

Attachment 2: Data Protection Provisions

Concluded by and between

The User

- User -

and

QPM Quality Personnel Management GmbH

Am Haferkamp 78

D-40589 Düsseldorf,

represented by the managing director Philipp Schuch or Lisanne Metz

- QPM -

on the processing of personal data on behalf of a controller in accordance with Article 28 (3) of the EU General Data Protection Regulation (GDPR).

§0. Preamble

This annex details the parties' obligations on the protection of personal data, associated with the processing of personal data on behalf of Company as a data controller, and described in detail in the foregoing agreement (hereinafter, the "Agreement"). Its regulations shall apply to any and all activities associated with the Agreement, in whose scope Supplier's employees or agents process Company's personal data (hereinafter, "Data") on behalf of Company as a controller (hereinafter, "Contract Processing")

§ 1. SCOPE, DURATION AND SPECIFICATION AS TO CONTRACT DATA

PROCESSING ON BEHALF

The scope and duration as well as the extent and nature of the collection, processing and use of personal data shall be as defined in the Agreement. Processing on behalf shall include in particular, but not be limited to, the categories of personal data listed in the table below:

Category of data	Purpose of collection, processing, or use of data	Subjects the data relates to
For the general use of gradar for job evaluation / management of a job architecture, among other things.		
First name, surname, business e-mail address, IP address, business phone number (optional)	Access to the Software as a Service on *.gradar.com, communication with the users (e.g. release notes, technical assistance)	Selected employees of the User which are allowed to use the gradar system
Timestamp "Last login"	Use of gradar software, documentation of changes, avoidance of version conflicts	Selected employees of the User which are allowed to use the gradar system
Timestamp Job data: "created, last changed"		
Counter "Number of logins"		
User profile with language, country, and time zone settings		
Job descriptions and commentaries	(optional) upload of job descriptions, documentation of decisions and results on *.gradar.com.	Employees and former employees of the User, provided they are identifiable from the uploaded documents / comments.
Category of data	Purpose of collection, processing, or use of data	Subjects the data relates to

Except where this annex expressly stipulates any surviving obligation, the term of this annex shall follow the term of the Agreement..

§ 2. Scope of Application and Responsibilities

- (1) QPM shall process personal data on behalf of User. The foregoing shall include the activities enumerated and detailed in the Agreement and its scope of work. Within the scope of the Agreement, User shall be solely responsible for complying with the statutory data privacy and protection regulations, including, but not limited to, the lawfulness of the transmission to the QPM and the lawfulness of processing; User shall be the »controller« in accordance with Article 4 no. 7 of the GDPR.
- (2) The User's individual instructions to QPM on Contractual Processing shall, initially, be as detailed in the Agreement. User shall, subsequently, be entitled to, in writing or in a machine-readable format (in text form), modifying, amending, or replacing such individual instructions by issuing such instructions to the point of contact designated by QPM. Instructions not foreseen in or covered by the Agreement shall be treated as requests for changes to the statement of work. User shall, without undue delay, confirm in writing or in text form any instruction issued orally.
- (3) The User shall determine the person(s) authorised to issue instructions in addition to the Company Administrators.
The contractor determines support@gradar.com as recipient of instructions. In the event of a change or longer-term prevention of the contact persons, the contracting party shall be informed immediately and in written or electronic form of the successors or representatives.

§ 3. QPM's Obligations

- (1) Except where expressly permitted by Article 28 (3)(a) of the GDPR, QPM shall process data subjects' Data only within the scope of the statement of work and the instructions issued by User. Where QPM believes that an instruction would be in breach of applicable law, QPM shall notify the User of such belief without undue delay. QPM shall be entitled to suspending performance on such instruction until User confirms or modifies such instruction.
- (2) QPM shall, within QPM's scope of responsibility, organise QPM's internal organisation so it satisfies the specific requirements of data protection. QPM shall implement technical and organisational measures (Attachment 3) to ensure the adequate protection of User's data, which measures shall fulfil the requirements of the GDPR and specifically its Article 32. QPM shall implement technical and organisational measures and safeguards that ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services. User is familiar with these technical and organisational measures, and it shall be User's responsibility that such measures ensure a level of security appropriate to the risk.

QPM reserves the right to modify the measures and safeguards implemented, provided, however, that the level of security shall not be less protective than initially agreed upon.
- (3) QPM shall support User, insofar as is possible for QPM, in fulfilling data subjects' requests and claims, as detailed in chapter III of the GDPR and in fulfilling the obligations enumerated in Articles 32 to 36 of the GDPR.
- (4) QPM warrants that all employees involved in Contractual Processing of User's Data and other such persons as may be involved in Contractual Processing within QPM's scope of responsibility shall be prohibited from processing Data outside the scope of the instructions. Furthermore, QPM warrants that any person entitled to process Data on behalf of Controller has undertaken a commitment to

secrecy or is subject to an appropriate statutory obligation to secrecy. All such secrecy obligations shall survive the termination or expiration of such Contractual Processing.

- (5) With reference to the commissioned processing in question, QPM shall inform the User without delay of any disruptions, suspected data protection violations or other irregularities in the processing of personal data. Article 33 of the GDPR applies to the obligation to notify.
QPM shall take the necessary measures to secure the data and to mitigate possible adverse consequences of the data subjects and shall provide the User with reasonable support.
- (6) QPM shall name to the User the contact details of QPM's data protection officer:
PROLIANCE GmbH
Mr. Dominik Fünkner
www.datenschutzexperte.de
Leopoldstr. 21
D-80802 Munich
Germany
datenschutzbeauftragter@datenschutzexperte.de
- (7) Contact details of QPM as the processor for the purpose of the GDPR:
QPM Quality Personnel Management GmbH
Managing Director
Am Haferkamp 78
D-40589 Düsseldorf
Germany
support@gradar.com
- (8) QPM warrants that QPM fulfils its obligations under Article 32 (1)(d) of the GDP to implement a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- (9) QPM shall correct or erase Data if so instructed by User. Where an erasure, consistent with data protection requirements, or a corresponding restriction of processing is impossible, QPM shall, based on User's instructions, and unless agreed upon differently in the Agreement, destroy, in compliance with data protection requirements, all carrier media and other material or return the same to User. Any processing (and thus also storage) going beyond the processing of the order shall only take place within the framework of the legally prescribed storage periods to which QPM as the contractor is subject.
In specific cases designated by User, such Data can be stored beyond the end of the contract period or handed over. The associated remuneration and protective measures shall be agreed upon separately, unless already agreed upon in the Agreement. Data, data carriers as well as all other materials shall, taking into account the mutual agreement of data and data sets falling under § 1 para. (2) I-III), either be surrendered or deleted after the end of the order at the request of the User.
- (10) Where a data subject asserts any claims against User in accordance with Article 82 of the GDPR, QPM shall support User in defending against such claims, where possible.

§ 4. User's Obligations

- (1) User shall notify QPM, without undue delay, and comprehensively, of any defect or irregularity with regards to provisions on data protection detected by User in the results of QPM's work.

- (2) Section 3 para. 11 above shall apply, mutatis mutandis, to claims asserted by data subjects against QPM in accordance with Article 82 of the GDPR.

§ 5. Enquiries by Data Subjects

- (1) Where a data subject asserts claims based on the rights listed in chapter III §15-22 of the GDPR:

- a) rectification,
- b) erasure
- c) restriction of processing
- d) data portability

against QPM, and where the QPM is able to correlate the data subject to the User, based on the information provided by the data subject, QPM shall refer such data subject to the User.

- (2) Direct contact with the data subject will be limited to this reply.
- (3) QPM shall forward the data subject's claim to the User without undue delay. QPM shall support the User, where possible, and based upon the User's instruction insofar as agreed upon. QPM shall not be liable in cases where the User fails to respond to the data subject's request in total, correctly, or in a timely manner.
- (4) User and QPM shall be liable to data subject in accordance with Article 82 of the GDPR.

§ 6. Options for Documentation

- (1) QPM shall provide the User, at the latter's request, with all information necessary to prove the obligations regulated in this contract and Art. 28 GDPR. In particular, QPM shall provide the User with information on the stored data and the data processing programmes.
- (2) QPM shall provide the User, on request, with appropriate evidence of compliance with the obligations under Art. 28 (1) and (4) GDPR. This proof can be provided by providing documents and certificates that reflect approved rules of conduct within the meaning of Art. 40 GDPR or approved certification procedures within the meaning of Art. 42 GDPR.
- (3) Where, in individual cases, audits and inspections by User or an auditor appointed by User are necessary, such audits and inspections will be conducted during regular business hours, and without interfering with QPM's operations, upon prior notice, and observing an appropriate notice period. QPM may also determine that such audits and inspections are subject to prior notice, the observation of an appropriate notice period, and the execution of a confidentiality undertaking protecting the data of other users and the confidentiality of the technical and organisational measures and safeguards implemented. QPM shall be entitled to rejecting auditors which are competitors of QPM.

In order to assist the User in carrying out an inspection, QPM may charge a fee in the amount of one consulting daily rate. The time and effort involved in an inspection is generally limited to one day per calendar year for the User

- (4) Where a data protection supervisory authority or another supervisory authority with statutory competence for User conducts an inspection, para. 2 above shall apply mutatis mutandis. The execution of a confidentiality undertaking shall not be required if such supervisory authority is subject

Page 6 of 7 to professional or statutory confidentiality obligations whose breach is sanctionable under the applicable criminal code.

§ 7. Subcontractors (further processors on behalf of User)

- (1) Subcontracting relationships within the meaning of this regulation shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which QPM uses, e.g. as telecommunications services, postal/transport services, maintenance and user service such as IT Helpdesk (without access to the gradar platform) 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, QPM is obliged to take appropriate and legally compliant control measures to ensure data protection and data security of the User's data, even in the case of outsourced ancillary services.
- (2) User agrees, that QPM shall use subcontractors as further processors. Prior to the use of new or the replacement of existing subcontractors QPM will inform User in written form (example e-mail). During a period of 3 weeks after receiving this information, User may object the change by giving material reasons related to statutory data protection regulations in written form (example e-mail). If no objection is made within the time limit, the consent to the amendment shall be deemed to have been granted.
- (3) A subcontractor relationship requiring such consent exists if the contractor commissions other contractors to perform all or part of the service agreed in the contract. QPM shall contractually ensure that the provisions agreed in this Contract also apply to subcontractors. The contractor's contract with the subcontractor shall be concluded in writing or in electronic format.
- (4) Subcontractors in third countries shall only be commissioned if the special requirements of Art. 44 et seq. GDPR are fulfilled.
- (5) The contractually agreed services or the partial services described below shall be performed with the involvement of the following subcontractors:

Subcontractor name and address	Description of the individual deliverables
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn, Germany	Hosting of the internet-based software "gradar the job evaluation engine" on *.gradar.com
STRATO AG, Pascalstraße 10, D-10587 Berlin, Germany	Hosting of QPM's websites such as www.qpm.de and its mailserver
Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland	Provision of Microsoft 365 applications such as Exchange (email for gradar.com), Office, Teams, OneDrive on servers in Europe / Germany, with support from service provider / solution partner STRATO AG.
Uniscon universal identity control GmbH, Ridlerstraße 57, 80339 Munich, Germany	Hosting of QPM's Secure File Exchange platform on https://www.idgard.de/

Mailjet SAS, 13-13 bis, rue de l'Aubrac, 75012 Paris, France	Email and SMS sending solution and related services
---	---

TeamDrive Systems GmbH, Max-Brauer-Allee 50, D-22765 Hamburg, Germany	Server-drive for saving and synchronising all files QPM GmbH with end-to-end encryption on servers in Europe
--	--

(6) Core and supporting processes are also documented in the processing directory of QPM.