Agreement

on the Processing of Personal Data

within the meaning of Article 28 (3) EU-Regulation 2016/679 (“GDPR”)

- Data Processing Agreement -

Between

Company	
Street, house number	
ZIP-Code, City, Country	

- person responsible within the meaning of Art. 4 no. 7 GDPR -

- hereinafter referred to also as "Controller" -

and

Bitly Europe GmbH
Am Lenkwerk 13
Bielefeld 33609
Germany

- processor within the meaning of Article 4 no. 8 GDPR -

- hereinafter referred to also as "Processor" or “Bitly Europe” -

- collectively referred to below as "Parties" -

The Controller (responsible for the processing) and the Processor conclude the following contract for data processing pursuant to Art. 28 GDPR. Based on the contractual relationship existing between the Parties ("Main Agreement"), Bitly Europe processes personal data for the Controller. The resulting data protection rights and obligations of the Parties are specified in this Data Processing Agreement. The annexes to this contract are an integral part of the agreement. The provisions made must apply to all services which the processor provides for the Controller and all associated activities which result in and may result in the processing of personal data.

§ 1 | Subject and Duration of Data processing

[1]Processor is providing the software as a service product QR Code Generator, accessible via the website https://www.qr-code-generator.com/ or application programming interface (API) to the Controller. [2]Within the platform of the processor, QR Codes can be created, designed, managed, and tracked for mobile campaigns. [3]The scope of data processing is the provision of web-based software for QR code campaigns ("QR Code Generator Pro"). [4]Further Details of the subject matter and the duration of the processing are defined in the Main Agreement between the Parties. [5]The precise functionality of the software and hence the service may change over time and may also be dependent on a specific service level agreement (SLA) between the Parties. [6]This contract is legally dependent and shares the legal fate of the Main Agreement. [7]A termination of the Main Agreement automatically causes a termination of this Agreement. [8]The Parties are aware that no (further) data processing may be carried out without the existence of a valid data processing agreement. [9]An isolated orderly termination of this Agreement is excluded.

§ 2| Specification of the Data Processing

(1) Type(s) and purpose(s) of Data Processing

[1]The processing of personal data is not to be qualified as the main object or purpose, but rather as a reflexive, unavoidable side effect of the provision of services by the processor. [2]Notwithstanding the above, it is not excluded that the Processor processes personal data within the meaning of Art. 4 No. 2 GDPR in order to be able to create the QR Codes and generate marketing campaigns. [3]Overall, the data processing fulfills the following purposes:

- Generation of QR Codes, based on the entered data (the entered data can be considered 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 and
- Maintenance and troubleshooting (it is not possible that the Controller or the Controller's Employees will be granted access to this personal data during this process. However, the processing of the data concerned is not the purpose of this activity and is performed only to the extent necessary to carry out maintenance and troubleshooting.

[3]In particular, the processing includes the collection, recording, organization, storage, reading out, use, disclosure by transmission, dissemination, or any other form of provisioning, reconciliation, deletion or erasure.

(2) Place of Processing

[1]The provision of the contractually agreed data processing generally takes place in a member state of the European Union (EU) or in another contracting state to the Agreement on the European Economic Area (EEA). [2]The Processor is nonetheless permitted to process personal data outside the EEA in compliance with the provisions of this contract if he informs the Controller in advance of the place of data processing and if the requirements of Art. 44 et seq. GDPR are met.

(3) Type(s) of data

The subject of the processing of personal data are the following data types / categories:

- People Master Data (Key Personal Data)
- Contact / Communication Data (e.g., telephone number, email address)
- Tracking data
- Usage data
- Geo-data (transmitted by IP location finding)

(4) Categories of Data Subjects

The categories of persons potentially affected by data processing activities include:

- Controller's customers and employees
- Persons that scan/click on the Controller's QR codes or short URLs that are created using the processor's platform

As the Processor provides the Controller with a web-based platform, the type(s) of data processed, and the categories of data subjects depend on the data entered by the Controller. The Controller shall ensure that the data entered has been lawfully collected and can lawfully be processed by the processor.

§ 3 | Technical and Organizational Measures

(1) [1]The Processor must document the implementation of the Technical and Organizational Measures (TOMs) set out prior to the award of the contract and prior to the start of processing, in particular regarding the specific execution of the processor, and hand them over to the Controller for review. [2]The Controller hereby accepts the Technical and Organizational Measures set out in Annex 1 to this Agreement. The documented measures become the basis of the contract. [3]If an inspection or audit of the Processor proves a need for adjustment, it shall be implemented in accordance with this Agreement.

(2) [1]The Processor shall establish the security in accordance with Art. 28 (3) lit. c and lit. e and Art. 32 GDPR, in particular in conjunction with Art. 5 (1) and (2) GDPR. [2]The actions to be taken are data security measures and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems and services. [3]Thereby, the state of the art, the implementation costs and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR must be considered. [Details in Annex 1].

(3) [1]The Technical and Organizational Measures are subject to technical progress and further development. [2]In that regard, the Processor is allowed to implement adequate alternative measures. [3]In doing so, the security level of the specified measures must not be reduced. [4]Substantial changes are to be documented.

§ 4 | Quality Assurance and other Obligations of the Processor pursuant Art. 28 (3) (1) GDPR

In addition to complying with the provisions of this Agreement, the Processor has his own statutory obligations of a processor; in particular, he ensures compliance with the following requirements:

a) [1]To the extent required by law, the Processor appoints a competent and reliable person as data protection officer, who carries out his activity in accordance with Art. 38, 39 GDPR. [2]The contact details of the named data protection officer are shared with the Controller for the purpose of direct contact. [3]All changes in the person of the data protection officer or the contact person must be reported to the Controller without delay.

b) In accordance with Art. 28 (3) (2) lit. b GDPR the Processor shall procure that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory secrecy obligation and have been previously familiarized with the data protection regulations relevant to them.

c) The Processor and any person subordinate to the Processor who has access to personal data may process this data exclusively in accordance with the instructions (Art. 29, 32 (4) GDPR) of the Controller, including the powers granted in this Agreement unless they are required by law to process.

d) The Processor guarantees the implementation and compliance with all TOMs required for this Agreement in accordance with Art. 28 (3) (2) lit. c, Art. 32 DSGVO [details in Annex 1].

e) The Controller and the Processor (and their representative if necessary) work together with the supervisory authority on request to fulfill their duties (Art. 31 GDPR).

f) [1]The Processor undertakes to inform the Controller without undue delay of any supervisory acts and measures which are pertinent to the processing insofar as they relate to this Agreement. [2]This also applies if a competent authority investigates the processing of personal data by the Processor in the context of an administrative offense or criminal proceedings.

g) Insofar as the Controller himself is subject to inspection by the supervisory authority, an administrative offense or criminal procedure, the liability claims of a data subject or a third party or any other claim in connection with the processing by the Processor, the Processor shall use his best efforts to support the Controller.

h) The Processor shall regularly review his internal processes and TOMs to ensure that the processing within his area of responsibility complies with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.

i) The Processor guarantees the verifiability of the Technical and Organizational Measures taken towards the Controller within the scope of his control powers pursuant to § 6 of this Agreement.

§ 5 | Conditions for Subcontracting pursuant to Art. 28 (3) (2) lit. d GDPR in conjunction with Art. 28 (2) and (4) GDPR

(1) [1]Subcontracting refers to adding services directly related to the provision of the main service. [2]Not as subcontracting, however, such services are to be regarded as those which the Processor claims from third parties as a mere ancillary service in order to carry out the business activity. [3]These include, for example, cleaning services, pure telecommunication services without specific reference to services rendered by the Processor to the Controller, postal and courier services, transport services or security services. [4]However, the Processor is obliged to ensure, even with ancillary services provided by third parties, that reasonable precautions and technical and organizational measures have been taken to ensure the protection of personal data. [5]The maintenance and servicing of IT systems or applications constitutes a subcontracting agreement subject to approval and data processing within the meaning of Art. 28 GDPR, if the maintenance and testing concerns systems that are also used in connection with the provision of services for the Controller and in the maintenance of personal data that can be accessed on behalf of the Controller.

(2) In accordance with the provisions of Art. 28 (1) (1) GDPR, the Processor will not use any other processor (sub-processor, sub-subprocessor) without prior separate or general written authorization by the Controller whereby all subcontracting provisions shall accordingly apply both to the sub-processor and to any subsequent (sub-) subprocessor subsequently used.

(3) Any existing or planned subcontracting by the Processor is listed in Annex 2 to this Agreement. [2]The Processor concludes these agreements in accordance with Art. 28 (2) and (4) GDPR if no such contract has already been concluded.

(4) [1]The Controller hereby authorizes in general terms the use of additional processors (sub-processors) by the Processor. [2]The Processor will inform the Controller of any intended changes in relation to the removal or replacement of other processors. In each individual case, the Controller has the right to object in writing or in text form to the procurement of a potential additional processor. [4]An objection may only be raised by the Controller for important reasons

to be proven to the Processor. ^{5}If the Controller does not object within 14 days after receipt of the notification, he shall have forfeited his right of objection to the corresponding assignment. ^{6}If the Controller objects for other than important reasons, the Processor may terminate this Agreement as well as, if applicable, the Main Agreement at the time of the intended use of the subcontractor.

(5) ^{1}The transfer of personal data of the Controller to the sub-processors and its initial action shall only be permitted upon fulfillment of all conditions for sub-processing. ^{2}The Processor shall contractually ensure that the provisions agreed between the Controller and the Processor also apply to sub-processors. ^{3}The contract with the sub-processors shall specify the details in a sufficiently specific manner to clearly separate the responsibilities of the Processor and the sub-processors. Where several sub-processors are used, this shall also apply to the responsibilities between those sub-processors. ^{2}In particular, it is the Processor's responsibility to transfer his data protection obligations under this contract to the other processor in accordance with Art. 28 (4) (1) GDPR.

(6) ^{1}If the sub-processor provides the agreed service outside the EU / EEA, the Processor shall ensure that the compliance with data protection law is fulfilled through appropriate measures. ^{2}The same applies if service providers within the meaning of paragraph 1 sentence 2 are to be used.

(7) Processor will bind sub-processors by contract, so that they will inform the Processor of any intended changes in relation to the removal or replacement of other sub-processors. Also in each individual case, the Processor will bind the sub-processors, so that he has the right to object to the procurement of a potential additional sub-processor.

§ 6 | Control Rights of the Controller in accordance with. Art. 28 (3) (2) lit. h GDPR

(1) ^{1}The Controller has the right to carry out inspections in consultation with the Processor or to have them carried out by auditors to be appointed in individual cases who are not allowed to compete with the Processor. ^{2}The Controller has the right to verify the compliance of the Processor with this Agreement in his business through sampling checks. Checks and Inspections may only be carried out in accordance with the Processor. They must be announced at least four weeks in advance, may only be carried out during normal business hours and may not disrupt business operations. Checks and inspections may only be carried out more often than once a year, in case that indications such as public media coverage give rise to concern and to question Processors security measures. Costs and expenses resulting

from this for the Processor shall be borne by the Controller, which are usually timely to be announced in advance.

(2) [1]The Processor shall ensure that the Controller can satisfy himself of the compliance with the obligations of the Processor in accordance with Art. 28 GDPR. [2]The Processor undertakes to provide the Controller with the necessary information upon request and in particular to prove the implementation of the TOMs.

(3) [1]The proof of such measures, which do not concern only the concrete processing, can be carried out by

a) compliance with approved codes of conduct pursuant to Art. 40 GDPR;
b) the certification according to an approved certification procedure according to Art. 42 GDPR
c) current certificates, reports or reports extracts of independent bodies (e.g., auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors) and / or
d) appropriate certification through an IT security or data protection audit [e.g., according to the Federal Office for Security in Information Technology (BSI Grundschutz)].

§ 7 | Support and Notification Obligations of the Processor pursuant to Art. 28 (3) (2) lit. e and f GDPR

(1) [1]The Controller is responsible for safeguarding the rights of the data subjects. [2]In this context, the Processor is nonetheless obligated, depending on the type of processing, to support the Controller – to the extent possible and adequate - with suitable technical and organizational measures to fulfill the Controller’s obligations with regard to the rights of the data subjects referred to in Chapter III of the GDPR, that is to say, when responding to data subjects' inquiries concerning the Controller’s information obligations to the persons concerned, their right of access, their right of rectification, erasure, restriction of processing, data portability and related communication obligations of the Controller, the right to object to automated decisions, including profiling, if the data subject asserts any such rights. [3]If the data subject complains at the Processor in order to assert a right, the latter forwards the inquiries to the Controller without undue delay.

(2) [1]The Processor shall also assist the Controller, taking into account the nature of the processing of the contract and the information available to the Processor, in compliance with the obligations set out in Articles 32 to 36 GDPR, i.e. in the performance of the Controller’s

legal obligations on data security, reporting of data breaches to supervisory authorities and the persons concerned, to carry out data protection impact assessments, and to prior consultation of the competent authority, if required by the data protection impact assessment. [2]The Processor and the Controller cooperate in response to inquiries from the relevant supervisory authorities in the performance of their duties.

§ 8 | Authority of the Controller

(1) [1]The Processor shall process personal data only in accordance with the agreements made and following the instructions of the Controller unless he is obliged to process otherwise by the law of the Union or of the member states to which the Processor is subject (Art. 28 (3) (3) lit. a, Art. 29 GDPR). [2]In the event of such an obligation, the Processor shall inform the Controller of these legal requirements prior to processing, unless the law prohibits such notification on grounds of a prevailing public interest.

(2) [1]The Processor warrants that the processing will be carried out in accordance with the instructions of the Controller. [2]If the Processor is of the opinion that an instruction of the Controller violates this Agreement or applicable data protection law, he must inform the Controller immediately. [3]Following a corresponding notification to the Controller, the Processor is entitled to suspend the execution of the instruction until the Controller confirms or changes the instruction. [4]The Parties agree that the sole responsibility for the processing according to instructions lies with the Controller.

(3) [1]The Controller's instructions are always in written or text form. If necessary, the Processor can also give verbal instructions (remotely). Remote verbally issued instructions are to be confirmed by the Controller immediately in written or text form.

§ 9 | Erasure and Return of Personal Data pursuant to Art. 28 (3) (2) lit. g GDPR

(1) [1]Copies or duplicates of the data are not made without the knowledge of the Controller. [2]Excluded from this are backup copies, to the extent necessary to ensure proper data processing, as well as data copies required regarding compliance with statutory retention requirements.

(2) [1]After the conclusion of the contractually agreed work or sooner upon request by the Controller - at the latest upon termination of the Main Agreement - the Processor has all

documents, processing and utilization results as well as data, which are related to the contractual relationship to hand over to the Controller or to destroy it after prior consent in accordance with data protection law. [2]The same applies to test and reject materials. [3]The log of the deletion must be submitted on request.

(3) [1]Documentation serving as proof of orderly and proper data processing shall be kept by the Processor according to the respective retention periods beyond the end of this Agreement. [2]He may hand them over to the Controller for his discharge at the end of this Agreement.

§ 10 | Miscellaneous

(1) [1]Both Parties are obligated to treat all knowledge of trade secrets and data security measures of the respective other party obtained in the contractual relationship as well as for the time after the termination of this Agreement confidential. [2]If there is any doubt as to whether any information is subject to the obligation of secrecy, it shall be treated as confidential pending the written approval of the other party.

(2) If the Processor's property is endangered by measures taken by third parties (such as seizure or confiscation), insolvency or settlement proceedings or other events, the Processor must immediately inform the Controller.

(3) For additional Agreements, the written form is required. This equally applies to the lack of this formal requirement.

(4) The objection of the right of retention, irrespective of the legal grounds, shall be excluded with regard to the data processed in context with this DPA and regarding relevant data carriers.

(5) This DPA shall also apply if and insofar as authorities or courts deviate mutatis mutandis from a joint responsibility of the contracting parties pursuant to Art. 26 GDPR.

(6) [1]Should individual provisions of this DPA be wholly or partially invalid or unenforceable or become ineffective or unenforceable because of changes in the legislation after conclusion of the DPA, its remaining provisions and the validity of the DPA as a whole shall remain unaffected thereby. [2]The invalid or unenforceable provision shall be replaced by an effective and enforceable provision which comes as close as possible to the purpose of the invalid provision. [3]If the DPA should prove to be incomplete, such provisions shall be deemed to have been agreed which correspond to the purpose of the DPA and would have been agreed upon in the case of consideration.

(7) The Processor may demand appropriate remuneration, to be agreed in advance with the Controller in each individual case, for additional expenditure incurred as a result of his support services in connection with additional services which are not included in the service description or which go beyond the statutory obligations of the Processor or are not attributable to misconduct on the part of the Processor.

(8) [1]The DPA is exclusively subject to the laws of the Federal Republic of Germany to the exclusion of its international laws of conflict.

(9) The exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement is the registered office of the Processor.

(10) In the event of any conflict or inconsistency between the Main Agreement or other Agreements between the Parties and this Data Processing Agreement regarding the subject matter of this DPA the following rule of precedence shall apply to the extent possible by applicable law:

1. This Data Processing Agreement
2. The Main Agreement
3. Other Agreements between the parties

____

Place, Date

For and on behalf of Controller	For and on behalf of Processor
______________________________ (Signature)	______________________________ (Signature)
______________________________ (Name, Position)	______________________________ (Name, Position)

Annex 1 – Technical- and Organizational Measures

Taking into account the

- state of the art,
- the costs of implementation,
- the nature, scope and circumstances,
- the purposes of the processing and
- the varying likelihood and severity of the risk to the rights and freedoms of natural persons

Bitly Europe shall implement appropriate technical and organizational measures to ensure a level of protection appropriate to the risk.

In assessing the adequate level of protection, particular account shall be taken of the risks inherent in the processing, in particular from destruction, loss, alteration or unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed, whether accidental or unlawful.

Bitly Europe shall take the following measures:

1. Physical Access control

- **Servers in company premises**: No servers are used on company premises.
- **Office Security:** Offices are locked and only accessible with keycards or personal authorization via an app.

2. Data carrier control

- **Locked storage of data carriers**: Data carriers can be stored locked.
- **Data carriers with personal data:** No data carriers with personal data are transferred.

3. Storage control

- **User authentication IT systems**. The following procedures are used for user authentication in IT systems: Passwords, 2-factor-authentication.
- **Password used for authentication:** Passwords are used for authentication.
- **Password for authentication - password length:** The following password length is prescribed: Minimum 20 characters
- **Password for authentication - Password complexity:** The following password complexity is prescribed: Letters, numbers, symbols, special characters.

- **Password for authentication - change intervals:** The following change intervals are implemented: Every three months, passwords cannot be reused.

4. User control

- **Employee Training Measures:** All employees are made aware of the importance of data protection and are trained on the subject of data privacy.
- **Confidentiality**: All employees are committed to data secrecy and confidentiality.

5. Access control

- **Minimum administration authorization scope:** Administration authorizations are limited to the minimum required group of persons. Role-based authorization management and regular recertification of authorizations (Need-to-know; Principle of Least Privilege) are in place.
- **Access to data basis:** For accessing the production databases, the developers need a personalized VPN access and personalized database credentials. Without the VPN the databases are only accessible within our VPC (Virtual Private Cloud).

- **VPN obligation for remote Work:** Policy only allows access to the systems via VPN.

6. Transmission control

- **Encryption of transmission:** Data is encrypted in transit using the following methods/protocols: SSL/TLS.
- **Software firewall:** A firewall is used against unwanted network accesses.
- **Hardware firewall:** Sophos device (Tier 1).

7. Server Security

- **Amazon Web Services (region eu-west-1/Ireland):** All applications and databases hosted within AWS are protected with AWS security measures. AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 9001:2015, and CSA STAR CCM v3.0.1.
  (Source: https://aws.amazon.com/compliance/iso-certified/?nc1=h_ls

8. Input control

- **Logging processing of personal data:** Logs of creation, deletion and modification of personal data are kept.
- **Logging of personal data modification - assignment:** It is possible to identify who entered or changed them.

- **Logging of personal data modification - storage:** Logs of creation, deletion and modification of personal data are stored.
- **Logging of changes to personal data - access:** Only authorized persons of the IT department and management have access to the logs or to the evaluation routine.
- **Anonymization/pseudonymization:** To protect personal data against unauthorized access, it is anonymized or pseudonymized.
- **Pseudonymization:** To protect data against unauthorized access, it is secured using the following method(s): Data Masking.

9. Recoverability

- **Recoverability:** States of systems and/or data can be restored for the following areas: Installations, data, system file and data containers, log data, user accounts and configurations (settings and shares).

10. Reliability

- **Network monitoring software:** Software is used to monitor the network/applications.
- **Third party network monitoring:** Specialized vendor for network monitoring (e.g. TecRacer).
- **Change management:** A change management process is used to prevent errors when programs are changed, which includes the steps of requesting, testing, and releasing.

11. Data integrity

- **Types of software used:** Purchased standard software and in-house developments are used.
- **Software Updates:** Updates are implemented in a timely manner both manually and automated.

12. Availability control

- **Backup types - media:** Data is backed up on Cloud, and additionally on a local NAS (Network Attached Storage). NAS is stored at an external provider in Germany, which is certified according to both ISO 27001 (native) and ISO 27001 on the basis of IT baseline protection.
- **Backup - accessibility:** It is accessible remotely through VPN, or on location through biometrics check and RFID card.
- **Backup - intervals**: Backup intervals are daily, weekly and monthly.

13. Separability

- **Separation between environments:** Production, test and development environments (including databases) are segregated from each other.
- **Separation of networks:** The corporate network is virtually separated into different segments.

14. Third Party Control

- **Third party services:** Information Security Systems of third party service providers are assessed.
- **Third parties obligations:** Third parties are contractually obliged to ensure security and confidentiality, including data processing agreements and standard contractual clauses according to GDPR.

Annex 2 - Subprocessor

This sub-processor list identifies processors within the meaning of Art. 28 GDPR of Bitly Europe that provide services to Bitly Europe.

Bitly Europe currently cooperates with the following sub-processors for the performance of the Agreement. The controller accepts the involvement of the following processors.

Name	Address	Service
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855, Luxembourg	Cloud hosting