Data Processing Agreement

Pursuant to Art. 28 (3) p. 1 GDPR

– hereinafter referred to as the **DPA** –

between

Name / Company:

Represented by:
John Doe
Address:
Goldschmiedstreet 1
1111 Vienna
Austria

– hereinafter referred to as **Controller** –

and

Name / Company:
qrd°by
Represented by:
Peter Hlavac
Address:
Deublergasse 37
1210 Vienna
Austria

– hereinafter referred to as **Processor** –

– The Processor and the Controller are hereinafter referred to as (contractual) **Parties**. –

Annexes:

- Annex 1: Security of processing
- Annex 2: Subprocessors

1.

The Subject-Matter of the Contract, Categories of Data, Data Subjects, Nature, Scope and Purpose of the Processing (Art. 28 (3), 30 (2) GDPR)

1.1

The subject of the DPA, the personal data processed within the scope of the assignment (Art, 4 Nos. 1 and 2 GDPR; hereinafter referred to as **Data**), the data subjects concerned and the nature, scope and purposes of the processing, are determined by the following legal relationship(s) between the contractual Parties (hereinafter referred to as the **Principal Agreement**):

Contract for the use of the Software (Software as a Service) *qrd°by* on the basis of the Contractor"s Terms and Conditions.

The provisions of this DPA take precedence over the Principal Agreement.

1.2

Type of data:

- Customer master data (company name, contact person, address, VAT no., e-mail address);
- User and account data (name, e-mail address, cryptographic hash of the password);
- Payment data (account data and/or credit card data);
- Contract data (type of service, fee, term, contract history, payment history);
- Content data that is entered in *qrd°by* by customers/users themselves (QR Codes, Landing Pages);
- Usage data / metadata (server logging, IP address, user agent, request parameters, time stamp).

1.3

Processing of special categories of Data (Art. 9 (1) GDPR):

- No special categories of Data are processed.

1.4

Categories of data subjects:

- Customers, users, business partners of the client;
- Employees of the client;

1.4

Purpose of the processing:

- Providing and operating *qrd°by* (Software as a Service) and related services (computing capacities, databases, software, maintenance and development).

2.

Controller and right of Instruction

2.1

As the person responsible pursuant to Art. 4 No. 7 GDPR, the Controller is responsible for compliance with data protection regulations, in particular the selection of the Processor, the Data transmitted to him and the instructions issued (Art. 28 (3) a, 29 and 32 (4) GDPR).

2.2

The Processor may process Data only within the framework of the Principal Agreement and the instructions of the Controller (including in particular the modification, erasure or restriction of the Data) and only to the extent that the processing is necessary for the agreed purpose, unless the Processor is required to process Data for another purpose by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28 (3) p. 2 a GDPR).

2.3

The Controller has the right to issue additional instructions at any time with regard to the processing of the Data and the security measures.

2.4

If the Processor is of the opinion that an instruction by the Controller violates applicable data protection law, he will immediately point this out to the Controller. If the Processor is of the opinion that an instruction of the Controller violates applicable data protection law, then the Processor is entitled to suspend the execution of the instruction until the Controller confirms the instruction or to reject the instruction in the case of an

obviously illegal instruction.

2.5

The Processor may refuse instructions if they are not possible or unreasonable for the Processor (in particular because compliance with them would impose disproportionate effort or due to a lack of technical possibilities of the Processor). The rejection is only admissible under appropriate consideration of the protection of the Data of the data subjects concerned and entitles the Controller to a termination without notice for a compelling reason of the Principal Agreement, if its continuation is unreasonable for the Controller. If termination takes place before expiry of the agreed contract period of the Principal Agreement, the Controller is obliged to continue paying the agreed remuneration, unless and insofar as the reason for the instruction leading to termination was attributable to the Processor or was in the Processor"s risk sphere.

2.6

If additional instructions of the Controller go beyond the contractual duty of the Processor under the Principal Agreement and are not based on misconduct on the part of the Processor, then the Controller shall reimburse the Processor separately for the additional time and effort arising therefrom.

2.7

The contracting Parties may appoint persons entitled to issue and receive instructions (in particular, if the responsible persons do not already follow from the Principal Agreement) and are obliged to notify the contractual Parties of any changes without delay.

3.

Security of Processing and Related Obligations

3.1

The Processor shall structure the internal organisation in his area of responsibility in accordance with the legal requirements and shall in particular take technical and organisational measures for appropriate security, in particular the confidentiality, integrity and availability of the Controller"s Data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects and ensuring their safeguarding (Art. 28 (3) and 32 - 39 in conjunction with Art 5 GDPR). Technical and organisational measures include in particular physical access control, access to processing systems, control of access to Data and input of Data, Data transfer control, control of orders and assignments, availability and integrity control, guarantee of the principle of purpose/ segregation of data and securing the rights of the affected data subjects.

3.2

The technical and organisational measures on which this DPA is based are set out in Annex 1 "Security of Processing". They may be further improved in the light of technical progress and replaced by adequate protective measures, provided that they do not fall below the safety level of the measures laid down and provided that the Controller is notified of any significant changes.

3.3

The Processor ensures that persons authorised to process the personal data have committed themselves to confidentiality (Art. 28 (3) S. 2 b. and 29, 32 (4) GDPR) and have been instructed in the data protection regulations of the GDPR or are subject to an appropriate statutory obligation of confidentiality.

3.4

The Data and data carriers and all copies made of them within the scope of the DPA shall remain the property of the Controller, shall be carefully stored by the Processor, protected from access by unauthorized third parties and may only be deleted with the consent of the Controller, and then only in accordance with data protection law. Copies of Data may only be made if they are necessary to fulfil the main and secondary contractual obligations of the Processor towards the Controller (e.g. backups).

3.5

If specified by the GDPR or supplementary regulations, in particular national regulations, the Processor shall appoint a data protection officer in accordance with legal requirements and inform the Controller accordingly (Art. 37 to 39 GDPR).

4.

Information Duties and Duties to Cooperate

4.1

The rights of the data subjects are to be fulfilled by the Controller, whereby the Processor supports the Controller according to Art. 28 (3) S. 2 e. GDPR and informs him in particular about the enquiries of the data subjects received by the Processor.

4.2

The Controller must inform the Processor immediately and completely if he detects errors or irregularities with regard to the processing of the Data or with regard to compliance with the provisions of this DPA or relevant data protection regulations.

4.3

In the event that the Processor ascertains facts which justify the assumption that the protection of the Data processed for the Controller has been breached, the Processor must immediately and completely inform the Controller, take the necessary protective measures without delay and assist in the fulfilment of the obligations incumbent on the Controller pursuant to Articles 33 and 34 GDPR.

4.4

Should the security of the Controller"s Data be endangered by third-party actions (e.g. creditors, authorities, courts with seizure, confiscation, insolvency proceedings, etc.) the Processor will immediately inform the third parties that the sovereignty and ownership of the Data lies exclusively with the Controller and, after consultation with the Controller, will, if necessary, take appropriate protective measures (e.g. file objections, applications, etc.).

4.5

The Processor shall inform the Controller without delay if a supervisory authority takes action against the Processor and its activities may affect the Data processed for the Controller. The Processor supports the Controller in the performance of his duties (in particular the provision of information and toleration of inspections) towards supervisory authorities (Art. 31 GDPR).

4.6

The Processor shall provide the Controller with the information necessary for the fulfilment of legal obligations (which may include, in particular, inquiries from data subjects or authorities and compliance with his accountability duties pursuant to Art. 5 (2) GDPR, as well as the carrying out of a data protection impact assessment pursuant to Art. 35 GDPR) and shall provide the necessary information regarding the processing of Data within the scope of this DPA, if the Controller cannot acquire this information himself. The information must be accessible to the Processor and does not have to be obtained from third parties, whereby employees, agents and subprocessors of the Controller are not considered as third parties.

4.7

If the provision of the necessary information and the cooperation go beyond the duties of the Processor according to the Principal Agreement and is not based on misconduct on the part of the Processor, the Controller shall reimburse the Processor separately for the additional work and expenses arising therefrom.

5.

Audits and Inspections

5.1

The Controller has the right to audit the Processor"s compliance with the legal requirements and the regulations of this DPA, in particular the technical and organisational measures, at any time to the required extent (Art. 28 (3) h. GDPR).

5.2

On-site inspections are carried out within normal business hours, must be announced by the Controller within a reasonable period (at least 14 days, except in emergencies) and have to be supported by the Processor (e.g. by the provision of the necessary personnel).

5.3

The inspections are liqrd°byd to the necessary scope and must take into account the Processor"s trade and business secrets as well as the protection of personal data of third parties (e.g. other Controllers or employees of the Processor). Only qualified inspectors are permitted to carry out the inspection, who also can identify themselves and who are bound to confidentiality with regard to the business and trade secrets and processes of the Processor and personal data or other confidential information of third parties.

5.4

Instead of audits and on-site inspections, the Processor may refer the Controller to an equivalent inspection or audit by independent third parties (e.g. neutral data protection auditors), compliance with approved rules of conduct (Art. 40 GDPR) or suitable data protection or IT security certifications in accordance with Art. 42 GDPR. This applies in particular if business and trade secrets of the Processor or personal data or other confidential information of third parties would be at risk due to the audits or inspections.

5.5

If the acceptance and cooperation in the inspections or adequate alternative measures of the Controller exceeds the contractual obligations of the Processor in accordance with the Principal Agreement and are not based on misconduct on the part of the Processor, the Controller shall reimburse the Processor separately for the additional time and effort arising therefrom.

6.

Engagement of Subprocessors

6.1

If the Processor uses the services of a subprocessor in order to carry out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this DPA or other legal act between the Controller and the Processor shall be imposed on the subprocessor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this DPA and the applicable data protection law (in particular with regard to compliance with instructions off the Controller, compliance with technical and organisational measures, provision of information and the toleration of inspections). Furthermore, the Processor must carefully select the subprocessor, check its reliability and monitor its compliance with the requirements of this DPA and the data protection law (Art. 28 (2) and 4 GDPR).

6.2

Without prejudice to any restrictions by the Principal Agreement, the Controller generally agrees that the Processor may engage subprocessors for the processing of the Data.

6.3

The subprocessing relationships already in existence at the time of the conclusion of this DPA are listed by the Processor in Annex 2 Subprocessors and are considered authorized by the Processor.

6.4

The Processor shall inform the Controller of any changes to the subprocessors that are relevant to the processing of the Data. The Controller shall exercise its right to object to the changes or new subprocessors only in compliance with the principles of good faith, fairness and equity.

6.5

Contractual relationships in which the Processor uses the services of third parties as a purely ancillary service in order to carry out his business activities (e.g. cleaning, security or transport services) do not constitute subprocessing within the meaning of the above provisions of this DPA. Nevertheless, the Processor must ensure, e.g. through contractual agreements or information and instructions, that the security of the Data is not endangered and that the requirements of this DPA and the data protection laws are complied with.

7.

Processing in Third Countries

7.1

The processing of Data as contractually specified is carried out only in a Member State of the European Union or in another state party to the Agreement on the European Economic Area (EEA).

7.2

The processing of Data in a third country, also by subprocessors, may only be carried out on documented instructions from the Controller and if the particular requirements of Art. 44 ff. GDPR are met, unless the Processor is obliged to carry out processing in the third country by the law of the Union or the Member States to which the Processor is subject, in which case the Processor shall notify the Controller of these legal requirements before processing, unless the law prohibits such an information on important grounds of public interest (Article 28 (3) S. 2 a. GDPR).

7.3

The authorisation of the Controller for processing in the third country shall be considered to have been given in respect of the processes listed in Annex 2 Subprocessors.

8.

Duration of the Processing, Termination of Contract and Deletion of Data

8.1

This DPA becomes valid upon its conclusion, is concluded for an indefinite period and ends at the latest with the term of the main agreement.

8.2

The right to termination without notice for a compelling reason is available to the contracting Parties, in particular in the event of a serious breach of the provisions of this DPA and applicable data protection law. The extraordinary termination must in general be preceded by a warning of the infringements with a reasonable period of notice, whereby the warning is not necessary if it is unlikely that the objected infringements will be remedied or if they are so severe that it is unreasonable to expect the terminating contracting party to adhere to this DPA.

8.3

After completion of the processing services under this DPA, the Processor will either delete or return all personal data and copies thereof (as well as all documents obtained in connection with the contractual relationship, processing and processing results obtained and datasets), at the choice of the Controller, unless an obligation to store the personal data exists under Union law or the law of the Member States (Art. 28 (3) S. 2 g. GDPR). The right of retention is excluded with regard to the processed Data and the associated data carriers. With regard to the cancellation or return of the Data, the Controller"s rights of information, documentation and inspection shall apply in accordance with this DPA.

8.4

In any case, the obligations arising from this DPA with regard to the Data processed in the assignment shall remain in force even after termination of the DPA.

8.5

If the deletion or the return of the Data exceeds the duties of the Processor according to the Principal Agreement and is not based on misconduct on the part of the Processor, then the Controller shall reimburse the Processor separately for the additional time and effort arising therefrom.

9.

Remuneration

9.1

The remuneration agreed under this DPA also includes an expense allowance for the working hours of the personnel utilized by the Processor as well as necessary expenses (e.g. travel or material costs). If possible, foreseeable and reasonable, the Processor shall inform the Controller of the amount of the remuneration by means of an appropriate estimation.

9.2

If the Processor is entitled to remuneration in accordance with this DPA, the remuneration shall be charged at an hourly rate of EUR 140.00 net. In all other respects, the remuneration provisions of the Principal

Agreement shall apply.

10. Liability

10.1

In the internal relationship with the Processor, the Controller alone shall be responsible to the data subject for the compensation of damages suffered by the data subject due to Data processing or use within the scope of processing instructions which is inadmissible or incorrect in accordance with data protection laws.

10.2

The contracting Parties shall indemnify each other from liability if a contracting party proves that it is in no way responsible for the circumstance by which the damage occurred to a data subject.

11. Final Provisions, Amendments, Form of Communication, Choice of Law, Place of Jurisdiction

11.1

Amendments, additional agreements and addenda to this DPA and its annexes require a written agreement and an express note that this is an amendment or addition to this DPA. This also applies to the waiver of this formal requirement.

11.2

This DPA shall only oblige the Processor in so far as this is necessary to fulfil the statutory obligations, in particular in accordance with Art. 28 ff. GDPR and does not impose any further duties on the Processor.

11.3

Unless otherwise stipulated in this DPA and in the main agreement, communication between the Processor and the Controller within the framework of this DPA (in particular with regard to instructions and provision of information) shall at least be in text form (e.g. e-mail). A lesser form (e.g. oral) may be permissible under the circumstances instead of the text form (e.g. in an emergency situation) but must be confirmed immediately at least in text form. If the written form is required, the written form is understood in the meaning of the GDPR.

11.4

The law of the Federal Republic of Austria shall apply. The exclusive place of jurisdiction for all disputes arising from or in connection with this DPA shall be the Processor''s registered office, provided that the Controller is a merchant, a legal entity under public law or a public law fund or the Controller has no place of jurisdiction in the Federal Republic of Austria. The Processor reserves the right to bring his claims to the legal place of jurisdiction.

Vienna, 2018-05-25, John Doe

Place, Date, Controller

Vienna, 2018-05-25

Place, Date, Processor

Data Processing Agreement

Annex 1 – Security of processing

Technical and organisational measures pursuant to Art. 32 GDPR

1.

Data Protection Management, Rights of Data Subjects, Privacy by Design and Data Protection regarding Employees

Fundamental measures that are aimed at safeguarding the rights of data subjects, immediate reaction in emergencies, the requirements of privacy by design and data protection with regard to employees:

- There is an in-house data protection management system, compliance with which is constantly monitored and evaluated on a case-by-case basis and at least every six months.
- There is a security concept that guarantees the protection of the rights of the data subjects (information, correction, deletion or restriction of processing, Data transfer, revocation & objections) within the legal time limits. It includes forms, instructions and implementation procedures set up, as well as the appointment of the persons in charge of implementation.
- A security concept exists that guarantees an immediate reaction to data breaches (evaluation, documentation, reporting) in accordance with legal requirements. It includes forms, instructions and implementation procedures set up, as well as the designation of the persons in charge of implementation.
- The protection of personal data is already incorporated in the development or selection of hardware, software and processes, taking into account the state of the art, the cost of implementation and the nature, scope, context and purpose of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, in accordance with the principle of data protection by design and by default (Art. 25 GDPR).
- The software used is always kept up to date, as are virus scanners and firewalls.
- The cleaning personnel, security guards and other service providers involved in the performance of ancillary business tasks are carefully selected and it is ensured that they comply with the protection of personal data.

2.

Physical Access Control

Measures to prevent unauthorised persons from accessing data processing facilities with which personal data is processed:

- A "paperless office" is maintained and documents are only stored digitally and only in exceptional cases in paper form.
- With the exception of workstations and mobile devices, no data processing systems are maintained in the company"s own business premises. The Controller"s Data is stored at external hosting providers in compliance with the specifications for processing on behalf of other Controllers.

- Server location: Electronic access control system (personal transponder, division into zones, onboarding process, electric door opener at the entrance door and self-closing outside doors, in the data centre additionally separation lock and alarm for non-closed doors)
- Server location: Specific access regulations for groups of persons (registration of visitors at reception, support of visitors by internal employees, additional access in the computer centre after prior personal registration as well as locked server rooms with access authorisation for authorised personnel only)
- Server location: Surveillance and alarm system (use of an alarm system and connection of security guards, in the event of an alarm monitoring is carried out by on-site security guards, in the data centre additionally video surveillance of the corridors by its operator)

3.

Control of Access to Processing Systems

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

- There is a rights management concept with which the access authorizations of employees, representatives and other persons (e.g. users within the system) are defined and only reach as far as they are required for the specified purpose.
- All data processing systems are password protected.
- There is a password policy that stipulates that passwords must have a minimum length and complexity that corresponds to the state of the art and security requirements.
- Registrations in the processing systems are logged.
- Anti-virus software is implemented.
- Hardware firewalls are implemented.
- Software firewalls are implemented.
- The website and/or access to online software services are protected by an up-to-date TLS/SSL encryption.
- The internal systems are protected against unauthorized access by firewall, user name and password and/or client certificates.
- There is a limitation of failed login attempts to internal systems (e.g. blocking logins or IP addresses).
- If technically supported, two-factor authentication is used.
- Server systems and services with intrusion detection systems are used.
- Server location: Access to internal systems is restricted by firewall or VPN systems
- Server Location: Encryption techniques are used to secure user authentication and administration processes over the Internet.
- Server location: Remote data access to production devices requires a connection to the company network, which is secured by VPN systems.
- Server location: A formal process exists to allow or deny access to resources. Various access protection mechanisms help to provide secure and flexible access.
- Server location: Access rights are assigned or changed on the basis of a rights management concept.

4.

Control of Access to Data and Input of Data

Measures to ensure that those entitled to use a Data processing system can only access the Data covered by their access authorisation and that personal data cannot be entered, inserted, read, copied, modified or removed without authorisation during processing, use and after storage; and measures to enable the processing operations to be subsequently reconstructed:

- There is a rights management concept with which the access authorizations of employees, representatives and other persons (e.g. users within the system) are defined and only extend as far as they are required for the specified use.
- Logging of every single step of Data processing, especially access to applications, especially during Data entry, modification and deletion.
- Logging of every single step, especially access to applications, especially when inputting, changing

and deleting Data.
- Data carriers are stored securely.
- There is a deleting and disposal concept in accordance with DIN 66399 (or an adequate deletion and destruction level) with defined responsibilities and reporting obligations. Employees were informed about legal requirements, deletion periods and specifications for Data deletion or equipment disposal by Data destruction service providers.
- The processing of Data that is not deleted (e.g. as a result of statutory archiving obligations) is restricted by restriction notes and segregation.
- Server location: Access through personalized accounts based on a rights management concept.
- Server location: accesses are logged.
- Server location: System and application log files are stored and administrative activities recorded for input control (logging).

5.

Data transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during transport or storage on data carriers and that it is possible to check and establish to which points personal data is to be transmitted by data transmission devices:

- The persons authorised to hand over data carriers and the persons authorised to receive them shall be determined.
- In the case of physical transport, secure transport containers or packaging are chosen, or the security of the Data is guaranteed by personal supervision, provided that this is sufficient in view of the risks to the Data.
- In the case of remote access to Data, protocol measures ensure that Data transmissions or disclosures are accountable.
- If necessary, possible and reasonable, Data will be passed on in anonymised form or in pseudonymised form.
- E-mail encryption is used if it is possible, reasonable and desired by the communication partner or otherwise considered necessary and/or appropriate.

6.

Control of Orders and Assignments

Measures to ensure that personal data processed on behalf of the Controller can only be processed in accordance with the instructions of the Controller:

- Obligation of employees and representatives to comply with instructions of the Controller.
- Written specification and documentation of the instructions.
- The contractual and legal requirements for the commissioning of subprocessors are complied with by concluding DPAs and securing and monitoring the necessary guarantees.
- It is ensured that Data is returned or deleted after completion of the assignment.

7.

Availability and Integrity Control

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

- Fail-safe server systems and services are used, which are designed in duplicate or in multiple instances, subject to load tests and hardware tests, have DDoS protection and provide an uninterruptible power supply (e.g. RAID, HA power supplies).
- Server systems and services are used that offer a backup system at other locations, or at least in other fire sections, on which the current Data is stored and thus provide an operational system even in the event of a disaster.
- Server systems and services are used which have moisture detectors as well as fire and smoke detection systems and corresponding fire extinguishing devices or fire extinguishers in the EDP

room.
- Server systems and services are used that offer a reliable and controlled backup and recovery concept. Backups are made daily. The backups are encrypted.
- The availability of the data processing systems is permanently monitored.

8.

Guarantee of the Principle of Purpose / Segregation of Data

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Measures to ensure that Data collected for different purposes can be processed separately:
- Where necessary, possible and reasonable, Data is physically separated (e.g. by using different servers). If there is no physical separation, the Data is separated logically (e.g. in different databases or by marking with appropriate purpose attributes or Data fields).
- An unauthorized access to the Data is prevented by a rights management concept.
- In the case of pseudonymised storage, the identification keys are stored separately from the Data and secured against unauthorised or unintended linkage during processing.
- Productive and test systems are separated.

9.

Authorized persons

- Only the administrators installed by the the controller are authorized to access all systems.
- Customers using *qrd°by* have non-administrative access to their customer area and the data processed for them within the scope of a user authorization. There can also be tiered authorizations for customers. Data Processing Agreement

Data Processing Agreement

Annex 2 – “Subprocessors”

GEVEST Steuer- und BetriebsberatungsgmbH - Schottenfeldgasse 40/8 - 1070 Vienna - Austria
Purpose: financial administration, tax consultants

DI Kurz Klaus e.U. - Untere Weißgerberstr. 28/11 - 1030 Vienna - Austria
Purpose: Hosting, infrastructure and platform services, computing capacity,
storage and database services, security services, technical maintenance services