SoftBCom Berlin GmbH
Schiffbauerdamm 19,
10117 Berlin
+49 30 51302118
www.softbcom.com

Data Processing Agreement (DPA)

pursuant to Article 28 GDPR

Version: 16.04.2026

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 Agreement 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, including AI-enabled SaaS services where applicable (e.g. QAWacht and SoftBCom AI Agents), or
- the utilisation of individual services on the basis of a separate service agreement.

(2) Duration

The duration of this Agreement corresponds to:

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

2. Specification of Processing

(1) Types of Personal Data

Personal data processed on behalf of the Customer may include, depending on the relevant service, configuration and use case:

- personal master data;
- communication data (e.g. telephone, email, chat content);
- Agreement master data;
- customer history and interaction history;
- billing and payment data;
- planning and control data;
- personnel data relating to the Customer's employees and agents;
- call audio, transcripts and related communication metadata;
- prompts, instructions, generated responses and workflow-related data;
- routing, handoff and operational metadata;
- external information provided by the Customer or made available through connected systems or authorised third-party sources.

(2) Type and purpose of data processing

The Contractor processes personal data on behalf of the Customer for the provision, operation, support and maintenance of the agreed services.

Depending on the relevant service and configuration, this may include in particular:

- the provision of SaaS functionalities for communication, service workflows, quality assurance, analytics and related operational purposes;
- the processing of Customer, employee, agent and end-user data made available within the Contractor's software or through connected systems;
- the receipt, transmission, storage, structuring, analysis and provision of communication content, including text- and voice-based interactions, transcripts and related metadata;
- the processing of prompts, instructions, workflow states, generated outputs, routing data and handoff information in connection with AI-enabled service functionalities;
- access by the Contractor's designated personnel to the relevant systems and data strictly to the extent necessary for the fulfilment of the agreed services, support obligations and documented instructions of the Customer.

(3) Categories of data subjects

The categories of data subjects affected by the processing under this Agreement may include, depending on the relevant service:

- customers;
- prospective customers and interested parties;
- subscribers;
- employees;
- agents and other authorised users;
- suppliers;
- sales representatives;
- contact persons;
- end users and other persons involved in communications processed within the scope of the service.

(4) Geography / transfers

The processing of personal data takes place in the geographical area defined in the Agreement, product or applicable service documentation.

For traditional SoftBCom products, including SoftBCom Contact Center, SoftBCom Service Desk, SoftBCom Managed Outbound and SoftBCom WFM, personal data is processed and stored exclusively within the agreed geographical area, unless otherwise expressly agreed in the applicable contractual documentation.

For AI-specific SoftBCom products, including QAWacht and SoftBCom AI Agents, personal data is primarily processed and stored in the agreed geographical area. Where technically feasible and commercially reasonable, the Contractor seeks, on a best-effort basis, to use hosting environments, subprocessors and regional endpoints within that area.

For such AI-specific products, the Contractor does not guarantee that all stages of processing will take place exclusively within the agreed primary region, in particular where enabled functionalities involve external providers, distributed infrastructure or subprocessors.

Where processing involves providers or infrastructure outside the agreed primary region or outside the EU/EEA, the relevant processing chain shall be covered by appropriate contractual, technical and organisational safeguards, including Data Processing Agreements (DPAs), Standard Contractual Clauses (SCCs) and, where applicable, measures such as anonymisation, pseudonymisation, minimisation and other product-specific protection mechanisms.

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 Agreement, in particular with regard to the specific execution of the Agreement, 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 are set out in the current Technical and Organisational Measures (TOM) made available by the Contractor and incorporated into this Agreement by reference: https://softbcom.com/hubfs/TOM.pdf.

(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 Agreement, 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) Appointment of a contact person responsible for data protection matters.
The Customer will be informed of the relevant contact details for direct contact. The

current contact details are easily accessible on the Contractor’s website. The Customer will be informed without undue delay of any relevant changes.

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 Agreement, 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.
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 Agreement.

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 subprocessors providing language models, speech technologies, telephony services or comparable externally supported functionalities is permitted in the context of AI-enabled SoftBCom services, including QAWacht and SoftBCom AI Agents, provided that the conditions of Art. 28 para. 2-4 GDPR are met and the applicable contractual, technical and organisational safeguards are in place.

a) Engaging subprocessors or changing existing subprocessors 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 and relevant service providers is available at https://www.softbcom.com/trust/subprocessors and forms part of this Agreement.

(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 where this is contractually ensured in accordance with Art. 28 GDPR, the Customer’s general or specific authorisation framework under this Agreement is respected, and all contractual provisions of this Agreement and the necessary data protection requirements are imposed on the further 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 Agreement shall be retained by the Contractor beyond the end of the Agreement in accordance with the statutory retention periods. The Contractor may hand them over to the Customer at the end of the Agreement in order to discharge the Customer.

Place, date: ______________________

For the Customer:

Name:

Function:

For the Contractor:

Signature:

Name: Vladimir V. Dudchenko

Function: Managing Director

SoftBCom Berlin GmbH