

Contract for the processing of data on Order

between

hereinafter, the Client
and

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

hereinafter, the Contractor

1.1. 1. Genral Conditions

- 1) The Contractor shall process personal data on behalf of the Client according to Art. 4 Sec. 8 and Art. 28 of the EU Regulation 2016/679 - General Data Protection Regulation (GDPR). This Contract governs the rights and obligations of the Parties in connection with the processing of personal data.
- 2) Insofar as the term "data processing" or "processing" (of data) is used in this Contract, the definition of "processing" will be according to Art. 4 Sec. 2.

1.2. 2. subject of the contract

Type of processing

The Contractor shall give services (maintenance and/or servicing of IT systems) on order. A contractual relationship („Main Contract ") based either on individual contractual agreements, general terms and conditions or statutory regulations (e.g., BGB – the civil code of Germany), already exists between the parties in this respect. This Contract shall come into effect when both parties have signed it and will remain valid for the duration of the respective main contract.

The order placed by the client with the contractor shall also include the following tasks and/or services:

- Cloud-based QM and audit system in the form of SaaS

Type of personal data (according to Art. 4 Sec. 1, 13, 14 and 15 DSGVO (Basic Data Protection Regulation))

- Name and contact details
- Task schedules and agenda
- Training and qualification data and certificates
- If applicable, documents containing personal content, uploaded by the client

Groups affected by the data processing:

- Employees of the client
- Suppliers and third parties within the framework of deposited emergency and contingency plans

1.3. 3. Rights and obligations of the client

(1) According to Art. 4 No. 7 DSGVO, the Client is the party responsible for data given to the Contractor for processing. Pursuant to Section 4 (3), the Contractor shall have the right to notify the Client if it is believed that legally inadmissible data processing is contained within an order and/or of an instruction.

(2) As the responsible party, the client shall be responsible for safeguarding the rights of the data subjects. responsible. The Contractor shall inform the Client without delay if data subjects assert their data subject rights against the Contractor.

(3) The Client has the right -- at any time -- to issue supplementary instructions to the Contractor regarding the type, scope and procedure of data processing. Instructions must be given in text form (e.g. e-mail).

(4) Regulations on any remuneration of additional expenses incurred by the Contractor due to supplementary instructions of the Client shall remain unaffected.

(6) If and when the Client has the obligation according to Art. 33, 34 DSGVO to inform third parties or if the Client is required by statute to give any notification, the Client shall be responsible for compliance of the same.

Persons authorized to give instructions on behalf of the Client are:

(Name, organization, role, telephone, e-mail address)

The recipients of instructions on behalf of the Contractor are:

Timo Müller, Management, +49 261 – 92164181, tm@qmspot.com

1.4. 4. General Obligations of the Contractor

(1) The Contractor shall process personal data exclusively within the scope of the agreements made with and/or in compliance with any supplementary instructions issued by the Client, whichever applies. Exceptions may arise if and when legal regulations oblige the Contractor to process the data in a different way. In such a case, the Contractor shall notify the Client of these legal requirements prior to the processing, provided that the relevant law does not prohibit such notification due to important public interest. The purpose, type and scope of data processing shall otherwise be governed exclusively by this Contract and/or the Client's instructions. The Contractor is not allowed to process the data in any other way unless the Client has consented to this in writing.

(2) The Contractor shall, as a matter of principle, process the data sent by the Client only in member states of the European Union (EU) or in the European Economic Area (EEA). The Contractor shall also be permitted to process data outside the EU or EEA, if corresponding subcontractors in the chosen country work in compliance with the requirements of Section 9 and if the requirements of Art. 44-48 DSGVO are met or if an exception as defined in Art. 49 DSGVO is in place.

(3) The Contractor shall inform the Client without delay if an instruction issued by the Client is believed to violate statutory regulations. The Contractor shall be entitled to suspend the implementation of the instruction in question until it is confirmed or amended by the Client. Should the Contractor be able to demonstrate that further processing in accordance with the Client's instructions may lead to legal liability on the part of the Contractor pursuant to Art. 82 of the GDPR, the Contractor shall have the right to suspend further processing until the liability between the parties has been clarified.

(4) The Contractor may give to the Client the names of the person(s) authorized to receive instructions from the Client. If persons authorized to receive instructions are to be named at all, they shall be named in **Annex 1**. In the event of a change in personnel authorized to receive instructions on behalf of the Contractor, the Contractor shall inform the Client thereof in writing.

1.5. 5. Data protection officer of the Contractor

(1) The Contractor confirms having appointed a data protection officer in accordance with Art. 37 DSGVO. The Contractor ensures that the data protection officer has the required qualifications and expertise.

(2) The obligation to appoint a data protection officer pursuant to paragraph 1 may be waived by the Client if the Contractor can prove that it is not required by law to appoint a data protection officer and if the Contractor can prove that operational regulations are in place to ensure that personal data is being processed in compliance with the statutory provisions, the provisions of this Contract and any further instructions issued by the Customer.

1.6. 6. Obligation of the contractor to report Infringements

(1) The Contractor shall be obligated to immediately notify the Client of any infringement of data protection regulations, of contractual agreements and/or of instructions issued by the Customer if the infringement occurs in the course of data processing by the Contractor or other persons involved in the processing. The same shall apply to any violation of the protection of personal data processed by the Contractor on behalf of the Client.

(2) Furthermore, the Contractor shall inform the Client without undue delay if a supervisory authority takes action against the Contractor in accordance with Art. 58 of the GDPR and controls a task being carried out by the Contractor for the Client.

(3) The Contractor is aware that, according to Art. 33, 34 of the GDPR, the Client may have to report to the supervisory authority within 72 hours of becoming aware of this obligation. The Contractor shall support the Client in fulfilling the obligation to report. In particular, the Contractor shall notify the Client of any unauthorized access to personal data processed on behalf of the Client as soon as such access is noticed. The Contractor's notification to the Client shall include the following information in particular:

- a description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of individuals affected, the categories affected, and the approximate number of personal data records affected;
- a description of the measures taken or proposed to be taken by the Contractor to address the personal data breach and, where appropriate, measures to mitigate its potential adverse effects.

1.7. 7. Contractor's obligation to cooperate

(1) The Contractor shall support the Customer in the latter's obligation to respond to requests for preserving data subject rights pursuant to Art. 12-23 GDPR. The provisions of Section 11 of this contract shall apply.

(2) The Contractor shall collaborate with the Client in preparing the directories of processing activities. The Contractor shall provide the Customer with relevant information in an appropriate manner.

(3) The Contractor shall support the Client in complying with the obligations set out in Art. 32-36 GDPR, taking into account the nature of the processing and the information available to the Contractor.

1.8. 8. Power of Inspection

(1) The Client shall have the right, to the extent necessary, to monitor compliance with the statutory provisions of data protection and/or compliance with the contractual provisions made between the parties and/or compliance of the Contractor with the instructions of the Client.

(2) The Contractor shall be obliged to provide the Client with any information required for carrying out the inspection according to of paragraph 1.

(3) The Client may, after prior notification reasonably early, carry out the inspection according to Paragraph 1 at the Contractor's premises during normal business hours. In doing so, the Customer shall ensure that inspections are carried out only to the extent necessary, so as not to disproportionately disrupt the Contractor's operations. The parties assume that an inspection is required no more than once a year. Further inspections shall be justified by the customer, giving an indication of the reason. In the case of on-site inspections, the Client shall reimburse the Contractor to a reasonable extent for the expenses incurred, including personnel costs for giving support to and accompanying the inspection personnel on site. The basis of the cost calculation shall be communicated to the Client by the Contractor prior to the inspection itself.

(4) At the Contractor's discretion, instead of an on-site inspection, proof of compliance with the technical and organizational measures may also be provided through the submission of a suitable, up-to-date audit certificate, reports or report extracts from independent bodies (e.g., auditors, auditing department, data protection officer, IT security department, data protection auditors or quality auditors) or appropriate certification, if the audit report reasonably convinces the Client of compliance according to Annex 2 with the technical and organizational measures named in this Contract. If the Client has reasonable doubts about the authenticity of the test document according to Sentence 1, an on-site inspection can be carried out by the client. The Client is aware that an on-site inspection in data centers is not possible or only possible in justified exceptional cases.

(5) In the event of measures taken by the supervisory authority against the Client according to Art. 58 DSGVO, the Contractor shall be obliged, based on obligations related to information and inspections, to provide the necessary information to the Client and enable the respective competent supervisory authority to carry out an on-site inspection. The Client shall be informed by the Contractor of any corresponding measures planned.

1.9. 9. Subcontracting conditions

(1) The Contractor shall be entitled to assign the subcontractors specified in **Annex 1** to this Contract for the processing of data on behalf of the Contractor.

Changing subcontractors or commissioning further subcontractors is permissible under the conditions specified in paragraph 2.

(2) The Contractor shall carefully select the subcontractor and verify before handing out an assignment that the subcontractor is able to comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organizational measures required under Art. 32 GDPR to protect personal data. The Contractor shall inform the Client in writing of any plans to change a subcontractor or any plans to commission a new subcontractor early enough but no later than 4 weeks before the change or the new commissioning ("Information"). The Client shall have the right to object in writing to the change or the new assignment of a subcontractor within three weeks after receipt of the "Information", stating the reasons. The objection may be withdrawn by the Customer in writing at any time. In the event of a contradiction, the Contractor may terminate the contractual relationship with the Client with a notice period of at least 14 days to the end of a calendar month. The Contractor shall reasonably consider the interests of the Client in the notice period. If no objection is made by the Customer within three weeks after receipt of the "Information", this shall be deemed to be the Customer's consent to the change of a subcontractor or the new assignment of the subcontractor in question.

(3) The Contractor shall be obliged to have the subcontractor confirm that the latter has appointed a company data protection officer in accordance with Art. 37 DSGVO, provided that the subcontractor is legally required to appoint a data protection officer.

(4) The Contractor shall ensure that the provisions agreed in this Contract and, if applicable, any supplementary instructions of the Customer also apply to the subcontractor.

(5) The Contractor shall sign with the subcontractor a contract processing agreement that complies with the requirements of Art. 28 GDPR. In addition, the Contractor shall impose on the subcontractor the same personal data protection obligations that are defined between the Client and the Contractor. On request, a copy of the commissioned data processing agreement shall be provided to the Client.

(6) The Contractor shall, in particular, be obliged to ensure by contractual provisions that the inspection powers (Clause 8 of this Contract) of the Client and of supervisory authorities also apply to the Subcontractor and that corresponding inspection rights of the Client and supervisory authorities are agreed upon. It shall also be contractually stipulated that the subcontractor shall collaborate with these inspection measures and any on-site inspections.

(7) Third-party services which the Contractor uses as a purely ancillary service in order to carry out business activities shall not count as Subcontracting as indicated in paragraphs 1 to 6. These include, for example, cleaning services, pure telecommunication services without any specific reference to services provided by the Contractor to the Client, postal and courier services,

transport services, guard services. The contractor is nevertheless obligated, also in the case of ancillary services provided by third parties, to ensure that adequate precautions along with technical and organizational measures have been taken to ensure the protection of personal data. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and commissioned processing according to Art. 28 of the GDPR if the maintenance and testing concerns IT systems that are also used in connection with the provision of services for the Client and personal data that is processed on behalf of the Client can be accessed during the maintenance.

1.10. 10. Confidentiality requirements

- (1) When processing data for the Client, the Contractor must maintain confidentiality with regard to data received in connection with the order or which the Contractor becomes aware of.
- (2) The Contractor has familiarized its employees with the data protection provisions applicable to them and has obligated them to maintain confidentiality.
- (3) The commitment of the employees, pursuant to paragraph 2, shall be proven to the Client upon request.

1.11. 11. Safeguarding the rights of of data subject

- (1) The Client shall be solely responsible for safeguarding the rights of data subjects. The Contractor is obligated to support the Client in the latter's job of processing applications from data subjects in accordance with Art. 12-23 GDPR. The Contractor shall ensure that the information required in this respect is provided to the Client without undue delay, so that the Client can comply with the obligations defined in Art. 12 (3) of the GDPR.
- (2) Insofar as the cooperation of the Contractor is required for the protection of data subject rights - in particular for information, correction, blocking or deletion - by the Client, the Contractor shall take the measures required in each case in accordance with the Client's instructions. The Contractor shall provide the Client with suitable technical and organizational measures as far as possible, so that the Client is able to respond to requests for the exercising of data subject rights.
- (3) Provisions on any remuneration of additional expenses incurred by the Contractor due to cooperation services in connection with the assertion of data subject rights vis-à-vis the Client shall remain unaffected.

1.12. 12. confidentiality

- (1) Both parties undertake to treat with greatest confidentiality all information received in connection with the performance of this Contract for an unlimited period of time and to use the information only for the performance of the Contract. Neither party shall be entitled to use this

information in whole or in part for purposes other than those mentioned above or to make this information available to third parties.

(2) The above-mentioned obligation shall not apply to information that one of the parties has demonstrably received from third parties without being obliged to maintain confidentiality or that is publicly known.

1.13. 13. Remuneration

The remuneration of the Contractor shall be agreed outside the scope of this Contract.

1.14. 14. Technical and organizational Data Security measures

(1) The Contractor is committed to the Client to observe the technical and organizational measures required to comply with the applicable data protection regulations. This includes in particular the specifications from Art. 32 DSGVO.

(2) The status of the technical and organizational measures in place at the time of signing this Contract is attached as Annex 2 to this Contract. The parties agree that changes to the technical and organizational measures may become necessary in order to adapt to technical and legal circumstances. The Contractor shall discuss with the Client in advance any significant changes that may affect the integrity, confidentiality or availability of the personal data. Measures that involve only minor technical or organizational changes and do not negatively affect the integrity, confidentiality and availability of the personal data can be implemented by the Contractor without coordination with the Client. Once a year or on justified occasions, the Client may request an up-to-date version of the technical and organizational measures taken by the Contractor .

1.15. 15. Duration of the Contract

(1) The Contract shall commence upon signing and shall continue for the duration of the main contract signed by the parties regarding the use of the Contractor's services by the Client.

(2) The Client may terminate this Contract at any time without prior notice if there is a serious breach by the Contractor of the applicable data protection regulations or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction given by the Client or if the Contractor refuses the Client's or the responsible supervisory authority's access in breach of the contract.

1.16. 16. Termination

(1) After termination of this Contract, the Contractor shall, according to the Client's wishes, return to the Client or delete all documents, data and processing or utilization results created in

connection with the contractual relationship that are still in the Contractor's possession. The deletion shall be documented in a suitable manner.

(2) The Contractor may retain personal data that has been processed in connection with an order beyond the termination of the contract if and to the extent that the Contractor has a legal obligation to retain the data. In such cases, the data may only be processed for the purpose of implementing the respective statutory retention obligations. After expiry of the retention obligation, the data must be deleted immediately.

1.17. 17. Right of retention

The Parties agree that an objection to the right of retention by the Contractor according to Section 273 of the German Civil Code (BGB) with regard to the processed data and the associated data carriers is out of the question.

1.18. 18. Final provisions

(1) If any of the Client's property that is still in the hands of the Contractor is endangered by third-party measures (for example by seizure or confiscation), by insolvency proceedings or by other events, the Contractor shall inform the Client without undue delay. The Contractor shall immediately inform the creditors that data being processed on order is involved.

(2) Any ancillary agreements must be made in writing.

(3) Should individual parts of this contract become invalid, this shall not affect the validity of the remaining provisions of the contract.

-----, the -----

Place

Date

-----, the -----

Place

Date

Client

Contractor

2. Annex 1

Subcontractor

For the processing of data on behalf of the Client, the Contractor shall use the services of third parties who process data on the Contractor's behalf ("Subcontractors").

The following company(ies) come under this provision:

Hosting:

Microsoft Ireland Operations Limited

A corporation (UK)

Registered in Ireland under the number 256796

Office:

70 Sir John Rogerson's Quay

Dublin2, Ireland

CRM System:

HubSpot, Inc.

Address: 25 First Street, Cambridge, MA 02141 USA

Mail: hubspotgermany@hubspot.com

Phone: +1 888 HUBSPOT. (+1 888 482 7768)

Fax: +1 617 812 5820

Web: www.hubspot.de

Board and management: Yamini Rangan

Tax number: 20-2632791

3. Annex 2

Technical and organizational measures of the Contractor

The Contractor undertakes vis-à-vis the Client to comply with the following technical and organizational measures, which are necessary to comply with the applicable data protection regulations:

a) Access control

Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used:

- All of the company's central IT systems are located in its own server room or are processed in Microsoft data centers.
- The server room is secured with the use of a locking system and only authorized persons have access.
- The server room is accessible only through the office floor. The office floor is secured by two doors in direct succession (1st door: locking system, 2nd door: locking system/biometric access control, 3rd door physical key).
- The office rooms are secured with a locking system. Keys or biometric access are authorized and issued by management.
- Backups are stored in a fire section other than the server room.

b) Access control

Measures to prevent the use of data processing systems by unauthorized persons:

- Unique user names and individual passwords are assigned for all IT systems in the company.
- The corporate network is protected by a firewall.
- The firewall has an integrated IDS / IPS.
- Both servers and clients are equipped with appropriate virus protection.
- Access from a home office to the company's IT systems is via a secure VPN connection.
- There is a group policy for all client PCs that automatically locks the screen after three minutes of inactivity.
- Systems are automatically locked after three incorrect password entries.
- A password manager is used throughout the company.

c) Access control

Measures that ensure that those authorized to use a data processing system can access only the data they are authorized to access and that personal data cannot be unduly, read, copied, modified, or removed during processing or use, or after storage:

- As part of the form-based check-in process, individual system authorizations for new employees are approved by the supervisor and assigned centrally by HR or management.
- The form-based check-out process ensures that, when an employee leaves, all authorizations are revoked and all IT systems and data carriers are returned.
- The services of a certified document destruction company (security level P-4) are used to ensure that sensitive and personal documents that are no longer needed are disposed of securely. (Garbage cans in the office rooms)

d) Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or during transport or storage on data media, and that make it possible to verify and establish to which bodies a transmission of personal data may perhaps be transmitted by data transmission equipment:

- Customer data is not passed on for error analyses or support activities.

e) Input control

Measures to ensure that it is possible to verify ex-post whether, and by whom, personal data can be entered into data processing systems, changed or removed in data processing systems:

- All central server systems create log files that are analyzed on an ad hoc basis.

f) Order placement control

Measures to ensure that personal data processed on behalf of a client can only be processed in accordance with the client's instructions:

- There are AV contracts with all partners. The party giving the instructions and the party receiving them are named in the order processing agreement.

g) Preservation control

Measures to ensure that personal data is protected against accidental destruction or loss:

- All servers are located in a special room protected by means of an uninterruptible power supply (UPS) with surge protection, smoke detectors, air conditioning and automatic sensors for temperature monitoring.
- In addition, data backups are made regularly and it is verified that they can be read again. The data backup media are stored securely in another fire compartment.
- Maintenance contracts for important systems are in place to regulate external support in the event of problems.

h) Separation of data

Measures to ensure that data collected for different purposes can be processed separately:

Data from different clients are stored and processed in logically separate systems. The same applies to data from one client that are collected and processed for different purposes. In concrete terms, the separation is realized through different databases, servers and storage accounts.

i) Data protection management

The Contractor has appointed an external data protection officer. This officer is responsible for data protection management and regularly informs the Contractor about current legal developments and the measures to be taken to satisfy them.

All employees of the Contractor entrusted with the processing of personal data are committed to data protection and instructed in compliance with the regulations. In addition, all employees of the Contractor are bound to confidentiality.

j) Data protection-friendly default settings Personal data is always processed in accordance with the principle of minimality. Only data that are necessary for given processes are collected and processed.