General Terms and Conditions for using the free Basic Edition of gradar.com

§ 1. Subject matter of this contract

(1) During the contract period (see § 2.) the User is authorised to use the internet based analytical job evaluation system “gradar the job evaluation engine” developed by QPM Quality Personnel Management GmbH in the “Basic” version.

(2) The system is available in the paid editions „Professional“ and „Enterprise“ as well.

(3) Functional scope and pre-requisites of use are specified in **attachments 1** and **4**.

§ 2. Contract Period

(1) The contracts starts with the date of the online registration and has a 3-month duration.

(2) The contract period expands automatically for another 3 months, if the contract is not terminated 4 weeks before expiration.

(3) The user has the right to terminate the contract at any time without giving reasons and without any period of notice. The termination can be declared in text form (e.g. email) or by deletion of the account by the user.

(4) If the e-mail address used for registration is not confirmed within 10 days, or if 210 days pass without log-in, the account will be deleted for reasons of data economy.

(5) QPM is entitled in addition to the time-bound termination to terminate the contract without notice exceptionally when there is good cause. A good cause exists in particular if the user

- uses the contact form to advertise or to send objectionable content,
- attempts to modify in whole or in part, adapt or decompile the software as far as it goes beyond the boundaries of §§ 69d Abs. 3, 69e UrhG,
- severely violates to fulfil his contractual obligations in any other way,
- seriously and culpably violates other legislation when using the website.

(6) In these cases QPM is also entitled to block or delete the user account for a limited time or permanently and to refuse the setup of a new user account.

§ 3. Fees, Due Date, Right of Retention

(1) The annual user fee to be paid by the user amounts to

for the **Basic-Version** with one user: 0,- €

The user fee includes hosting and technical support.

(2) An upgrade from the Basic edition to the Starter, Professional or Enterprise edition is possible at any time.

(3) The user fee does not include consulting or training. These services need to be agreed separately.

(4) If the user falls behind on payment for agreed additional services by more than 14 days, QPM can exercise its right of retention and lock access to the basic-edition of the software.

§ 4. Contact

For support services, the QPM team is available via phone on +49 (0) 211 9367 249-0 or via email on support@gradar.com

gradar the job evaluation engine is a product of:
QPM Quality Personnel Management GmbH
Am Haferkamp 78
D-40589 Düsseldorf

Managing Directors: Philipp Schuch & Lisanne Metz
Registered Office: Düsseldorf
District Court: Düsseldorf, HRB 73656
VAT-ID: DE297336053
Tax-ID: 106/5722/0606

§ 5. Data Protection and Data security

(1) The internet-based job evaluation programme is hosted on servers provided by Telekom Deutschland GmbH, Landgrabenweg 151, D-53227 Bonn, Germany. The internet connection is encrypted with SSL.

(2) All data copied in the clipboard is deleted once the browser connection is terminated or the user logs out or the content is overwritten with something else.

(3) The software evaluates positions. This means that no personal data needs to be transmitted. In the paid versions it is possible (but not required) to save personal data on the server in the comment fields or by uploading job-descriptions.

(4) Data protection provisions for all contract partners are regulated separately in attachment 2.

(5) A list of technical and organisational measures for data protection is provided in attachment 3 of this contract.

(6) By using the basic edition of gradar and confirming the e-mail address, the user agrees that QPM may contact him by phone, e-mail or by means of automated notifications (e-mail). This consent can be revoked at any time informally in writing or by e-mail.

(7) QPM reserves the right to forward the contact data (name, e-mail address, telephone number) of newly registered basic users to a local partner for the purpose of a sales follow-up. The list of partners is published on www.gradar.com/en/implementation-support/implementation-partners

(8) The partners are obliged to use the contact data only for individual, sales-oriented follow-ups and not to store the data in CRM systems or use it for mailing campaigns.

§ 6. Place of Jurisdiction and Applicable Law

(1) If the user is merchant acc. to German law, the place of jurisdiction is Dusseldorf, Germany.

(2) This contract is subject to German jurisdiction to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods, (CISG, April 4th, 1980) and German international civil law.

Attachment 1: Pre-Requisites of Use

§ 1. Technical Pre-Requisites

(1) gradar.com is a web-based application, thus the use requires a web-enabled end device as well as an internet connection on the side of the client.

(2) The internet connection should meet current state of the art technical requirements in terms of stability and bandwidth.

(3) To use the software, knowledge on using internet browsers, simple web applications and office software is required as well as a valid email account.

(4) The client purchases a temporary user licence and is provided with access data by QPM as the provider of the application. Access and use take place by using an internet browser.

§ 2. Access

Access is enabled via an individual Login-ID (email address) and a password through an encrypted SSL connection to www.gradar.com.

§ 3. Updatemanagement

(1) Updates of the gradar application will be published on the server in the case of technical or contentual necessity.

(2) The grading results are saved with a version code. This is to ensure, that the result stays consistent when a position is re-evaluated, even if a new version of the application or the algorithm of the job evaluation has been published.

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" **Timestamp** Job data: "created, last changed" **Counter** "Number of logins" **User profile** with language, country, and time zone settings	Use of gradar software, documentation of changes, avoidance of version conflicts	Selected employees of the User which are allowed to use the gradar system
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 r'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

 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.

Attachment 3: Technical and organisational measures for data protection in accordance with Article 32 of the GDPR

+++ As of November 10th, 2022 +++

hosting partner:

Information on the technical and organisational measures of our hosting partners T-Systems International GmbH and Strato AG can be found on the following websites:

- **T-Systems International GmbH:**
  https://cloud.telekom.de/en/infrastructure/open-telekom-cloud/more/compliance
- **Strato AG:**
  https://www.strato.de/sicherheit/
  https://www.strato-hosting.co.uk/about-us/data-centres/

Both data centres are certified according to ISO 27001, among others.

Our technical and organisational measures are divided into

a) measures in the business operations of QPM GmbH and
b) measures for the operation of the gradar.com platform.

Technical and organisational measures for the business operations of QPM Quality Personnel Management GmbH

Access / entry control

"to prevent unauthorised persons from having access to data processing equipment which processes or uses personal data".

- No public business / external visitors on premise
- Security locks and doors (RC4)
- Windows with 3-fold glazing and timer-controlled electric roller shutters

Access control

"to prevent data processing systems from being used by unauthorised persons

Technical measures:

- Authentication with individual, local user account + password
- Separate administrator account
- Use of Two-Factor-Authentication (2FA) where possible
- Regular updating of all operating systems and locally installed software components
- Use and regular updating of anti-virus software
- Use of firewalls at the LAN / WAN transition
- Encryption of data carriers in laptops / desktops
- Locally installed TeamDrive client for AES256 encrypted data synchronization
- Blocking of auto-installation of foreign / new hardware
- Locking of mobile data media on laptops / desktops
- Encryption of smartphones
- Regular control of all accesses
- Regular internal information security audits
- IT monitoring and antivirus protection via ESET – clients
- Use of intrusion prevention system (short: IPS) and intrusion detection system (short: IDS) - server

Organisational measures:

- Administration and documentation of user authorisations in accordance with the authorisation concept for granting and withdrawing access rights
- Clean Desk Policy
- Password assignment / password rules
- Provision of corporate hardware and software licenses
- Provision of hardware tokens for 2FA
- Installation of new hardware (e.g. via Bluetooth or USB) by IT support only
- Refrain from using mobile data carriers on laptops / desktops
- Level of protection determined by an information security management system (ISMS)

Access control

"to ensure that persons authorised to use a data processing system have access only to the data covered by their access authorisation and that personal data cannot be read, copied, altered or removed by unauthorised persons during processing, use or after storage".

Technical measures:

- Use of document shredders
- No use of and blocking of mobile data media on laptops / desktops
- Logging of accesses to applications, especially when entering changing and deleting data

Organisational measures:

- Reduction of the number of administrators to the minimum
- Password policy incl. length and change
- User rights management by system administrators
- Refrain from using mobile data carriers
- Regular data protection training for all employees

Transfer control

" to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data storage devices and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data communication equipment".

Technical measures:

- Encryption and password protection of individual documents during data exchange with clients, e.g. via idgard.de
- Encrypted TeamDrive for administrative client data with separate access rights
- Encrypted TeamDrive for project-related customer data with separate access rights and Locking of mobile data carriers on laptops / desktops

Organisational measures:

- Exchange of client data exclusively via encrypted connections
- Anonymisation or pseudonymisation of client data, e.g. for remuneration analyses
- Refrain from using mobile data carriers
- Raising employee awareness through regular training on data protection

Data entry control

"to ensure that it is possible to verify and establish a posteriori whether and by whom personal data have been input, altered or removed in data processing systems".

Technical measures:

- Logging of data entry, modification and deletion

Organisational measures:

- Traceability of input, modification and deletion of data through individual usernames

Contractor control

"to ensure that personal data processed under contract can only be processed in accordance with the instructions of the principal".

Organisational measures:

- Selection of the contractor under due diligence (in particular with regard to data security and technical competence)
- Conclusion of sub-contracting agreements with contractors
- Overview and listing of all order processing contracts
- Ongoing review of contractors and their activities for changes in the data processed and protective measures
- Written instructions to the contractor
- Ensuring the destruction of data after completion of the contract
- Obligation of the contractor's employees to maintain confidentiality with regard to data protection

Availability control/integrity

"to ensure that personal data are protected against accidental destruction or loss

Technical measures:

- Fire extinguishing equipment
- smoke detection system
- devices for monitoring temperature and humidity in business premises
- Protective socket strips in business premises
- Uninterruptible power supply (UPS) for local server systems in business premises
- IT monitoring and antivirus protection via ESET – clients
- Use of intrusion prevention system (short: IPS) and intrusion detection system (short: IDS) - server

Organisational measures:

- Storage of data backup in a secure, outsourced location
- Testing data recovery
- Local server systems not under sanitary facilities

Separation control

"to ensure that data collected for different purposes can be processed separately".

Technical measures:

- Separation of company data from administrative client data and project-related data in separate TeamDrive Spaces

Organisational measures:

- Definition and documentation of access rights

Technical and organisational measures for the operation of gradar.com

Access / entry control

"to prevent unauthorised persons from having access to data processing equipment which processes or uses personal data".

- Here we refer to the measures of our hosting partner T-Systems International:
  "No unauthorised access to data processing equipment, e.g: magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems; "

Access control

"to prevent data processing systems from being used by unauthorised persons

Technical measures:

- Authentication of system administrators using E-mail + password + OTP (2FA)
- Optional two-factor authentication (2FA) for enterprise users
- Optional Single Sign-On (SSO) with Google Workspace, Microsoft Azure or Okta for business users
- Use of firewalls
- Encryption of the data storage device of the (*stateless*) application server
- Encryption of databases
- Encrypted communication between application server and database or end user client

Organisational measures:

- Separate user accounts for system administration, business support, personal use
- Management of user authorisations by company administrators

Access control

"to ensure that persons authorised to use a data processing system have access only to the data covered by their access authorisation and that personal data cannot be read, copied, altered or removed by unauthorised persons during processing, use or after storage".

Technical measures:

- Access to server systems only via VPN
- Port sharing reduced to the essentials,
- Separate systems for application server and database
- Encryption of passwords with Bcrypt algorithm
- Client separation in all relevant database tables
- Encryption of the database
- Encryption of communication between application server and database
- Encryption of communication between application server and end user client

Organisational measures:

- Number of administrators reduced to the bare minimum
- User rights management by system administrators
- Two-Factor Authentication (2FA) for System Administrators
- Management of company specific access rights to job evaluation results by company administrators
- Setup and management of company-specific organisational structure (as a basis for access management to job profiles)
- Setup and management of company-specific locations / populations (as a basis for access management to compensation information)
- Regular control and documentation of access management

Transfer control

" to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data storage devices and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data communication equipment".

Technical measures:

- Logical, software-based client separation of the company accounts created with dedicated subdomains
- Encryption of data storage devices and databases and backups
- Setup and management of company-specific organisational structure (as a basis for access management to job profiles)
- Setup and management of company-specific locations / populations (as a basis for access management to compensation information)

Organisational measures:

- Raising awareness and actively supporting company administrators regarding user administration and access management options

Data entry control

"to ensure that it is possible to verify and establish a posteriori whether and by whom personal data have been input, altered or removed in data processing systems".

The application is used to evaluate jobs so that no personal data of job holders need to be transferred. It is possible (but not required) to store personal data on the server side in comment fields or job descriptions.

By default, only the user's name, e-mail address and telephone number are saved.

Organisational measures:

- Traceability of input and modification of jobs as well as results of job evaluation through individual usernames

Contractor control

"to ensure that personal data processed under contract can only be processed in accordance with the instructions of the principal".

Organisational measures:

- Selection of the contractor under due diligence (in particular with regard to data security and technical competence)
- Conclusion of sub-contracting agreements with contractors
- Overview and listing of all order processing contracts
- Ongoing review of contractors and their activities for changes in the data processed and protective measures
- Written instructions to the contractors

Availability control/integrity

"to ensure that personal data are protected against accidental destruction or loss

Technical measures:

- Here we also refer to the measures of our hosting partner T-Systems International:
  " Protection against accidental or deliberate destruction or loss, e.g: Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans.
- Software Design Pattern for automated limitation of data access
- Stateless application servers
- Separation of production and test systems
- Pseudonymised test data

Organisational measures:

- Definition and documentation of access rights

Separation control

"to ensure that data collected for different purposes can be processed separately".

Technical measures:

- Separation of production and test systems
- Pseudonymisation of test data

Organisational measures:

- Definition and documentation of access rights

QPM Quality Personnel Management

gradar the job evaluation engine

Attachment 4: gradar features and pricing 2023

gradar Edition	Basic	Starter Plus	Professional Plus	Enterprise
Annual licence fee (SaaS)	0 €	2.000 €	4.000 €	6.000 €
Job Evaluation	**not stored on server**	**up to 75 jobs**	**unlimited jobs**	**unlimited jobs**
20+ language versions	●	●	●	●
Three gradar career paths: Individual Contributor, Project Management, Management	●	●	●	●
Detailed factor descriptions	○	●	●	●
Global Job Families, incl. detailed definitions and typical activities	○	●	●	●
Company specific grading levels: Create your own levelling system based on gradar grades and configured variables	○	●	●	●
Results Management / Documentation				
Copy and paste: Results copied to clipboard	●	●	●	●
Draft, save and resume: Data stored on server	○	●	●	●
Comment on and document the grading results	○	●	●	●
Upload of jobs and company specific variables	○	●	●	●
Upload of job descriptions and other documents	○	●	●	●
User / Access Management				
Multi-user license (additional user licences are priced at €250/yr)	○ **(1)**	● **(1)**	● **(3)**	● **(6)**
Standard User Types	○	●	●	●
Unlimited number of read-only-users	○	○	●	●
Functional, role-based access management built on default group policies	○	●	●	●
Fully customisable, enterprise-grade access management based on group policies together with *organisational structures* and *locations/populations*	○	○	○	●

● = available ○ = not available *implementation at cost depending on expenditure

Version as of October 19th, 2022

QPM Quality Personnel Management

gradar the job evaluation engine

gradar Edition	Basic	Starter Plus	Professional Plus	Enterprise
Default model based on gradar's global job families	○	●	●	●
Customisation of job specific competencies, based on global model	○	●	●	●
Company specific model based on custom variables and/or competencies	○	○	○	● (*)
Working Conditions				
Custom model to assess the working conditions in an organisation	○	○	● (*)	● (*)
Job Matching				
Job matching to compensation surveys based on gradar's global job families and QPM's compensation survey rosetta stone	○	●	●	●
Localised job matches, to adjust global job matches for locations / populations	○	●	●	●
Custom job matching tables to benchmark job codes / labour agreements	○	○	○	● (*)
Compensation Information				
Upload and integration of third-party data, e.g. compensation surveys that need to be purchased separately	○	●	●	●
Compensation structuring, design and setup of e.g. pay bands	○	●	●	●
Compensation analytics and market comparison				
Upload and administration of employee (salary) data	○	●	●	●
Statistical analysis of actual remuneration with regard to e.g. distribution of salaries (percentiles)	○	●	●	●
Equal pay analysis to determine unadjusted and adjusted pay gap, e.g. by gender	○	●	●	●
Expanded possibilities for remuneration structuring, e.g.	○	●	●	●

● = available ○ = not available *implementation at cost depending on expenditure

Version as of October 19th, 2022

gradar Edition	Basic	Starter Plus	Professional Plus	Enterprise
analysis-based modelling of salary bands				
System Customisation				
Dedicated subdomain	●	●	●	●
Custom logo upload	○	●	●	●
Custom variabels (e.g. job families, regions, etc.) with detailed discription	○	● (3)	● (3)	● (6)
Custom organisational structure (for access management in Enterprise Edition)	○	●	●	●
Organisation specific wording	○	○	○	● (*)
Analytics & Reports				
Cross Comparison	○	●	●	●
Export of tabular grading results / competencies in CSV / XLSX	○	●	●	●
Export of job specific grading results / competencies in DOCX	○	●	●	●
Security				
Hosting in data centre of Telekom Deutschland, certified CSA Star Level 2, Trusted Cloud Data Protection Profile (TCDP) 1.0, ISO 9001, 14001, 22301, 20000, 27001, 27017, 27018, TÜV Trusted Cloud	●	●	●	●
Comprehensive overview of technical and organisational measures for data protection in accordance with Article 32 of the GDPR	●	●	●	●
Two-factor authentication (2FA), which effectively protects a user account from unauthorised access.	○	●	●	●
Single Sign-On (SSO) with Google Workspace, Microsoft Azure or Okta. Use your organisation's identity access management to log users into the gradar app.	○	○	●	●