Data Processing Contract

Agreement in accordance with Art 28 GDPR for the processing of data on behalf of a controller

Between

Company	
Street/no.:	
Place/postal code:	

– Controller – hereinafter referred to as the **Client** –

And

Egoditor GmbH
Am Lenkwerk 13
Bielefeld 33609

– Processor – hereinafter referred to as **Contractor** or **Egoditor**

§ 1 Scope and duration of order processing

(1) Scope
The scope of order processing is the provision of web-based
software for QR code campaigns ("QR Code Generator PRO"). Other details are as set out in the Main Contract (hereafter: "Performance Agreement") between the parties that is based on the Client's Terms and Conditions and on its Price List.

The precise functionality of the software and hence the service may change over time and may also be dependent on the specific performance agreed between the Client and the Contractor.

(2) Duration
The duration of this order processing (term) is identical to the duration of the Performance Agreement.

§ 2 Specification of the order details

(1) Within the framework of the order, personal data is

- collected
- recorded
- organised
- stored
- readout
- retrieved
- used
- disclosed
- reconciled
- erased

Namely for the following purpose:

- Generation of QR codes, based on the entered data. The entered data may be personal data.
- Caching of the entered data for performance reasons
- Long-term (no longer than until the end of the Performance Agreement) storage of the data saved by the Client for easier reusability by the Client.
- Publication on websites (e.g. vCardPlus, event pages) and hosting of such websites
- Integration of social media plugins on these websites
- Tracking by means of the generated QR codes
- Maintenance and troubleshooting. It is not possible to exclude the possibility that the Contractor/Contractor's employees will be granted access to this personal data during this process. However, the processing of this data is not the purpose of this activity and is performed only to the extent necessary to carry out maintenance and troubleshooting.

The provision of the contractually agreed data processing takes place exclusively in a Member State of the European Union, another country that is a signatory to the Agreement on the European

Economic Area or a third country, whereby the Contractor ensure that processing in the third country is permitted in accordance with Art. 44–50 GDPR.

(2) Types of data
Processing applies to the following types/categories of personal data:

- personnel master data
- communication data (e.g. telephone, email)
- tracking data
- usage data
- geo-data (transmitted by IP location finding)

(3) Categories of data subjects
The categories of data subjects include, in particular:

- the Client's customers and employees
- prospective customers, including:
    - visitors to the Client's website
    - persons that scan/click on the Client's QR codes or short URLs that are created using the Contractor's software
- subscribers
- visitors to the Client's website
- suppliers

(4) As the Contractor provides the Client with a web-based application, the type of data processed and the categories of data subjects depend on the data entered by the Client. The Client shall ensure that the data entered has been lawfully collected and may be processed by the Contractor.

§ 3 Technical and organisational measures

(1) Before the commencement of processing, the Contractor shall document the implementation of the necessary technical and organisational measures set out prior to the award of the order, in particular with regard to the detailed execution of the order, and present these documented measures to the Client for inspection. If accepted by the Client, the documented measures become the foundation of the order. Insofar as the inspections/audits by the Client show the need for amendments, such amendments must be implemented by mutual agreement.

(2) The Contractor shall establish the security in accordance with Art. 28 paragraph 3 letter c and letter e, half-sentence 1 GDPR, Article 32 GDPR in particular, in conjunction with Art. 5 paragraphs 1 and 2 GDPR. Overall, the measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems and services. The state-of-the-art, the implementation costs, the nature, scope and purposes of processing, as well as the various probabilities of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 paragraph 1 GDPR must be taken into account;
refer to Annex 1.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, it is permissible for the Contractor to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

§ 4 Rectification, restriction and erasure of data

(1) The Contractor may not on its own authority rectify, erase or restrict the processing of data which is processed in the order, but only upon documented instructions from the Client. Insofar as a data subject contacts the Contractor directly concerning rectification, erasure or restriction of processing, the Contractor shall immediately forward the data subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access must be ensured directly by the Contractor in accordance with documented instructions from the Client.

§ 5 Quality assurance and other duties of the Contractor in accordance with Art. 28 paragraph 3 sentence 1 GDPR

In addition to complying with the rules set out in this order, the Contractor must comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Contractor ensures, in particular, compliance with the following requirements:

a) Appointment of a data protection officer to perform duties in accordance with Art. 38 and 39 GDPR. The contact details of this person must be posted at an easily retrievable location on the Contractor's website.

b) Maintaining confidentiality in accordance with Art. 28 paragraph 3 sentence 2 letter b GDPR. The Contractor will entrust only such employees with the data processing outlined in this order who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work.

c) The Contractor and any person acting under its authority who has access to personal data shall not process that data unless on instructions from the Client (Art. 29, Art. 32 paragraph 4 GDPR), which includes the powers granted in this Contract, unless required to do so by law.

d) Implementation of and compliance with all technical and organisational measures necessary for this order in accordance with Art. 28 paragraph 3 sentence 2 letter c, Article 32 GDPR; refer to Annex 1.

e) The Client and the Contractor (and, where appropriate, their representatives) shall cooperate, on
request, with the supervisory authority in performance of their tasks (Art. 31 GDPR).

f) Immediate information of the Client with regard to any inspections and measures conducted by the supervisory authority, insofar as they relate to this order. This also applies insofar as the Contractor is under investigation by a competent authority in connection with infringements to

any criminal law or administrative rule regarding the processing of personal data in connection with the processing of this order.

g) Insofar as the Client is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party, or any other claim in connection with the order processing by the Contractor, the Contractor shall make every effort to support the Client.

h) The Contractor shall regularly check its internal processes and the technical and organisational measures in order to guarantee that the processing that takes place in its area of responsibility is in compliance with the applicable requirements of data protection laws and that the rights of the data subjects are protected.

i) Verification of the implemented technical and organisational measures vis-à-vis the Client within der framework of its powers of inspection conferred in § 7 of this Contract.

§ 6 Subcontracting in accordance with Art. 28 paragraph 3 sentence 2 letter d GDPR in conjunction with paragraphs 2 and 4 GDPR

(1) Subcontracting for the purpose of this provision are taken to mean services which relate directly to the provision of the main service. This does not include the following ancillary services: e.g. telecommunication services, postal/transport services, maintenance and user support services 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 equipment. The Contractor, however, is obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Contractor may commission subcontractors (additional contract processors) only after the Client's prior explicit, written or documented consent.

a) The Client agrees to the commissioning of the subcontractors named in Annex 2 on the condition of a contractual agreement in accordance with Art. 28 paragraphs 2–4 GDPR:

b) Outsourcing to subcontractors and/or changing the existing subcontractor is permitted in the case of the Client's prior, general and written consent when:

- the Contractor notifies the Client of such outsourcing in writing or in text form in advance; and
- the Client has not objected to the planned outsourcing in writing or in text form to the Contractor by the date of
- the planned handing over of data; and
- the outsourcing has been based on a contractual agreement in accordance with Art. 28 paragraphs 2–4 GDPR.

c) Where the Client objects to the change of subcontractor or outsourcing to a subcontractor, the Contractor is entitled to terminate the Performance Agreement with the Client within a period of two weeks to the end of the calendar month.

(3) The transfer of the Client's personal data to the subcontractor and the subcontractor's commencement of data processing are only permitted if all requirements for subcontracting are met.

(4) Insofar as the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall take suitable measures to ensure permissibility under data protection laws. The same applies insofar as service providers in the meaning of § 8 paragraph 1 sentence 2 of this Contract are to be used.

(5) Further outsourcing by the subcontractor in the case of the Client's prior, general, written consent requires the express consent of the Main Contractor (at least in text form). All contractual provisions in the contract chain must also be imposed upon the other subcontractor.

§ 7 Client's supervisory powers in accordance with Art. 28 paragraph 3 sentence 2 letter h GDPR

(1) The Client has the right, after consultation with the Contractor, to carry out inspections or to have them carried out by an auditor to be appointed in each individual case. It has the right to convince itself of the compliance with this Agreement by the Contractor in its business operations by means of random checks, which as a rule must be notified in good time.

(2) The Contractor shall ensure that the Client is able to verify compliance with the obligations of the Contractor in accordance with Art. 28 GDPR. The Contractor undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the technical and organisational measures.

(3) Evidence of such measures, which do not only concern the specific order, may be carried out by

- compliance with approved codes of conduct in accordance with Art. 40 GDPR;
- certification according to an approved certification procedure in accordance with Art. 42 GDPR; or
- current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data privacy auditor, quality auditor); or
- suitable certification by IT security or by data protection auditing (e.g., in accordance with BSI-Grundschutz).

(4) Where the Contractor facilitates inspections by the Client, the Contractor is entitled to claim remuneration.

§ 8 **Notification of Contractor's breaches in accordance with Art. 28 paragraph 3 sentence 2 letter f GDPR**

(1) The Contractor shall assist the Client in complying with the obligations referred to in Articles 32 to 36 GDPR concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations. These include, among others:

a) ensuring an appropriate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing, as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities, and that enable an immediate detection of relevant infringement events;

b) the obligation to report a personal data breach immediately to the Client;

c) the duty to assist the Client with regard to the Client's obligation to provide information to the data subject concerned and to immediately provide the Client with all relevant information in this regard;

d) supporting the Client with its data protection impact assessment;

e) supporting the Client with regard to prior consultation of the supervisory authority.

(2) Where support services are not included in the description of services or do not result from misconduct on the part of the Contractor, the Contractor is entitled to demand remuneration.

§ 9 Client's authority to issue instructions in accordance with Art. 28 paragraph 3 sentence 3 GDPR

(1) The Client shall confirm verbal instructions without undue delay (at least in text form).

(2) The Contractor shall inform the Client immediately if it considers that an instruction violates data protection regulations. The Contractor is then entitled to suspend execution of the relevant instructions until the Client confirms or changes them.

§ 10 Erasure and return of personal data in accordance Art. 28 paragraph 3 sentence 2 letter g GDPR

(1) Copies or duplicates of the data must not be produced without the knowledge of the Client. Excepted from this are backup copies as far as they are necessary to ensure orderly data processing, as well as data required to meet legal requirements for the retention of data.

(2) After completion of the contractual works or earlier upon request by the Client – no later than at the end of the Performance Agreement – the Contractor shall return any documents received, prepared results of processing and use, as well as data sets if related to the contractual relationship with the Client, or destroy such records in accordance with the data protection provisions and subject to the Client's prior consent. The same applies to test and rejected materials. The erasure log must be submitted to the Client on request.

(3) Documentation serving as evidence of the data processing in accordance with the order must be kept by the Contractor as set out in the respective retention periods, even beyond the end of the contract. The Contractor may hand this over to the Client at the end of the contract for the purpose of exoneration.

§ 11 Rights of the data subjects in accordance with Art. 28 paragraph 3 sentence 2 letter e half-sentence 2 GDPR.

The Contractor shall fulfil its obligation to respond to requests for the assertion of the rights of data subjects as set out in Chapter III GDPR. In particular, these rights are:

- Art. 13 GDPR Duty to inform and right to information where personal data is collected from the data subject.
- Art. 14 GDPR Duty to inform if personal data is not collected from the data subject.
- Art. 15 GDPR Rights of the data subject to information
- Art. 16 GDPR Right to rectification.
- Art. 17 GDPR Right to cancellation ('right to be forgotten').
- Art. 18 GDPR Right to restriction of processing.
- Art. 19 GDPR Notification obligation regarding rectification or deletion of personal data or restriction of processing.
- Art. 20 GDPR Right to data portability.
- Art. 21 GDPR Right to object.
- Art. 22 GDPR Right not to be subject to a decision based solely on automated processing.

§ 12 Miscellaneous

(1) Both parties undertake to maintain confidentiality in regard to the business secrets and data security measures of the other Party of which they acquire knowledge within the framework of their contractual relationship. This undertaking survives the end of the Contract. Where there are doubts as to the confidentiality of particular information, this information must be treated confidentially until it is released by the other Party in writing.

(2) Where measures by third parties (for instance seizure or confiscation), insolvency or composition proceedings or other circumstances place property of the Client that is in the possession of the Contractor at risk, the Contractor must inform the Client without undue delay.

(3) Ancillary agreements must be made in writing.

(4) A right of retention as set out in § 273 BGB (German Civil Code) is explicitly excluded with regard to the

data processed as part of the order, as well as to the associated data storage media.

(5) This Agreement also applies insofar and inasmuch as the competent authorities or a court of law deviate
mutually from accepting joint responsibility of the contractual parties in accordance with Art. 26 GDPR.

(6) The invalidity of individual sections of this Agreement will not affect the validity of the Agreement as a whole.

BIELEFELD, 06.02.2019	
Place, date	Place, date

Contractor	Client

Annex 1: Technical and organisational measures by the Contractor

The following describes the technical and organisational measures implemented by the Contractor for data security in the meaning of Art. 32 GDPR. The necessary technical and organisational measures were implemented for contract data processing to ensure a level of security appropriate to the risk, with due consideration of:

- the state-of-the-art
- the costs of implementation
- the scope
- the nature
- the context
- the purposes of processing
- the likelihood of occurrence
- the severity for the rights and freedoms of the data subjects associated with the processing.

For security reasons, only a general description is provided.

§ 1 Confidentiality

Access control

The Contractor guarantees with the following measures that unauthorised persons are denied access to the data processing equipment with which personal data is processed or used (access control).

- Keys are assigned exclusively to authorised persons in accordance with a defined process, which, through use of electronic keys with appropriate central assignment of permissions, provides for the issue, i.e. withdrawal of access rights to rooms both at the beginning of the working relationship as well as at the end of the working relationship.
- Only the landlord and the tenants of the office space have access to the office building.
- Only authorised persons, i.e. authorised employees, have access to the relevant rooms. Visitors are always accompanied by authorised employees.
- Only authorised employees have access to the locked server rack and router/firewall.
- Personal data belonging to the Client is not ordinarily stored on the office premises of Egoditor. All of the IT systems relating to the order are located in the data centers used by Egoditor.

Access control

The following measures have been implemented to prevent unauthorised third parties from using the data processing systems (computers):

- Access to the IT systems is only possible if the user has appropriate access permission. Access permissions are only assigned when approved by management.
- All systems are protected by passwords comprising at least 8 characters, whereby the passwords consist of upper and lower case letters, numerals and special characters and are protected by two-factor authentication when possible.
- Encrypted connections are always used for remote access to Egoditor IT systems.
- All servers are protected by firewalls that are maintained and supplied with all updates and patches.
- All employees are instructed to lock their IT systems when absent from their workstations. The IT system is locked automatically after more than 10 minutes of inactivity.
- Passwords are always stored in an encrypted form.

Access control

The Contractor guarantees that persons authorised to use its data processing systems are only able to access the data for which they have permissions.

- Data is only released to authorised persons.
- Exclusively the administrators assign permissions for Egoditor IT systems and applications.
- Employees are inducted in the systems with due consideration of their individual access permissions for personal data.
- A firewall is configured to protect against unauthorised internal and external access.
- Permissions are assigned exclusively based on the need-to-know principle. Therefore, access permissions for data, databases or applications are only assigned to persons that maintain the data, databases or applications, i.e. that are involved in their development.
- Destruction of data storage media and hard copy is managed by a service provider that guarantees destruction in accordance with DIN 66399.
- Employees are strictly forbidden from installing unauthorised software on the IT systems.
- All server and client systems are regularly updated with security updates.

Separation

The following measures guarantee that data collected for different purposes can be stored separately:

- Separate processing and/or storage of data is ensured for data that is processed for different purposes.
- A system of graded access permissions have been installed for employees in the IT (administration) and support departments.

Pseudonymization, encryption and anonymization

The following measures guarantee that personal data is processed such that the data cannot be associated with a specific data subject without recourse to additional information, provided this additional information is stored separately and is subject to suitable technical and organisational measures.

- Encrypted connections are always used to access server systems for administrative purposes.
- Where possible, IP addresses are anonymised or masked.

§ 2 Integrity

Input control

The following measures are suitable for the downstream review and identification of whether and by whom personal data was entered, modified or erased in data processing systems:

- The input, modification and deletion of data is logged at database level.
- It is the responsibility of the Contractor, for the duration of the Contract, to enter any personal data into the QR code software with which it has been provided and in particular to use exclusively suitable third parties for this purpose (e.g. web agencies, administrators). The Contractor's employees are always prohibited from entering, modifying or erasing this data.
- Where the contract data processor (Egoditor) is required to remove or to block information for compliance with legal obligations (e.g. in the case of using tele-media systems or electronic communications services kept by the customer on the IT systems on behalf of third parties), this blocking, i.e. removal of content will be logged.

Transfer control

The following measures guarantee that unauthorised persons cannot read, copy, modify or remove personal data during electronic transmission or during its transport or storage on data storage media.

- Only encrypted connections are used for server administration. The Client's data is not transferred to third parties or is only transferred to Egoditor's order processors when required due to system organisation. Excluded from this are cases in which Egoditor is obliged to disclose data for compliance with legal obligations or by court order.
- All employees working on a customer project are instructed on the permissible use of data and the terms that apply to the transfer of data.
- As far as possible data is transferred to recipients in encrypted form.
- The use of personal data storage media is explicitly prohibited for Egoditor employees.
- Egoditor employees receive regular training in data protection issues. All employees have been obliged to treat personal data confidentially.

§ 3 Availability and resilience

The following measures guarantee that the data processing systems used
work faultlessly at all times and that personal data is protected from accidental destruction or loss.

- The data centers used by Egoditor have backup uninterruptible power supply (USP), air conditioning in the server rooms, devices to monitor temperature and humidity in the server rooms, fire and smoke alarm systems and backup systems.
- A comprehensive fire and early warning system is in operation. Incremental backups of all data on Egoditor server systems are produced at least daily, and "full" backups are created weekly.

§ 4 Data protection management

- The employees receive regular training.
- The data protection measures are regularly reviewed and adapted with regard to their effectiveness.
- In particular, it is ensured that all data protection incidents are recognised by all employees and reported without undue delay. Incidents are analysed immediately. Where this affects data that is processed on behalf of customers, it must be ensured that the customers are informed of the nature and scope of the breaches without undue delay.
- Where data is processed for proprietary purposes, and where the conditions of Art. 33 GDPR are satisfied, a notification is sent to the supervisory authority within 72 hours after awareness of the incident.

§ 5 Order control in the case of subcontracting to third parties

The following measures guarantee that order processing of personal data only takes place in accordance with the instructions of the Client.

- Egoditor has appointed an external data protection officer.
- Following prior review, a data processing agreement will be concluded in accordance with the terms of the applicable data protection laws whenever external service providers are contracted. Contractors are audited regularly over the term of the contractual relationship.

Annex 2: Subcontractors

The Contractor uses the services of the following subcontractors that process data on its behalf.

Subcontractor	Address/country	Service
Amazon Web Services Inc.	410 Terry Avenue North Seattle, WA 98109, United States	Storage and administration of backups. (Amazon Glacier) Hosting and back-end services. (Amazon Web Services (AWS))
Crazy Egg, Inc.	16220 E. Ridgeview Lane, La Mirada, CA 90638, United States	Heat mapping services
Google Analytics	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	User statistics
Google Fonts	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	Web fonts
Google Maps	Google LLC, 1600, Amphitheatre Parkway, Mountain View, CA 94043, USA	Maps plug-in
Google Optimize	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	A/B testing
Google Tag Manager	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Online tag manager for web analysis
Intercom Inc.	55 2nd Street, 4th Floor, San Francisco, CA 94105, United States	Integration of communication systems (email, push notifications and live chats) with **Egoditor** / qr-code-genera-tor.com.

Mixpanel	405 Howard St., 2nd Floor, San Francisco, CA 94105, United States	Web analysis services
SupportYourApp Inc.	11 Kryvorizhska St., Kyiv 03118 Ukraine	Remote support and development services
tecRacer GmbH & Co. KG	Vahrenwalder Str. 156 30165 Hannover, Germany	Database and server management and maintenance
The Rocket Science Group, LLC. (Mailchimp/Mandrill)	512 Means Street, Suite 404, Atlanta, GA 30318, United States	Newsletter mailings and transactional emails