# Data Processing Agreement

According to Art 28 ff General Data Protection Regulation ("GDPR")

Version 02.02.2023

**Processor:**

baningo GmbH
Sechskrügelgasse 2/7
1070 Vienna
Austria

## 1. Preamble

1. On the basis of this data processing agreement (hereinafter DPA), baningo GmbH (hereinafter referred to as Contractor) processes personal data within the meaning of Art 4 Z 1 General Data Protection Regulation (GDPR) for its customers (hereinafter referred to as “Client”).
2. This contract supplements our General Terms and Conditions (GTC) and forms the contractual basis for order data processing within the meaning of Art. 28 Para. 3 DSGVO. In the event of contradictions, this contract takes precedence over the GTC and is to be interpreted in accordance with the GDPR and the accompanying data protection laws.
3. The Contractor provides the Client with baningo cards, a software solution for digital business cards. Here, employee data of the Client is processed. Depending on the functions used by the Client, the Client's customer data may be processed.

## 2. Subject of the contract

1. The Contractor as a processor within the meaning of Art 4 Z 8 GDPR processes the personal data on behalf of the Client as the person responsible within the scope of their activity(s).
2. This agreement includes all personal data (Art 4 Z 1 DSGVO),
    a. which the Contractor processes for the Client in fulfillment of their contractual obligations under the service contract or
    b. which the Contractor accesses or can access, even if they are not expressly listed in Annex 1.

## 3. Rights and obligations of the Client

1. The customer expressly declares that it is the “responsible person” for the personal data that is the subject of the contract within the meaning of Art. 4 Z 7 GDPR. Therefore, within the framework of the contractual relationship between the contracting parties, the Client alone decides on the purposes and means of processing the personal data.
2. The Client is responsible, among other things, for ensuring that there is a sufficient legal basis for the processing of personal data with which the processor is commissioned and for ensuring that the processing of personal data is admissible for compliance with the GDPR and the accompanying data protection laws and the granting of the rights of those affected.
3. Therefore, the customer is also entitled to instructions under data protection law, in which form and to what extent the personal data are to be processed by the Contractor; if the Client's instructions violate data protection law, the Contractor has a duty to inform (Art. 28 para. 3 3rd sentence GDPR). Instructions that are obviously illegal are not to be followed by the Contractor.
4. The Client alone is therefore entitled to decide on the use, deletion and correction of personal data.

5. In the interests of transparency, the Client alone appears to third parties as the person responsible.

## 4. Type and scope of data processing

1. The personal data are from the Contractor
    a. to be used exclusively for the purpose of fulfilling the contractual obligations towards the customer;
    b. not to use for own or third-party purposes;
    c. to be returned exclusively to the Client and only to be passed on to third parties following a written order;
    d. to process within the territorial scope of the GDPR, unless the Client expressly agrees to this in writing;
    e. to process it in such a way that the Client is able to fulfill its data protection obligations towards data subjects and supervisory authorities at all times.
2. Any violation of the type and scope of data processing by the Contractor means that it is itself responsible for the unlawful data processing (Article 28 (10) GDPR).

## 5. Obligations of the Contractor

1. Within the scope of the contractual obligations assumed, the Contractor is responsible for the proper order of data processing within the framework of the service contract and the existing data protection laws.
2. Obligations that do not already arise from the service contract or the objective law are shown separately as "Instructions for data processing" in Appendix 3 of this agreement. These can be adjusted by the Client at any time. The Contractor is obliged to properly document such instructions from the Client (Article 28 (3) (a) GDPR).

3. The Contractor undertakes that it has obliged all persons authorized to process the personal data to maintain data secrecy within the meaning of Section 6 DSG and Art 28 Para 3 lit b GDPR, or that they are subject to an appropriate, in particular statutory, confidentiality obligation (Art 28 para. 3 lit b GDPR).
4. The Contractor expressly agrees that these authorized persons have been verifiably trained and instructed on the issues of data protection, data security and confidentiality, in particular to comply with data protection regulations and principles of the GDPR and the provisions of this agreement. The confidentiality obligation must already exist for the customer before the start of data processing and continue to exist indefinitely after the end of the activity. The obligation of confidentiality also applies to data from legal entities.
5. The Contractor also undertakes to take all technical and organizational measures required under Art. 32 GDPR in order to be able to guarantee the security of data processing (Art. 28 para. 3 lit. c GDPR). The Contractor will therefore take all organizational and technical measures at its own expense that it deems necessary to (i) ensure the security and integrity of data processing, (ii) prevent loss of personal data, and (iii) unauthorized access by third parties to prevent personal data. The measures taken by the Contractor at the time this agreement was signed are described in their security concept and can be found in Appendix 2.
6. The Contractor undertakes to support the Client in asserting the rights of data subjects to the best of his ability (Article 28 (3) (e) GDPR). In particular, the Contractor shall ensure that the technical and organizational requirements are met so that the Client fulfills its obligations regarding the right to information (Article 15 GDPR), the right to rectification (Article 16 GDPR) and the right to erasure (“right to be forgotten”, Article 17 GDPR). to the data subject at any time within the statutory time limits. The Contractor shall provide the Client with all the necessary information for this.
7. The Contractor undertakes to support the Client to the best of its ability in complying with its obligations in accordance with Articles 32 to 36 GDPR (in particular for taking sufficient technical and organizational measures, for data

protection impact assessment and for security breach notification) (Article 28 (3) lit f GDPR) .

8. The Contractor is also obliged to inform the Client immediately of any breach of data protection or data security, especially in the case of official measures or insolvency proceedings.

## 6. Use of other processors

(Art 28 para 2 and para 4 lit d GDPR)

1. The Client hereby grants general written approval in accordance with Article 28 Paragraph 2 GDPR that the Contractor may transfer its contractual obligations arising from this agreement to other companies ("other processors"), provided that they also have an agreement within the meaning of Article 28 Paragraph 4 GDPR completes. However, the Contractor must inform the Client of the intended use of another processor in good time so that the Client can prohibit this in accordance with Art. 28 Para. 2 GDPR.

   All other processors must comply with the terms contained in this agreement. The Contractor is fully responsible under data protection law for the actions and omissions of these sub-processors. A list of the current additional processors is included in Appendix 4.

2. In any case, the Contractor will only commission other processors outside the EEA if (i) they are established in a third country that has an appropriate level of data protection accepted by the EU Commission by decision (adequacy decision) or (ii) with them the EU Standard contractual clauses or equivalent contract templates issued by the EU Commission have been agreed as suitable guarantees within the meaning of Art. 46 Para. 2 lit c and d GDPR.

## 7. Control rights

(Art 28 para 3 lit h GDPR

For a period of up to 1 year after the end of the service contract, the Contractor undertakes to prove to the Client, at the request of the Client, but no more frequently than once a year, that the conditions of this agreement have been fulfilled. This proof relates in particular to the implemented technical and organizational security measures. Such proof can consist of confirmations or certifications from internal or external auditors or the data protection officer, in special cases also through inspections.

## 8. Data Protection Officer

1. If the requirements of Art. 37 GDPR are met, the Contractor is obliged (at least) for the term of this agreement to appoint a data protection officer.
2. At the request of the Client, the Contractor will immediately inform the Client of the name of the respective data protection officer.

## 9. Contract duration

1. This agreement comes into force when signed by both contracting parties and is concluded for the period of validity of the referenced service contract.
2. After the end of its service, the Contractor is obliged to return all data, processing results and documents or to delete them as instructed by the Client.
3. The obligation to maintain confidentiality lasts indefinitely over the period of the upright contractual relationship.

## 10. Final Provisions

1. Changes and additions to this contract must be in writing, which can also be done in an electronic format. The same applies to the agreement to waive the written form requirement. The agreement, including its annexes, must be kept in writing by both parties, including electronically.
2. This agreement is subject to substantive Austrian law to the exclusion of the reference standards and the relevant Union law, in particular the GDPR. The place of jurisdiction for disputes regarding this agreement is at the registered office of the Contractor.
3. Otherwise, the regulations of the service contract concluded between the contracting parties continue to apply unchanged.

# Enclosure 1:**Specification of Personal Data**

Description of the type of personal data processed on behalf of the person responsible within the meaning of the underlying agreement on order processing:

| **Data of our Clients and their employees / disclosed by our Clients:** | **Mandatory Y/N** | **Comment** |
|---|---|---|
| First name Last Name | J | |
| Academic degree | N | |
| E-Mail-Address (n) | J | |
| Telephone number (n) | N | |
| employer / company | J | |
| Position | N | |
| Address | J | |
| Date of birth | N | |
| Photo | N | |
| password | J | |
| Video | N | |
| Uploaded Data | N | |
| Individual content:<br>E.g. About me, professional experience, education and training, knowledge, moto, credo, products, services, etc. | N | |
| **Data from customers of our Clients** | | |

| | | |
|---|---|---|
| First name / Last Name | N | Only if contact modules are used |
| Phone number | N | Only if contact modules are used |
| E-Mail-Address | N | Only if contact modules are used |
| News content | N | Only if contact modules are used |
| **additionally collected by the Contractor** | | |
| Access log entries web server:<br>- IP addresses<br>- HTTP Communication Protocol | J | Affects all accesses to the application |
| Information on the use of our products (e.g. creation date of profiles, number of logins or page views, metrics regarding the use of links and contact options, date of last login) | J | This information is used to analyze the use of our services, enable us to make improvements and to monitor and continuously improve the security of our services. |

# Enclosure 2: **Technical and organizational measures**

1. The processor ensures through technical and organizational Measures that are based on the state of the art, the implementation costs and the specific risks and are suitable for ensuring an appropriate level of protection for the rights of the data subject.

2. The state of the art refers to advanced processes, facilities and operating methods which, according to the prevailing opinion of competent experts, make it appear that the legally specified goal in data protection is achieved. Procedures, equipment and operating methods or comparable procedures must have proven themselves in practice and should be successfully tested in operation.

3. The technical and organizational measures taken by the Contractor can be described as follows:

**(i) Access control**

The facilities of baningo GmbH are locked with locking cylinders. Only employees of baningo GmbH have keys. Visitors are always accompanied by an employee of baningo GmbH. The key is taken away from employees who leave the company. Keys issued to the facilities are documented in writing (list of keys) and regularly checked for completeness

**(ii) System access control**

The systems of baningo GmbH are protected against unauthorized system use by firewalls and malware filters on the perimeter and virus scanners on the inside. Systems are accessed using personal passwords.

According to internal work instructions, a minimum password length and composition of characters is prescribed for all systems used. Passing on or sharing passwords is strictly prohibited.

If possible, the use of two-factor authentication is mandatory.

**(iii) Data access control**

Unauthorized reading, copying, changing or removing within the system is prevented by encryption of data carriers and access management. Access authorizations are based on role descriptions including differentiated authorizations. These are regularly reviewed and only granted to authorized personnel to the extent and for the duration necessary to perform the function of the respective person ("need-to-know" principle).

If possible for the respective data processing, the primary identification features of the personal data are removed in the respective data application and stored separately (pseudonymized). As far as possible, encryption technologies are also used to protect personal data or anonymized as early as possible if the purpose allows it.

The accesses are logged by the system and are not accessible to the accessing party. When accessing the database, the IP address, time and date stamp are logged for traceability.

**(iv) Disclosure control**

baningo GmbH uses layered encryption to protect data that is transmitted. Communication between the customer systems and the Contractor's system takes place via an encrypted transmission channel (e.g. HTTPS) in order to secure data transmission and to create trust through the use of certificates and server validation.

A determination as to whether and by whom personal data has been entered, changed or removed in data processing systems is carried out by appropriate logging.

**(in) Performance control**

The systems of baningo GmbH are balanced in terms of load and designed redundantly as far as possible. They are based on several server stations that are able to compensate for a failure or defect. Our web and database servers are protected by firewalls and their use is documented in writing. Daily backups protect against data loss of personal data (data backup). Access authorizations differentiated according to confidentiality also protect personal productive data against accidental destruction, loss or misuse.

**(we) Evaluation measures**

For special questions, we obtain external expertise, for example on data protection-compliant logging or data protection-compliant implementation in test data management. In addition, regular employee training courses are held with a focus on data protection and information security.

# Attachment 3: **Sub-processors**

The table below contains sub-processors used by baningo GmbH within the meaning of Art. 28 Para. 2 GDPR.

| **Other Processors** | **Purpose** |
|---|---|
| Hetzner Online GmbH<br>Industriestr. 25<br>91710 Gunzenhausen<br>Registered office: Germany<br>Registration court: Ansbach, HRB 6089 | Data center operator for our services. |
| Twilio Ireland Limited<br>25-28 North Wall Quay<br>Dublin 1, Ireland<br>Registered office: Dublin, Ireland<br>Register Number:IE557454, CRO ie | Sending system-relevant transactional emails to our customers and their users. |
| Stripe Europe LTD<br>C/O A&L GOODBODY, IFSC,<br>NORTH WALL QUAY, DUBLIN 1,<br>Ireland<br>Register Number:IE513174 | Payment service provider for the billing of our services |

| | |
|---|---|
| Google Dublin, Google Ireland Ltd.<br>Gordon House, Barrow Street<br>Dublin 4<br>Registered office: Ireland | **Google Maps:** This service is used to open the address on the digital business card directly in the Google Maps application.<br>Here, only the address data and no other personal data are sent to Google in order to obtain a section of the map of the location.<br>By not filling in the address information in the profile, this service can be deactivated by the person responsible.<br><br>**ReCaptcha:** We have implemented this service in the sense of privacy by design in accordance with ErG 78. The Google recaptcha is only activated if there are several login attempts or contact actions using forms within a defined period of time. This technical measure specifically wards off brute force attacks and thus protects the personal data of our customers. Users with “normal” login behavior are therefore not affected by processing by Google Recaptcha. |

# Beilage 4: **Other Transmission Recipients**

| **Other Transmission Recipients** | **Purpose** |
|---|---|
| Stripe Europe LTD<br>C/O A&L GOODBODY, IFSC,<br>NORTH WALL QUAY, DUBLIN 1,<br>Ireland<br>Register Nummer: IE513174 | Zahlungsdienstleister für die Abrechnung unserer Services |