

SOPHY

Agreement on Contract Data Processing

between
Sophy GmbH
Lehmweg 17, 20251 Hamburg
Germany

- contractor -

and

- Client -

The client has concluded a main contract with the contractor. Within the scope of the performance of the main contract, the contractor will process personal data through its software product for the client, who is responsible for the data protection regulations.

1. General

(1) The contractor processes personal data on behalf and under the instructions of the client (hereinafter referred to as "client data"). Operations referred to herein as "processing," "processing," or "processing" (as referred to by Orderer's data) generally refer to the use of personal data. A "use" of client data includes in particular the collection, storage, transmission, blocking, deletion, anonymization, pseudonymization, encryption of client data.

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

- Person master data (name, first name)
- Communication data (address, e-mail address, telephone)
- Free data fields (client defines data type)

2. Subject of the contract, place of data processing

(1) The order includes the services described in more detail in the main contract. The circle that includes persons affected by data processing

- Employee of the client
- Applicant of the client

(2) The processing of the contractor data by the contractor shall take place exclusively in Member States of the European Union or in a State party to the Agreement on the European Economic Area (EEA). Any use of the data outside this area, including by granting access to the data of the Client to persons outside the named area, requires the prior written consent of the Client. Use of data in countries that are neither Member States of the European Union nor Contracting States of the EEA ("third countries") may only be made subject to the further condition that the requirements of Article 44 et seq. of the GDPR are sufficiently fulfilled.

(3) The contractor does not acquire any rights to the client data.

SOPHY

3. Rights and obligations of the client

(1) The client is responsible within the meaning of art. 4 No. 7 GDPR for the processing of client data on behalf of the contractor.

(2) The Principal shall stand by third parties and the persons concerned for the protection of the persons concerned according to Art. 15 et seq. GDPR. Affected rights must be asserted to the client.

(3) The client is the owner of the client data and, in the relationship of the parties to each other, the owner of all possible rights to the client data.

(4) The client is responsible for the fulfillment of information obligations to third parties pursuant to Art. 34 GDPR.

4. Obligations of the contractor, data security

(1) The contractor processes client data exclusively within the framework of the agreements made, the legal obligations and according to the instructions of the client.

(2) The contractor may not make any copies or duplicates of the client data without prior consent in text form by the client, as far as and as long as they are not required to ensure proper data processing or compliance with statutory retention requirements. The contractor may not hand over client data to third parties or other recipients without the prior written consent of the client. Exceptions to this are data transfers to subcontractors whose commissioning has been approved by the client in accordance with Section 6.1.

(3) The Contractor shall appropriately mark the data which it processes on behalf of the Client and keep it separate from any other data.

(4) If the data is processed for different purposes, the contractor will mark the data with the respective purpose.

(5) Upon request, the contractor shall immediately provide the client with a current list of procedures pursuant to Art. 30 para. 2 and 3 GDPR.

(6) The contractor is not obliged to appoint a company data protection officer. In the case of the appointment of a data protection officer, the contractor will communicate his contact details.

(7) The contractor is obliged to design their company and their operational procedures in such a way that the data of the client are secured to the extent necessary and protected against unauthorized knowledge of third parties. The contractor will inform the client in good time about changes in the organization of the data processing on behalf, which are significant for the security of the data.

(8) The contractor is obliged to immediately notify the client of any breach of data protection regulations or of the contractual agreements and / or the instructions given by the client in the course of the processing of data by them or other persons involved in the processing or their appointed subcontractor has taken place.

(9) In the event that the contractor determines or facts justify the assumption that processed by her for the client

- special types of personal data (Article 9 GDPR) or
- personal data relating to criminal acts or misdemeanors (Article 10 of the GDPR)

the contractor has to inform the client immediately and completely about the time, type and extent in written or textual form (fax / e-mail), or otherwise illegally notified to third parties or data processing operations that require a data protection impact assessment. The contractor is also obliged to inform immediately which measures were taken by the contractor to prevent this in the future.

(10) The Contractor shall promptly notify the Principal of an infringement of the protection of personal data and to assist them in their efforts to provide information, remedies and information, including all acts of fulfillment of statutory obligations, at their first request to the extent practicable. In particular, the Contractor will, without delay, take all reasonable measures to minimize and eliminate the risks to the integrity or confidentiality of the Client's data, to safeguard the Client's data and to prevent possible adverse consequences for affected parties, or as far as possible possible to limit.

SOPHY

5. Scope of authority

- (1) The client has the right to issue additional instructions regarding the type and scope of data processing.
- (2) The contractor will inform the client without delay if, in their opinion, a directive issued by the client violates legal regulations.

6. subcontracting

- (1) The commissioning of subcontractors by the contractor is only permitted with prior written consent. The commissioning of the subcontractors named in Annex 1 has been approved by the client.
- (2) The contractor shall carefully select the subcontractor and verify before subcontracting that he / she can comply with the agreements reached between the parties.
- (3) The contractor must also oblige the subcontractor in the subcontract processing contract in writing in the same way as the contractor is obliged to the client due to this contract. In the subcontracting contract, the responsibilities of the contractor and the subcontractor must be clearly distinguished. If several subcontractors are employed, this also applies to the responsibilities between the individual subcontractors. The contractor is liable for the fault of its subcontractors as if it were its own fault.
- (4) Submission of data to the subcontractor shall only be permitted if all the conditions for subcontracting have been fulfilled and the subcontractor has fulfilled the obligation under Section 8 of this contract.
- (5) The contractor has derived control obligations to its subcontractors, which are to be exercised under this contract. The contractor must regularly check compliance with the contractual obligations of the subcontractor in a suitable form, document the result of the test and make the corresponding test report available to the client on request. The client remains entitled to fully supervise the exercise of the control authority by the contractor.

7. Control powers

- (1) The client has the right to control the processing of client data by the contractor to the extent necessary. In particular, the contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with Art. 28 GDPR.
- (2) The contractor is obliged to inform the client to provide information, insofar as this is necessary to carry out the inspection with the meaning of Paragraph 1 is required.
- (3) The client may request inspection of the client data processed by the contractor for the client and of the data processing systems and programs used.
- (4) After prior notification, the client may, within a reasonable period of time, carry out the inspection within the meaning of subsection (1) in the place of business of the contractor during normal business hours. If there are subcontracting conditions, the contractor will carry out these inspections of the respective establishment (s) on behalf and according to instructions of the client. The client will ensure that the checks are only carried out to the extent necessary if the operations of the contractor are disturbed by the controls.
- (5) In accordance with the applicable data protection regulations, the client and the contractor are subject to public controls by the competent supervisory authority. At the request of the client, the contractor shall support the client as much as possible within the framework of regulatory supervision procedures if and insofar as the contractual processing of client data is the subject of the supervisory procedure. In particular, at the request of the Principal, the Contractor will immediately provide her or the Supervisory Authority with all information in connection with this contract and provide the Supervisory Authority with the opportunity to carry out audits to the same extent as the Supervisory Authority may carry out with the Principal. The contractor also grants the competent supervisory authority all necessary access, information and inspection rights in this context. In the event that the supervisor carries out control actions, investigations or actions concerning contractor data with the contractor, the contractor shall inform the client as soon as possible and, as a rule, immediately upon receipt of the notification of the supervisory measure by the authority.

SOPHY

8. Confidentiality

(1) The contractor is obliged to maintain the confidentiality when processing client data. The contractor undertakes to observe the same confidentiality rules as are the responsibility of the client. The client is obliged to inform the contractor of any special secrecy rules.

(2) The Contractor warrants that it is aware of the respective applicable data protection regulations and that it is familiar with their application. The contractor further assures that it complies with the confidentiality pursuant to Art. 28 para. 3 sentence 2 lit. 4 b. 29, 32 para. 4 GDPR and only uses employees or freelancers who are committed to confidentiality and have been familiarized with the data protection regulations that are relevant to them. The Contractor and any person subordinated to the Contractor who has access to personal data may process such data only in accordance with the instructions of the Client, including the powers granted in this Contract, unless they are legally obliged to process them.

(3) The contractor will document these obligations in writing. Upon demand the contracting authority will prove to the contractor that it complies with this provision by submitting the undertakings or by any other suitable means.

9. Maintenance of data subjects

(1) The client is solely responsible for the protection of the persons concerned. Insofar as an affected party should contact the contractor directly for information, correction, deletion or blocking of the client data concerning him, the contractor will immediately forward this request to the client and will not contact the person concerned without a corresponding documented individual instruction from the client. The contractor may provide information to those affected only after prior instruction by the client.

(2) Insofar as the contractor is required to cooperate for the protection of data subjects - in particular those for information, correction, blocking, deletion, data portability - the contractor will take the necessary measures in accordance with the instruction of the client.

(3) Provisions regarding any compensation for additional expenses incurred as a result of supplementary instructions from the client to the contractor shall remain unaffected.

10. Confidentiality

(1) Both parties undertake to treat as confidential all information received in connection with the execution of this contract and to use it only for the purpose of executing the contract. No party is entitled to use this information in whole or in part for purposes other than those stated or to make this information available to third parties.

(2) The above obligation does not apply to information which one of the parties demonstrably received from third parties without being obliged to maintain secrecy or which is publicly known.

11. Technical and organizational measures for data security (Annex 2)

The contractor agrees to the client, the security acc. Art. 28 para. 3 sentence 2 lit. c, 32 GDPR, in particular in conjunction with Art. 5 para. 1, para. 2 GDPR, by means of technical and organizational measures. In this context, the state of the art, the implementation costs and the type, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account. The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is allowed to implement alternative adequate measures. At the same time, the safety level of the specified measures must not be undershot. Significant changes must be documented.

12. Duration of the contract, termination

(1) The contract begins with the signing by the client and ends with the termination of the main contract.

SOPHY

(2) The Principal may terminate the Contract at any time without notice if there is a serious breach by the Contractor of the applicable data protection regulations or obligations under this contract, if the Contractor can not or does not intend to execute the Client's instructions or if the Contractor has access to the Contracting authority or the competent supervisory authority.

13. Return and deletion of data provided

(1) The contractor is prohibited from actively processing client data after termination of this contract; only further storage of the client data remains permitted until the contractor has provided this customer data as intended to the client or deleted or destroyed it; In this case, the provisions of this contract shall continue to apply even after the termination of the contract until the time when the contractor no longer has any client data.

(2) The contractor must completely or irretrievably hand over or delete or destroy her client data and all processing and utilization results obtained from the client as well as all processing and utilization results as soon as her knowledge of the customer is available. Fulfillment of the purpose of the respective collection and use is no longer required, but at the latest after completion of the contractual service. The parties are aware that it is not always technically possible to purposely delete data from the client. In these cases, the contractor undertakes to deactivate the data as far as possible or to no longer actively use it or to use it.

(3) The Contractor shall document the measures in accordance with Section 13.2 in an appropriate manner and confirm to the Client the complete and contractual return or destruction / deletion of the data carriers and data. The client is authorized to control this. Section 7 applies accordingly.

(5) The contractor has no right of retention with regard to the data carrier and client data.

14. Liability

The client and the contractor are liable to the persons concerned in accordance with the provisions of Art. 82 GDPR. In internal relationship, Art. 28 (4) sentence 2 GDPR applies. Without prejudice to Articles 82, 83 and 84 GDPR, the Contractor shall, in violation of data protection regulations, determine the purposes and means of processing and, in particular, exceed the instructions of the Principal with respect to such processing.

15. Final provisions

(1) Amendments, additions and the repeal of this contract must be made in writing. The same applies to a change or cancellation of the written form requirement.

(2) Should individual provisions of this contract be or become invalid or contain a gap, the remaining provisions shall remain unaffected. The parties undertake to replace the ineffective provision with such legally permissible provision which comes closest to the purpose of the invalid provision and best meets the requirements of Art. 28 of the GDPR.

Hamburg,

Directory of general technical-organizational Measures pursuant to Article 32 (1) GDPR

Responsible / processors:

SOPHY GmbH, Lehmweg 17, 20251 Hamburg, Germany

Managing Director: Oliver Knoblauch

Commercial Register: Registergericht Amtsgericht HRB 154658

List of general technical and organizational measures	
1 pseudonymization	<ul style="list-style-type: none"> ▪ The IT systems are restricted to the level required to fulfill the purpose of the contract by means of appropriate privacy-friendly presettings, and accordingly only those personal data are processed which are also necessary for the purpose pursued. The goal is data minimization through the separation of personal identification features and content data, the use of aliases and anonymization and the deletion of personal data as soon as they are no longer needed to achieve the purpose pursued.
2 encryption	<ul style="list-style-type: none"> ▪ mobile workstations are at least protected by encryption of the home drives, by built-in mechanisms (such as FileVault or Bitlocker) ▪ confidential data should be sent taking into account suitable measures according to the categorization of the data (encryption).
3 confidentiality	The data is stored according to ISO 27001, SOC 2/3 and PCI DSS 3.0 in the Google data center Frankfurt
4 integration	<p>To prevent the unauthorized change of personal data, among other things:</p> <ul style="list-style-type: none"> ▪ Authorization and access concepts ▪ Authorization mechanism with possibility for exact differentiation ▪ Audit-proof, binding authorization procedure ▪ Entry Control <p>All administrative activities (such as setting up and changing backups, software updates, etc.) that the contractor carries out for the client based on organizational agreements are always logged and can be traced over the prescribed period.</p>

SOPHY

List of general technical and organizational measures	
5 availability	<ul style="list-style-type: none">▪ Availability Control is ensured by the Google data center▪ job control The personal data of the client are processed exclusively on the basis of the contractually agreed regulations and additional written instructions.
6 Load capacity	<p>The systems and services must be designed in such a way that they remain efficient even in the case of occasionally high or permanently high loads of processing</p> <p>These include, among others:</p> <ul style="list-style-type: none">▪ storage▪ access capacity▪ line capacity
7 physical or technical incident	<p>For quick recovery of systems and databases during physical or technical incidents, among others:</p> <ul style="list-style-type: none">▪ Backup Concepts▪ Redundant data storage▪ cloud services
8 methods for Review, rating and evaluation of Effectiveness of TOM	<p>These include, among others:</p> <ul style="list-style-type: none">▪ Regular audit IT infrastructure▪ Regular check by independent data protection officer

Hamburg 2019/08/16


Responsible