

Data Processing Agreement (DPA)

pursuant to Article 28 GDPR

Agreement

between the

Company_____

Address_____

- Controller- hereinafter referred to as the Customer

and the

SoftBCom Berlin GmbH

Schiffbauerdamm 19, 10117 Berlin

- Processor - hereinafter referred to as Contractor

1. Subject and Duration of the Agreement

(1) Subject

The subject matter of this contract is the use of the Contractor's services by the Customer within the framework of the existing contractual relationship, in particular:

- the use of Software-as-a-Service (SaaS) services in accordance with the applicable terms of use and product descriptions of the contractor (e.g. QAWacht), or
- the utilisation of individual services on the basis of a separate service agreement.

(2) Duration

The duration of this order corresponds to:

- for SaaS services: the duration of active use by the Customer;
- for individual services: the term of the underlying service contract.

2. Specification of Processing

(1) Types of Personal Data

Personal data of the Customer: data of Customers, Customers' Customers, potential Customers and employees of the Customer, namely:

- Personal master data
- Communication data (e.g. telephone, e-mail)
- Contract master data (contractual relationship, product or contractual interest)
- Customer history
- Contract billing and payment data
- Planning and control data
- External information (from third parties, e.g. credit agencies, or from public directories)
- Personnel data (including payroll data)

(2) Type and purpose of data processing

The personal data of the Customer's clients are available in the Contractor's software or are entered there to enable the transmission of information from the Customer's clients or the receipt of information in surveys, alerts and other communications.

The personal data of the Customer's employees is available in the service desk system through which the contractor's enquiries are processed. In order to fulfil their tasks, the

Contractor's designated employees have access to these systems and therefore to certain specified data.

(3) Categories of data subjects

The group of data subjects affected by the handling of their personal data within the scope of this contract includes

- Customers
- Interested parties
- Subscribers
- Employees
- Suppliers
- Sales representative
- Contact persons

The processing of personal data takes place exclusively in the contractually or product-related defined geographical area (e.g. Germany, EU). Personal data is not transferred to third countries outside this area.

If processing outside the defined area is required for the use of functionalities such as external AI services, this is done exclusively with previously completely anonymised data that no longer has any personal reference.

3. Technical and Organizational Measures (TOM)

(1) The Contractor shall document the implementation of the necessary technical and organisational measures set out prior to the award of the contract, in particular with regard to the specific execution of the contract, before the start of processing and submit them to the Customer for review. If accepted by the Customer, the documented

measures shall form the basis of the order. If the Customer's review/audit reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The Contractor shall establish security in accordance with Art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 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 para. 1 GDPR must be taken into account [details: softbcom.com/TOM].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor shall be permitted to implement alternative adequate measures. In doing so, the security level of the specified measures may not be undercut. Significant changes must be documented.

4. Rectification, Restriction, and Deletion of Data

(1) The Contractor may not rectify, delete or restrict the processing of Customer data without authorisation, but only in accordance with documented instructions from the Customer. If a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Customer without delay.

(2) If included in the scope of services, the deletion concept, right to be forgotten, rectification, data portability and information shall be ensured directly by the Contractor in accordance with the documented instructions of the Customer.

5. Quality Assurance and Other Obligations

In addition to complying with the provisions of this contract, the Contractor has legal obligations pursuant to Art. 28 to 33 GDPR; in this respect, the Contractor guarantees compliance with the following requirements in particular:

- a) Written appointment of a data protection officer who performs his or her duties in accordance with Art. 38 and 39 GDPR.
 - The Customer will be informed of their contact details for the purpose of direct contact. The Customer will be informed immediately of any change of data protection officer.
 - Mr. Vladimir Dudchenko, CEO, +49 30 467 268201, vdudchenko@softbcom.com has been appointed as the data protection officer at the Contractor. The Customer must be informed immediately of any change of data protection officer.
 - Their current contact details are easily accessible on the contractor's website.
- b) Maintaining confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obliged to maintain confidentiality and have been familiarised with the data protection provisions relevant to them in advance. The Contractor and any person subordinate to the Contractor who has access to personal data may only process this data in accordance with the instructions of the Customer, including the authorisations granted in this contract, unless they are legally obliged to process it.
- c) The implementation of and compliance with all technical and organisational measures required for this order in accordance with Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Annex 1].
- d) The Customer and the Contractor shall cooperate with the supervisory authority in the fulfilment of their tasks upon request.
- e) Immediately informing the Customer about inspections and measures taken by the supervisory authority insofar as they relate to this order. This also applies if a competent authority investigates the processing of personal data in the context of an administrative offence or criminal proceedings relating to the processing of personal data by the contractor.
- f) If the Customer is subject to an inspection by the supervisory authority, misdemeanour or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Customer to the best of its ability.
- g) The Contractor shall regularly monitor the internal processes and the technical and organisational measures to ensure that the processing in its area of responsibility is

carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

- h) Verifiability of the technical and organisational measures within the scope of the Customer's control powers in accordance with section 7 of this contract.

6. Subprocessors

(1) Subprocessing relationships within the meaning of this provision shall be understood as those services that relate directly to the provision of the main service. This does not include ancillary services which the contractor utilises, e.g. as telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. 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 Customer's data, even in the case of outsourced ancillary services.

(2) The Contractor may only commission subprocessors with the prior express written or documented consent of the Customer.

By way of derogation from sentence 1, the use of OpenAI (ChatGPT) and comparable providers of large language models (LLMs) as possible subprocessors is permitted in the context of the use of QAWacht, provided that the conditions of Art. 28 para. 2-4 GDPR are met.

- a) Outsourcing to subprocessors or changing the existing subprocessor is permitted, provided that:

- the Contractor notifies the Customer of such outsourcing to subprocessors a reasonable time in advance in writing or in text form and
- the Customer does not object to the planned outsourcing in writing or in text form to the contractor by the time the data is handed over, and
- is based on a contractual agreement in accordance with Art. 28 (2-4) GDPR.

- b) The current list of subprocessors is available at

<https://www.softbcom.de/trust/subprocessors> and forms part of this contract.

(3) The transfer of personal data of the Customer to the subprocessor and the subprocessor's initial activities are only permitted once all requirements for subcontracting have been met.

(4) If the subprocessor provides the agreed service outside the EU/EEA, the Contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subprocessor is only permitted,

- a) if the main contractor and the main Customer have expressly agreed in advance (at least in text form) and
- b) all contractual provisions of this data processing agreement and the necessary data protection requirements are also imposed on the other subprocessor.

7. Audit Rights

(1) The Customer shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be appointed in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time.

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

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

- a) compliance with approved codes of conduct in accordance with Art. 40 GDPR;
- b) certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;

- c) Current certificates, reports or report extracts from independent bodies (e.g. auditors, internal audit, data protection officer, IT security department, data protection auditors, quality auditors);
- d) suitable certification through 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 the Customer to carry out inspections. This includes, in particular, the time and effort beyond the usual extent that the Contractor spends on carrying out the inspection.

8. Incident Notification

(1) The Contractor shall support the Customer 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, inter alia:

- a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential breach through security vulnerabilities and enable the immediate detection of relevant breach events;
- b) the obligation to report personal data breaches to the Customer without delay;
- c) the obligation to support the Customer within the scope of its duty to inform the data subject and to provide it with all relevant information in this context without delay;
- d) supporting the Customer for its data protection impact assessment;
- e) supporting the Customer in the context of prior consultations with the supervisory authority.

(2) The Contractor may claim remuneration for support services that are not included in the service description or are not attributable to misconduct on the part of the Contractor.

9. Authority of the Customer to Issue Instructions

(1) The Customer shall confirm verbal instructions without delay (at least in text form).

(2) The Contractor shall inform the Customer immediately if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the data shall not be created without the knowledge of the Customer. Excluded from this are backup copies, insofar as they are necessary to ensure proper data processing, as well as data that is required in order to comply with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier at the request of the Customer - at the latest upon termination of the service agreement - the Contractor shall hand over to the Customer all documents, processing and utilisation results and data pertaining to the contractual relationship that have come into its possession or, with prior consent, destroy them in accordance with data protection regulations. The same applies to test and scrap material. The deletion log must be submitted on request. **The Customer shall decide whether the material is to be returned or deleted.**

(3) Documentation that serves as proof of proper data processing in accordance with the contract shall be retained by the Contractor beyond the end of the contract in accordance with the statutory retention periods. The Contractor may hand them over to the Customer at the end of the contract in order to discharge the Customer.

Place, date: _____

For the Customer:

Name:

Function:

For the contractor:

Signature:



Name: Vladimir Dudchenko

Function: Managing Director

SoftBCom Berlin GmbH