing to subcontractors in writing or in text form a reasonable time in advance, and
- the client does not object to the planned outsourcing in writing or in text form to the contractor within 14 days of the contractor's notification of the outsourcing to subcontractors or change of the existing subcontractor, and
- a contractual agreement in accordance with Art. 28 (2)-(4) GDPR is used as a basis.

The consent of the main client may only be refused if there is an important reason. If a subcontractor selected by the contractor is rejected, the contractor shall be entitled to a special right of termination of 4 weeks to the end of the quarter within 14 days.

(6) The transfer of the client's personal data to the subcontractor and the subcontractor's first activity are only permitted once all the requirements for subcontracting have been met.

## 7. Client's rights of control

(1) The client has the right to carry out checks in consultation with the contractor or to have them carried out by auditors to be appointed in individual cases. The client has the right to verify the contractor's compliance with this agreement in its business operations by means of random checks, which must be announced in good time.

(2) The contractor shall ensure that the client can verify the contractor's compliance with its obligations under Art. 28 GDPR. The contractor undertakes to provide the client with the necessary information upon request and, in particular, to provide evidence of the implementation of technical and organizational measures.

(3) Proof of such measures, which do not only relate to the specific order, can be provided by

- compliance with approved codes of conduct in accordance with Art. 40 GDPR;
- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;
- current certificates, reports, or report excerpts from independent bodies (e.g., auditors, internal auditors, data protection officers, IT security departments, data protection auditors, quality auditors);
- suitable certification by means of an IT security or data protection audit (e.g. in accordance with BSI basic protection).

(4) The contractor may assert a claim for remuneration for enabling checks by the client. Expenses incurred by the contractor in connection with the review, control, and documentation of data protection matters

matters (in particular the completion of individual questionnaires) shall be invoiced in accordance with the contractor's current price list.

## 8. Notification of violations by the contractor

(1) The contractor shall support the client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments, and prior consultations. This includes, among other things

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 possible breach of security and enable immediate detection of relevant breach events
b) the obligation to report personal data breaches to the client without delay
c) the obligation to support the client in its duty to inform the data subject and to provide it with all relevant information without delay in this context
d) support for the client in its data protection impact assessment
e) Support for the client in the context of prior consultations with the supervisory authority

(2) For support services that are not included in the service description or are not attributable to misconduct on the part of the contractor, the contractor may claim remuneration in accordance with the current price list.

## 9. Authority of the client to issue instructions

(1) The client shall confirm verbal instructions immediately (at least in text

form). The persons receiving instructions at the contractor are:
Andreas Fritz, Management
Tobias Volk, Head of Hosting
Phone: +49 6028 9916001
Email: datenschutz@icaro.com

(2) The contractor must inform the client immediately if it believes that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the client. In the event of a change or departure of the authorized persons, the parties are obliged to notify each other immediately.

## 10. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the client's knowledge. This does not apply to backup copies, insofar as they are necessary to ensure proper data processing, or to data that is necessary for compliance with statutory retention obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the client – at the latest upon termination of the service agreement – the contractor shall hand over to the client all documents that have come into its possession, processing and usage results created, and data stocks related to the contractual relationship, or destroy them in accordance with data protection regulations after prior consent. The same applies to test and reject material. The deletion log must be presented upon request.

(3) Documentation serving as proof of proper and orderly data processing shall be retained by the contractor beyond the end of the contract in accordance with the respective retention periods. The contractor may hand it over to the client at the end of the contract for the purpose of discharging its obligations.

## 11. Miscellaneous

(1) If the client's data at the contractor's premises is endangered by seizure or confiscation, by insolvency or composition proceedings, or by other events or measures taken by third parties, the contractor shall inform the client immediately. The contractor shall immediately inform all parties responsible in this context that the client retains sovereignty over the data.

(2) Amendments and additions to this annex and all its components – including any assurances made by the contractor – require a written agreement and an express reference to the fact that they constitute an amendment or addition to these terms and conditions. This also applies to any waiver of this formal requirement. Should any provision of this agreement or any further agreement concluded with reference thereto be or become invalid at any time and for any reason, or should the agreement contain a loophole that the parties agree needs to be closed, this shall not affect the validity of the remaining provisions. The invalid provision shall be replaced or the loophole filled by the statutory provisions.

(3) German law shall apply.

| | |
|---|---|
| , | Sulzbach, |
| Place, date | Place, date |
| | |
| Signature of client | Signature of contractor |

**Appendix 1 – Technical and organizational measures**

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

- **Access control**
  Access to the business premises of ICARO Software GmbH is regulated by a security lock.
- **Access control**
  - Users log in to operating systems by entering a password.
  - Only one access per user is used.
  - The password must be at least eight characters long.
  - The password must contain characters from three of the following categories:
    - Uppercase letters (A to Z)
    - Lowercase letters (a to z)
    - Numbers in base 10 (0 to 9)
    - Non-alphabetic characters (e.g., !, $, #, %)
  - All ICARO employees' laptops are encrypted.
  - USB sticks are only used in exceptional cases and exclusively with company-owned encrypted USB sticks.
- **Access control**
  Users are divided into several user groups and also have differentiated permissions for accessing data.
- **Separation control**
  The development systems are multi-layered and separated into local development, demo, and test environments.
- **Pseudonymization** (Art. 32 (1) (a) GDPR; Art. 25 (1) GDPR)
  Where possible, personal data is 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 this additional information is kept separately and is subject to appropriate technical and organizational measures.

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

- **Control of disclosure**
  External access to the company network is only possible via VPN. All accesses are logged.
  Encryption for data transfer/data exchange: Customer-specific encryption software is used on request. All data traffic from ICARO or by ICARO customers is encrypted using SSL.
- **Input control**
  Logging is performed via a log file that records login attempts, logouts, password changes, and write access to a data record, where technically possible and specified.

## 3. Availability and resilience (Art. 32 (1) (b) GDPR)

- **Availability control**
  A complete backup is performed daily.

  The systems are equipped with a hardware RAID controller. An uninterruptible power supply (UPS) is used. The systems are protected from the outside by a firewall.
- Rapid recoverability through appropriate high-availability agreements
  (Art. 32 (1) (c) GDPR);

## 4. Procedures for regular review, assessment, and evaluation (Art. 32 (1) (d) GDPR; Art. 25 (1) GDPR)

- Data protection management;
- Data protection-friendly default settings (Art. 25 (2) GDPR);
- Order control
  No order data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client, e.g.: Clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.