Data Processing Agreement

Data Processing Agreement pursuant to Article 28 of the GDPR

between

[Name of the data controller / Address of the data controller]

— Data Controller —

and

QM Software GmbH

Blocksbergstraße 183

66955 Pirmasens

— Contractor —

1. General

(1) The Contractor processes personal data on behalf of the Client within the meaning of Article 4(8) and Article 28 of Regulation (EU) 2016/679 — the General Data Protection Regulation (GDPR). This contract governs the rights and obligations of the parties in connection with the processing of personal data.

(2) Wherever the term “data processing” or “processing” (of data) is used in this contract, the definition of “processing” within the meaning of Article 4(2) of the GDPR shall apply.

2. Subject matter of the contract

Nature of the processing

The Contractor shall perform services for the Client in the field of maintenance, support, provision and management of IT systems, software and data. A contractual relationship exists between the parties in this regard (“Main Contract”), which is based on the General Terms and Conditions of QM Software GmbH and the relevant Special Contractual Conditions (SCC). This agreement commences upon signature by both parties and shall remain in force for the duration of the respective Main Contract.

The Client’s order to the Contractor comprises, in particular, the following work and/or services, insofar as agreed in the respective Main Contract:

- Cloud-based QM and audit system as SaaS (QMSpot Cloud / Professional)
- Managed services for the QMSpot platform (Managed QM)
- IoT connectivity and managed IoT services (provision of SIM cards and data transmission, device monitoring, firmware maintenance)
- Managed workplace services for client end devices (patch management, endpoint security, user helpdesk)

- Managed backup services (data backup and recovery)
- Managed monitoring services (technical monitoring of servers, workstations, network devices)
- Managed MDM services (management of mobile devices)
- Managed AI services (provision of AI-based functions via Azure OpenAI)
- Services such as onboarding, training, migration and consultancy

Type of personal data (as defined in Articles 4(1), 13, 14 and 15 of the GDPR)

- Name and contact details (employees, suppliers, clients of the client)
- Task and work schedules, training and qualification data, certificates
- Where applicable, documents containing personal data uploaded by the client to QMSpot
- Device and usage data from end devices managed by the contractor (in particular within the scope of Managed Workplace, Managed MDM, Managed Monitoring)
- Authentication data (usernames, technical identifiers) of users
- Content from backup data sets — these may include all personal data processed by the client on the backed-up systems
- Inputs into the AI platform (prompts, uploaded documents), insofar as the Client uses Managed AI services
- Sensor and device data from IoT components

Group of data subjects affected by the data processing

- The client's employees (including applicants, freelancers, trainees and interns)
- The client's customers, suppliers and business partners
- Third parties in the context of documented contingency and emergency plans
- Other individuals whose data the client processes in the course of its business activities and stores on the systems we manage or in the secure database

The persons authorised to issue instructions at the contractor are:

Timo Müller, Managing Director, +49 261 134 989 10, tm@qmspot.com

3. Rights and obligations of the client

(1) The client is the controller within the meaning of Article 4(7) of the GDPR for the processing of data on behalf of the contractor. Pursuant to Clause 4(3), the contractor is entitled to notify the client if, in its opinion, the contract and/or an instruction involves data processing that is legally impermissible.

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

(3) The Client has the right to issue supplementary instructions to the Contractor at any time regarding the nature, scope and procedures of data processing. Instructions must be provided in writing (e.g. by email).

(4) Provisions regarding any compensation for additional costs incurred by the Contractor as a result of supplementary instructions from the Client remain unaffected.

(5) The Client shall inform the Contractor immediately if it discovers any errors or irregularities in connection with the processing of personal data by the Contractor.

(6) In the event that there is a duty to inform third parties pursuant to Articles 33 and 34 of the GDPR or any other statutory reporting obligation applicable to the Client, the Client shall be responsible for compliance therewith.

4. General obligations of the Contractor

(1) The Contractor shall process personal data exclusively within the scope of the agreements entered into and/or in compliance with any supplementary instructions issued by the Client. This does not apply to statutory provisions which may oblige the Contractor to process data in any other manner. In such a case, the Contractor shall inform the Client of these legal requirements prior to processing, provided that the relevant law does not prohibit such notification on grounds of an important public interest. Otherwise, the purpose, nature and scope of data processing shall be governed exclusively by this contract and/or the Client's instructions. The Contractor is prohibited from processing data in any manner deviating from this, unless the Client has consented to this in writing.

(2) The Contractor shall, as a general rule, carry out data processing on behalf of the Client in Member States of the European Union (EU) or the European Economic Area (EEA). The Contractor is also permitted to process data outside the EU or EEA if appropriate sub-processors in the third country are engaged in compliance with the conditions set out in Clause 9 and the requirements of Articles 44–48 of the GDPR are met or an exception within the meaning of Article 49 of the GDPR applies.

(3) The Contractor shall inform the Client without delay if, in its opinion, an instruction issued by the Client contravenes statutory provisions. The Contractor is entitled to suspend the implementation of the instruction in question until it is confirmed or amended by the Client. Provided the Contractor can demonstrate that processing in accordance with the Client's instructions may result in the Contractor's liability under Article 82 of the GDPR, the Contractor is free to suspend further processing to that extent until liability between the parties has been clarified.

(4) The Contractor may designate to the Client the person(s) authorised to receive instructions from the Client. Where persons authorised to receive instructions are to be designated, these shall be listed in Annex 1. In the event that the persons authorised to receive instructions at the Contractor's premises change, the Contractor shall notify the Client of this in writing.

5. Data Protection Officer of the Contractor

(1) The Contractor confirms that it has appointed a Data Protection Officer in accordance with Article 37 of the GDPR. The Contractor shall ensure that the Data Protection Officer possesses the necessary qualifications and expertise.

(2) The obligation to appoint a data protection officer pursuant to paragraph 1 may, at the Client's discretion, be waived if the Contractor can demonstrate that it is not legally obliged to appoint a data protection officer and the Contractor can demonstrate that operational regulations are in place which ensure the processing of personal data in compliance with statutory provisions, the provisions of this contract and any further instructions from the Client.

6. Contractor's reporting obligations

(1) The Contractor is obliged to notify the Client immediately of any breach of data protection regulations or of the contractual agreements made and/or the instructions issued by the Client, which has occurred in the course of the processing of data by the Contractor or other persons involved in the processing. The same applies to any breach of the protection of personal data which the Contractor processes on behalf of the Client.

(2) Furthermore, the Contractor shall immediately inform the Client if a supervisory authority takes action against the Contractor pursuant to Article 58 of the GDPR and this may also concern an inspection of the processing carried out by the Contractor on behalf of the Client.

(3) The Contractor is aware that the Client may be subject to a notification obligation under Articles 33 and 34 of the GDPR, which requires notification to the supervisory authority within 72 hours of becoming aware of the breach. The Contractor shall assist the Client in fulfilling these notification obligations. In particular, the Contractor shall notify the Client immediately upon becoming aware of any unauthorised access to personal data processed on the Client's behalf. The Contractor's notification to the Client must include, in particular, the following information:

- a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, the categories of personal data concerned and the approximate number of personal data records concerned;
- a description of the measures taken or proposed by the Contractor to remedy the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

7. Obligations of the Contractor to cooperate

(1) The Contractor shall assist the Client in fulfilling its obligation to respond to requests for the exercise of data subjects' rights pursuant to Articles 12–23 of the GDPR. The provisions of Clause 11 of this Agreement shall apply.

(2) The Contractor shall assist the Client in compiling the records of processing activities. The Contractor shall provide the Client with the necessary information in this regard in an appropriate manner.

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

8. Powers of inspection

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

(2) The Contractor is obliged to provide the Client with information to the extent necessary for the performance of the inspection within the meaning of paragraph 1.

(3) The Client may, upon prior notice given with reasonable notice, carry out the inspection within the meaning of paragraph 1 at the Contractor's premises during normal business hours. In doing so, the Client shall ensure that the inspections are carried out only to the extent necessary so as not to unduly disrupt the Contractor's business operations. The parties assume that an inspection will be required no more than once a year. The Client must justify any further inspections by stating the reason. In the event of on-site inspections, the Client shall reimburse the Contractor for the costs incurred, including personnel costs for the supervision and accompaniment of the inspectors on site, to a reasonable extent. The basis for the cost calculation shall be communicated to the Client by the Contractor prior to the inspection.

(4) At the Contractor's discretion, proof of compliance with the technical and organisational measures may, instead of an on-site inspection, also be provided by submitting a suitable, up-to-date certificate, reports or report extracts from independent bodies (e.g. auditors, auditors, data protection officers, IT security departments, data protection auditors or quality auditors) or a suitable certification (e.g. ISO/IEC 27001), provided that the audit report enables the Client, to a reasonable extent, to satisfy itself of compliance with the technical and organisational measures in accordance with Annex 2 to this contract. Should the Client have reasonable doubts as to the suitability of the audit document within the meaning of the first sentence, the Client may carry out an on-site inspection. The Client is aware that an on-site inspection in data centres is not possible, or is only possible in justified exceptional cases.

(5) The Contractor is obliged, in the event of measures taken by the supervisory authority against the Client within the meaning of Article 58 of the GDPR, in particular with regard to obligations to provide information and allow inspections, to provide the Client with the necessary information and to allow the relevant supervisory authority to carry out an on-site inspection. The Client must be informed by the Contractor of any such planned measures.

9. Subcontracting

(1) The Contractor is entitled to engage the subcontractors listed in Annex 1 to this contract for the processing of data on its behalf. A change of subcontractors or the engagement of further subcontractors is permitted subject to the conditions set out in paragraph 2.

(2) The Contractor must select the subcontractor with due care and verify, prior to engaging them, that the subcontractor is able to comply with the agreements made between the Client and the Contractor. In particular, the Contractor must verify in advance and regularly throughout the term of the contract that the subcontractor has implemented the technical and organisational measures required under Article 32 of the GDPR for the protection of personal data. The Contractor shall inform the Client in writing in good time, but no later than 4 weeks prior to the change or the new appointment, in the event of a planned change of a sub-contractor or the planned appointment of a new sub-contractor ("Notification"). The Client shall have the right to object to the change or the engagement of a new sub-processor in writing, stating reasons, within three weeks of receiving the "Notification". The Client may withdraw this objection in writing at any time. In the event of an objection, the Contractor may terminate the contractual relationship with the Client with at least 14 days' notice to the end of a calendar month. The Contractor shall take the Client's interests into account appropriately when determining the notice period. If the Client does not object within three weeks of receiving the "notification", this shall be deemed to constitute the Client's consent to the change or re-appointment of the subcontractor in question.

(3) The Contractor is obliged to obtain confirmation from the Subcontractor that the latter has appointed a data protection officer in accordance with Article 37 of the GDPR, provided that the Subcontractor is legally obliged to appoint a data protection officer.

(4) The Contractor must ensure that the provisions agreed in this contract and, where applicable, any supplementary instructions from the Client also apply to the sub-contractor.

(5) The Contractor must conclude a data processing agreement with the sub-processor that complies with the requirements of Article 28 of the GDPR. Furthermore, the Contractor must impose on the sub-processor the same obligations regarding the protection of personal data as those agreed between the Client and the Contractor. A copy of the data processing agreement must be provided to the Client upon request.

(6) In particular, the Contractor is obliged to ensure, through contractual provisions, that the supervisory powers (Clause 8 of this contract) of the Client and of supervisory authorities also apply to the sub-contractor and that corresponding supervisory rights of the Client and supervisory authorities are agreed. It must also be contractually stipulated that the sub-processor must tolerate these control measures and any on-site inspections.

(7) Services which the Contractor engages from third parties as purely ancillary services in order to carry out its business activities are not to be regarded as subcontracting relationships within the meaning of paragraphs 1 to 6. These include, for example, cleaning services, pure telecommunications services without

specifically relating to services provided by the Contractor to the Client, postal and courier services, transport services, security services. The Contractor is nevertheless obliged, even in the case of ancillary services provided by third parties, to ensure that appropriate precautions and technical and organisational measures have been taken to guarantee the protection of personal data. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and data processing within the meaning of Article 28 of the GDPR if the maintenance and testing concern IT systems that are also used in connection with the provision of services for the Client and if, during maintenance, access can be gained to personal data processed on behalf of the Client.

10. Confidentiality obligation

(1) When processing data on behalf of the client, the contractor is obliged to maintain confidentiality regarding data which it receives or becomes aware of in connection with the contract.

(2) The Contractor shall have familiarised its employees with the data protection provisions applicable to them and shall have bound them to confidentiality.

(3) Proof of the employees' obligations under paragraph 2 must be provided to the client upon request.

11. Safeguarding the rights of data subjects

(1) The Client is solely responsible for safeguarding the rights of data subjects. The Contractor is obliged to support the Client in fulfilling its duty to process requests from data subjects in accordance with Articles 12–23 of the GDPR. In doing so, the Contractor must, in particular, ensure that the necessary information is provided to the Client without delay so that the Client can, in particular, fulfil its obligations under Article 12(3) of the GDPR.

(2) Insofar as the Contractor's cooperation is required for the Client to safeguard data subjects' rights — in particular the rights to access, rectification, restriction of processing or erasure — the Contractor shall take the necessary measures in accordance with the Client's instructions. The Contractor shall, where possible, support the Client with appropriate technical and organisational measures in fulfilling its obligation to respond to requests for the exercise of data subjects' rights.

(3) Provisions regarding any remuneration for additional costs incurred by the Contractor in connection with cooperation with the Client in relation to the exercise of data subjects' rights remain unaffected.

12. Confidentiality obligations

(1) Both parties undertake to treat all information received in connection with the performance of this contract as confidential for an indefinite period and to use it solely for the performance of the contract. Neither party is entitled to use this information, in whole or in part, for purposes other than those specified above or to make this information available to third parties.

(2) The foregoing obligation does not apply to information which a party can prove it has received from third parties without being bound to confidentiality, or which is in the public domain.

13. Remuneration

The contractor's remuneration shall be agreed separately.

14. Technical and organisational measures for data security

(1) The Contractor undertakes to the Client to comply with the technical and organisational measures necessary to ensure compliance with the applicable data protection regulations. This includes, in particular, the requirements set out in Article 32 of the GDPR. The Contractor is certified to ISO/IEC 27001 in the QMSpot business unit (software development and cloud operations) (as of March 2026); the certification covers the entire product lifecycle from development to hosting of the QMSpot product. In the ITSpot business unit, the technical and organisational measures are implemented in accordance with the requirements of the ISO/IEC 27001 standard; for the operational provision of services, ITSpot exclusively uses partners certified to ISO/IEC 27001 (in particular Microsoft Ireland Operations Limited and Hetzner Online GmbH).

(2) The status of the technical and organisational measures in place at the time of conclusion of the contract is attached as Annex 2 to this contract. The parties agree that changes to the technical and organisational measures may be necessary to adapt to technical and legal circumstances. The Contractor shall consult with the Client in advance regarding any significant changes that may affect the integrity, confidentiality or availability of personal data. Measures that entail only minor technical or organisational changes and do not adversely affect the integrity, confidentiality and availability of personal data may be implemented by the Contractor without consultation with the Client. The Client may request an up-to-date version of the technical and organisational measures taken by the Contractor once a year or on justified occasions.

15. Duration of the contract

(1) The contract shall commence upon signature and shall run for the duration of the main contract between the parties concerning the use of the Contractor's services by the Client.

(2) The Client may terminate the contract at any time without notice if the Contractor commits a serious breach of the applicable data protection regulations or of obligations under this contract, if the Contractor is unable or unwilling to carry out an instruction from the Client, or if the Contractor refuses access to the Client or the competent supervisory authority in breach of the contract.

16. Termination

(1) Upon termination of the contract, the Contractor shall return all documents, data and results of processing or use that have come into its possession and that relate to the

contractual relationship, to be returned to the client or deleted at the client's discretion. The deletion must be documented in an appropriate manner.

(2) The Contractor may store personal data processed in connection with the contract beyond the termination of the contract if and to the extent that the Contractor is subject to a statutory obligation to retain such data. In such cases, the data may only be processed for the purposes of complying with the relevant statutory retention obligations. Upon expiry of the retention obligation, the data must be deleted without delay.

17. Right of retention

The parties agree that the Contractor is precluded from invoking a right of retention within the meaning of Section 273 of the German Civil Code (BGB) in respect of the processed data and the associated data carriers.

18. Final provisions

(1) Should the Client's ownership of the data held by the Contractor be jeopardised by actions of third parties (such as attachment or seizure), by insolvency proceedings or by other events, the Contractor must inform the Client without delay. The Contractor shall immediately inform the creditors of the fact that the data is being processed on behalf of the Client.

(2) Any ancillary agreements must be in writing.

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

Date, Client's signature

Date, Contractor's signature

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Tel: +49 261 134 989 10
Email:info@qmspot.com
Web: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Munich Local Court Registration number: HRB: 284652 VAT No.: DE361579292

Managing Directors Timo Müller Peter Scharf

Appendix 1 to the General Terms and Conditions for QMSoftware: Subcontractors

The Contractor shall engage third parties to process data on behalf of the Client, who shall process data on the Contractor's behalf ("Subcontractors").

These are the following companies:

Hosting QMSpot Cloud and Azure OpenAI Service (Managed AI)

Microsoft Ireland Operations Limited

70 Sir John Rogerson's Quay,

Dublin 2, Ireland

Registered in Ireland under number 256796

Activity: Hosting of the QMSpot Cloud infrastructure and provision of the Azure OpenAI Service for managed AI services. Processing takes place in an Azure region within the European Union; the specific region will be agreed and documented prior to the commencement of the contract. Certification: ISO/IEC 27001. Third-country involvement: none.

Hosting of managed backup infrastructure

Hetzner Online GmbH

Industriestraße 25

91710

Gunzenhausen,

Germany

Activity: Provision of server and storage infrastructure for managed backup services. Data centre location: Nuremberg, Germany. Certification: ISO/IEC 27001. Third-country involvement: none.

CRM system

HubSpot, Inc.

25 First Street

Cambridge, MA 02141

USA

Activity: Provision of the CRM system for business communication. Third-country connection: yes (USA); data transfer takes place in compliance with the requirements of the EU-US Data Privacy Framework.

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Tel: +49 261 134 989 10
Email:info@qmspot.com
Website: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Munich Local Court Registration number: HRB: 284652 VAT No.: DE361579292

Managing Directors Timo Müller Peter Scharf

Appendix 2 to the General Terms and Conditions for QMSoftware: Technical and Organisational Measures

The Contractor undertakes to the Client to comply with the following technical and organisational measures, which are necessary to comply with the applicable data protection regulations. The Contractor is certified to ISO/IEC 27001 in the QMSpot business division (as of March 2026). The following measures are implemented across all business divisions and apply equally to the ITSpot business division; for the operational provision of services, ITSpot predominantly and, where possible, uses partners certified to ISO/IEC 27001.

a) Access control

Measures designed to prevent unauthorised persons from gaining access to data processing facilities used to process or utilise personal data:

- Central systems are either located in our own server room or are processed in data centres operated by Microsoft (QMSpot Cloud, Azure OpenAI) or Hetzner (Managed Backup).
- Our own server room is secured by a locking system and only authorised persons have access.
- The server room is accessible only via the internal stairwell. Access is secured by three consecutive doors (1st door: main entrance locking system; 2nd door: physical key (issued only to authorised persons from a safe); 3rd door: physical key (issued only to authorised persons from a safe)).
- The office premises are secured by a locking system. Keys and biometric access credentials are authorised and issued by the IT management.
- Data backups are stored in a different fire compartment to the server room.

b) Access control

Measures to prevent unauthorised use of data processing systems:

- Unique usernames and individual passwords are assigned for all IT systems within the company.
- Multi-factor authentication (MFA) is used for administrative access and for access to cloud services (Microsoft 365, Azure, Hetzner).
- The company network is protected by a firewall with integrated IDS/IPS.
- Both servers and clients are equipped with appropriate virus protection.
- Access to the company's IT systems from a home workstation 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 attempts.
- A password manager is used company-wide.

c) Access control

Measures ensuring that persons authorised to use a data processing system can access only the data covered by their access authorisation, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage:

- As part of the form-based check-in process, individual system authorisations for new employees are approved by the line manager and assigned centrally by operational or IT management.
- The form-based check-out process ensures that, upon an employee's departure, all authorisations are revoked and all IT systems and data storage media are returned.
- With the help of a certified document destruction company (security level P-4), it is ensured that sensitive and personal documents that are no longer required are disposed of securely.

d) Data disclosure control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission, transport or storage on data storage media, and that it is possible to verify and determine to which destinations the transmission of personal data via data transmission facilities is intended:

- The disclosure of personal data takes place exclusively in encrypted form (TLS for data transmission, encryption at rest in data centres).
- In the context of fault analysis and support activities, access to customer systems is always carried out in accordance with the principle of data minimisation and only for documented reasons.
- External data storage devices (USB sticks, external hard drives) are not used for the transport of personal data.
- Transfers to subcontractors (see Appendix 1) are carried out exclusively in encrypted form.

e) Input control

Measures to ensure that it is possible to verify retrospectively whether and by whom personal data has been entered, modified or deleted in data processing systems:

- All central server systems generate log files, which are collected centrally and stored in a format suitable for analysis (SIEM-capable log infrastructure).
- Ad hoc and random evaluations of the log files are carried out by IT Security or the Data Protection Officer.

f) Order control

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

- Data processing agreements in accordance with Article 28 of the GDPR are in place with all subcontractors.

g) Availability checks

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

- All servers are located in dedicated rooms or data centres equipped with an uninterruptible power supply (UPS) with surge protection, smoke detectors, air conditioning and automatic sensors for temperature monitoring.
- Data backups are performed regularly and verified for recoverability. The backup media are stored securely in a separate fire compartment.
- Maintenance contracts are in place for critical systems, which provide for external support in the event of problems.

h) Separation principle

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

Data from different clients is stored and processed in systems that are logically separated from one another. The same applies to data from a single client that is collected and processed for different purposes. In practice, this separation is achieved through the use of different databases, servers and storage accounts.

i) Data protection management

The contractor has appointed an external data protection officer. This person is responsible for data protection management and regularly informs the contractor about current legal developments and the measures to be taken as a result. All of the Contractor's employees entrusted with the processing of personal data are bound by data protection obligations and are instructed in compliance with the regulations. Furthermore, all of the Contractor's employees are bound by confidentiality obligations. The Contractor is certified to ISO/IEC 27001 in the QMSpot business area; the certification is maintained through regular audits.

j) Privacy-friendly default settings

The processing of personal data is always carried out in accordance with the principle of data minimisation. Only data necessary for the respective processes is collected and processed.

QM Software GmbH
Blocksbergstraße 183
66955 Pirmasens

Tel: +49 261 134 989 10
Email:info@qmspot.com
Web: qmspot.com

Bank 1 Saar eG
IBAN: DE92 5919 0000 0126 4670 01
BIC: SABADE5SXXX

Munich Local Court Registration number: HRB: 284652 VAT No.: DE361579292

Managing Directors Timo Müller Peter Scharf