­­­

**Data-processing agreement**

|  |  |
| --- | --- |
| between | and |
|  | **plazz AG**  Bahnhofstr. 5a, 99084 Erfurt |
| *represented by* | *represented by*  Jürgen Mayer (CEO) |
|  |  |
| In the following: **Client** | In the following: **Contractor** |

# Introduction, scope, definitions

1. This Agreement regulates the rights and obligations of the Client and the Contractor (hereinafter referred to as the "Parties") in the context of the processing of personal data on behalf of the Client.
2. This contract applies to all activities in which employees of the Contractor or subcontractors commissioned by the Contractor (subcontractors) process personal data of the Client.
3. Terms used in this Agreement shall be understood as defined in the EU General Data Protection Regulation. Insofar as declarations in the following must be made "in writing", the written form according to § 126 BGB is meant. In addition, declarations may also be made in other forms, provided that adequate verifiability is guaranteed.

# Subject matter and duration of processing

## Object

The Contractor shall carry out the following processing:

Processing of data in the context of the provision of the # (employee app).

The processing is based on the service contract of XYZ between the parties (hereinafter referred to as the "Main Agreement").

## Duration

The processing shall commence on [DATE] and shall continue for an indefinite period of time until the termination of this Agreement or the Principal Agreement by one of the parties.

# Type and purpose of data collection, processing or use:

## Type and purpose of processing

Processing is of the following nature: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

The processing serves the following purposes: Provision and interaction with the # (employee app)

## Type of data

The following data is processed:

* Profile data (e.g. ID, first name, last name, e-mail address, company, position, city, profile picture, other description texts, group memberships)
* Eigener User Generated Content (z.B. Notizen)
* Shared user-generated content (e.g. submitted reviews, chat messages, appointments (stored in the app), posts and likes)

The following are affected by the processing:

* Projektbeteilig
* Employees and employees

# Obligations of the Contractor

1. The Contractor shall process personal data only as contractually agreed or as instructed by the Client, unless the Contractor is legally obliged to carry out specific processing. If such obligations exist for the Contractor, the Contractor shall notify the Client of them prior to processing, unless such notification is prohibited by law. In addition, the Contractor shall not use the data provided for processing for any other purposes, in particular not for its own purposes.
2. The Contractor confirms that it is aware of the relevant, general data protection regulations. It observes the principles of proper data processing.
3. The Contractor undertakes to strictly maintain confidentiality during processing.
4. Persons who may become aware of the data processed in the order must commit themselves in writing to confidentiality, unless they are already subject to a relevant duty of confidentiality by law.
5. The Contractor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of the Data Protection Act and this Agreement before the start of the processing. Appropriate training and awareness-raising measures must be repeated on an appropriate regular basis. The Contractor shall ensure that persons employed for order processing are appropriately instructed and monitored on an ongoing basis with regard to the fulfilment of data protection requirements.
6. In connection with the commissioned processing, the Contractor shall support the Client in the preparation and updating of the register of processing activities and in carrying out the data protection impact assessment. All necessary information and documentation must be kept and forwarded to the Client immediately upon request.
7. If the Client is subject to control by supervisory authorities or other bodies, or if data subjects assert rights against the Client, the Contractor undertakes to support the Client to the extent necessary insofar as the processing in the order is concerned.
8. The Contractor may only provide information to third parties or the person concerned with the prior consent of the Client. Enquiries addressed directly to him shall be forwarded to the Client without delay.
9. To the extent required by law, the Contractor shall appoint a competent and reliable person as the data protection officer. It must be ensured that there are no conflicts of interest for the agent. In cases of doubt, the client can contact the data protection officer directly. The Contractor shall immediately inform the Client of the contact details of the Data Protection Officer or give reasons why no Commissioner has been appointed. The Contractor shall inform the Client immediately of any changes in the person or internal tasks of the Agent.
10. In principle, order processing takes place within the EU or the EEA. Any relocation to a third country may take place under the conditions set out in Chapter V of the General Data Protection Regulation and subject to compliance with the provisions of this Treaty.

# Technical and organizational measures

1. The data security measures described in Appendix 1 are defined as mandatory. They define the minimum owed by the contractor. The measures are intended to ensure the confidentiality, integrity, availability and resilience of the systems and services related to processing in the long term. The client is aware of these technical and organisational measures. He is responsible for ensuring that they provide an adequate level of protection for the risks of the data to be processed.
2. The data security measures can be adapted according to technical and organizational developments, as long as the level agreed here is not undercut. The Contractor must implement any changes necessary to maintain information security without delay. The Client must be notified of any changes without delay. Significant changes are to be agreed between the parties.
3. If the security measures taken do not or no longer meet the requirements of the Client, the Contractor shall notify the Client immediately.
4. The Contractor assures that the data processed in the order will be strictly separated from other databases.
5. Copies or duplicates will not be made without the knowledge of the client. Technically necessary, temporary reproductions are excluded, provided that an impairment of the level of data protection agreed here is excluded.
6. Before the start of data processing and then regularly for the duration of the contract, the Client shall satisfy itself of the Contractor's technical and organisational measures and document the result. The Contractor undertakes to provide the Client with all information and evidence necessary to carry out an inspection upon written request within a reasonable period of time.

# Regulations on the correction, deletion and blocking of data

1. The Contractor shall correct or delete the data subject to the contract if the Client instructs this and this is covered by the framework of instructions. If deletion in accordance with data protection regulations or a corresponding restriction of data processing is not possible, the Contractor shall undertake the destruction of data carriers and other materials in accordance with data protection regulations on the basis of an individual order by the Client, unless already agreed in the contract.

# Subcontracting

1. The processor is permitted to commission subcontractors in the future to process data of the client without separate permission from the client, Art. 28 (2) sentence 2 GDPR. In this case, the Processor shall also always inform the Controller of any intended change in relation to the involvement or replacement of other Processors.
2. Subcontractors may only be commissioned in third countries if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved rules of conduct).
3. At present, the subcontractors documented in Appendix 2 are engaged in the processing of personal data for the processor to the extent specified therein. The Client agrees to the commissioning of the subcontractors listed in Appendix 2.
4. If the Contractor places orders with subcontractors, it is the Contractor's responsibility to transfer its data protection obligations under this contract to the subcontractor.
5. Upon written request by the Client, the Contractor shall at any time provide information about the data protection-related obligations of its subcontractor.

# Rights and obligations of the client

1. The Client is solely responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.
2. The Client shall issue all orders, partial orders or instructions in a documented manner. In urgent cases, instructions can be given orally. The Client shall immediately confirm such instructions in a documented manner.
3. The Client shall inform the Contractor immediately if it discovers any errors or irregularities in the examination of the results of the contract.
4. The Contractor is free to prove the sufficient implementation of the obligations under this GCU contract, in particular the technical-organisational measures (§ 7) and measures that do not only affect the specific order, by providing the following evidence:

compliance with approved codes of conduct;

certification according to an approved certification procedure;

current attestations, reports or report extracts from independent bodies (e.g. auditors, auditers);

an appropriate certification through IT security or data protection audit;

Self-declaration by the Contractor.

1. The Client may, at its own expense, check compliance with the provisions on data protection and the obligations laid down in this DPA Agreement by obtaining information and requesting the evidence referred to in (4) from the Contractor with regard to the processing concerning it. The contracting authority shall examine as a matter of priority whether the possibility of verification granted in sentence 1 of this paragraph is sufficient. The Client may also monitor compliance with data protection regulations on site at its own expense. The Client may carry out the inspections himself or have them carried out by a third party commissioned by him at his own expense. Persons entrusted with the control by the client or third parties must be demonstrably obliged to maintain confidentiality when they are commissioned. The persons entrusted with the inspection by the Client or third parties shall be notified to the Contractor in an appropriate form in advance and shall be put in a position to prove their legitimacy to carry out the inspections. Third parties within the meaning of this paragraph shall not be representatives of competitors of the Contractor. The Client shall announce inspections with a reasonable period of time and shall take into account business operations and operating procedures when carrying them out.

# Notification obligations

1. The Contractor shall immediately notify the Client of any personal data breaches. Justified cases of suspicion of this must also be reported.
2. Significant disruptions in the execution of the order as well as violations of data protection regulations or the stipulations made in this contract by the Contractor or the persons employed by him must also be reported immediately.
3. The Contractor shall immediately inform the Client of any controls or measures taken by supervisory authorities or other third parties, insofar as these have references to order processing.
4. The Contractor undertakes to support the Client in its obligations under Articles 33 and 34 of the General Data Protection Regulation to the extent necessary.
5. The Client shall notify the person authorised to issue instructions specified in the Annex.

# Instructions

1. The Client reserves the right to issue comprehensive instructions with regard to the processing on the behalf.
2. The Client and the Contractor shall designate the persons who are exclusively authorised to issue and accept instructions in Appendix 3.
3. In the event of a change or a long-term impediment of the named persons, the successor or representative must be notified to the other party immediately.
4. The Contractor shall immediately draw the Client's attention to it if, in its opinion, an instruction given by the Client violates statutory provisions. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller at the Client.
5. The contractor must document instructions given to him and their implementation.

# Termination of the order

1. Upon termination of the contractual relationship, the Contractor shall either destroy the data processed in the order or hand it over to the Client at its option. All existing copies of the data must also be destroyed. The destruction must be carried out in such a way that it is no longer possible to restore even residual information with reasonable effort.
2. The Contractor is obliged to bring about the immediate return or deletion of the defect even in the case of subcontractors.
3. The Contractor shall provide proof of proper destruction and submit it to the Client without delay.
4. Documentation that serves to prove proper data processing must be retained by the Contractor even after the end of the contract in accordance with the respective retention periods. He can hand them over to the client at the end of the contract to relieve him.
5. The costs for destruction or surrender shall be borne by the client.

# Remuneration

The remuneration of the contractor is conclusively regulated in the main contract. Separate remuneration or reimbursement of costs within the framework of this contract shall only be made to the extent expressly regulated.

# Liability

1. The Contractor is responsible for implementing the measures set out in this Agreement. The Contractor shall not be liable in the event that these measures prove to be insufficient. The Client shall indemnify the Contractor against all claims by third parties, in particular by authorities, with regard to the processing of personal data in accordance with this Agreement. Art. 82 (5) GDPR remains unaffected by this.
2. Any liability of the Contractor due to attributable failure to perform this Agreement or for any other reason shall be subject to the limitation of liability agreed in the Main Agreement.

# Special right of termination

1. The Client may terminate the Main Agreement and this Agreement at any time without notice ("extraordinary termination") if there is a serious breach by the Contractor of data protection regulations or the provisions of this Agreement, if the Contractor is unable or unwilling to carry out a lawful instruction of the Client, or if the Contractor refuses to exercise the Client's control rights in breach of the contract.
2. A serious breach shall exist in particular if the Contractor has not fulfilled or has not fulfilled the obligations specified in this agreement, in particular the agreed technical and organisational measures, to a significant extent.
3. In the event of insignificant violations, the Client shall set the Contractor a reasonable period of time for remedy. If the remedy is not made in time, the Client shall be entitled to extraordinary termination as described in this section.
4. The Contractor shall reimburse the Client for all costs incurred by the Client as a result of the premature termination of the main contract or this contract as a result of extraordinary termination by the Client.

# Other

1. Both parties are obliged to treat confidentially all knowledge of trade secrets and data security measures of the other party acquired in the context of the contractual relationship, even after the termination of the contract. If there are doubts as to whether information is subject to confidentiality, it is to be treated as confidential until it has been released in writing by the other party.
2. For ancillary agreements, the written form is required.
3. Should individual parts of this agreement be invalid, this shall not affect the validity of the remainder of the agreement.

**Signatures**

Location, Date Location, Date

Client Contractor

##### Appendix 1 – technical and organisational measures

The technical and organisational measures to ensure data protection and data security are set out below, which the Contractor must at least set up and maintain on an ongoing basis. The aim is to guarantee, in particular, the confidentiality, integrity and availability of the information processed on behalf of the company.

**Note:** The measures must be described as concretely as possible in the interest of both parties! They are the benchmark for inspections by the client and also decisive for the question of whether a breach of duty may have occurred. This annex determines very decisively what the contractor has to do and prove and what not. Unclear or interpretable paraphrases must be avoided at all costs!

Description of the technical and organisational security measures taken by the controller(s) (including all relevant certifications) to ensure an adequate level of protection, taking into account the nature, scope, circumstances and purpose of the processing, as well as the risks to the rights and freedoms of natural persons:

**1 Confidentiality**

**1.1 Access control**

The hosting of the plazz AG software platform takes place in a Google data center (Google Cloud Platform) in Frankfurt (EU-West 03).

Detailed documentation of Google's technical and organizational data security measures and Google's certifications in the field of information security (including ISO 27001) can be found here: <https://cloud.google.com/terms/data-processing-terms-20180313>.

The offices of plazz AG are located in an office building in Erfurt. The entrances to the office building and also to the offices of plazz AG are closed day and night. An electronic locking system is used. The human resources department of plazz AG manages the keys/transponders and issues and revokes the respective access rights. Key allocation and key management are carried out according to a defined process that regulates the granting or withdrawal of access authorisations to rooms both at the beginning of an employment relationship and at the end of an employment relationship.

Access authorizations are only granted to an employee if this has been requested by the respective supervisor and/or the HR department. The principle of necessity is taken into account when granting authorisations.

Visitors are only granted access to the office building and then to the offices after the doors have been opened by the reception. The reception can see the entrance door and ensures that every visitor reports to the reception. Each visitor is recorded in a visitor list and then accompanied by the receptionist to his or her respective contact person. Visitors are not allowed to move freely in the offices unaccompanied.

The entrances and windows of the office building and also the offices are secured with an alarm system. This can be activated and deactivated manually. Regardless of this, the alarm system is activated automatically every day, but always in the evening.

**1.2 Access control**

In order to gain access to the software platform of plazz AG and to the IT systems of plazz AG in general, users must have the appropriate access authorization. For this purpose, appropriate access authorizations are assigned by administrators. Access authorisations are only granted if this has been requested by the respective supervisor.

Users receive a user name and an initial password, which must be changed when logging in for the first time. The password requirements include a minimum password length of 8 characters, whereby the password must consist of upper/lower case letters, numbers and special characters. A password history is stored to ensure that the past 10 passwords cannot be used again.

Failed login attempts are logged. If you enter 10 incorrect entries, the respective account will be blocked.

Passwords are always stored in encrypted form.

Remote access to IT systems always takes place via encrypted connections.

An intrusion prevention system is in use on the servers. All server and client systems have virus protection software, which ensures a daily supply of signature updates.

All servers are protected by firewalls that are constantly maintained and provided with updates and patches.

The access of servers and clients to the Internet and access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them.

**1.3 Access Control**

Access authorizations within the framework of the plazz AG software platform and generally for plazz AG's IT systems and applications are set up exclusively by administrators.

Access authorizations can be set flexibly and granularly and are generally assigned according to the "need to know" principle on a "least privilege" basis. Accordingly, only those employees who maintain and maintain these data, databases and/or applications or who are active in development and who absolutely need such access in the course of their work are granted access rights. The prerequisite is a corresponding request for access authorization for an employee by a supervisor.

There is a role-based authorization concept with the possibility of differentiated assignment of access authorizations, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project-by-project basis.

The assignment of admin rights is handled extremely restrictively.

The destruction of data carriers and paper is carried out by a service provider who guarantees destruction in accordance with DIN 66399.

All employees are instructed to deposit information containing personal data and/or information about projects in the designated destruction containers.

Employees are generally prohibited from installing unapproved software on the IT systems of plazz AG.

All server and client systems are regularly updated with security updates.

**1.4 Separation**

All IT systems used as part of the plazz AG software platform are multi-client capable, and the logical separation of data is always guaranteed.

The production environment is strictly separated from the test environment.

**1.5 Encryption & Pseudonymization**

Administrative access to server systems is generally carried out via encrypted connections. In addition, data on server and client systems is stored on encrypted disks. Corresponding hard disk encryption systems are in use.

In the case of pseudonymization of personal data, there is a strict separation of the assignment data from the pseudonymized data.

Employees are instructed to always check the possibility of pseudonymization or anonymization of personal data and, if necessary, to implement it.

**2 Integrity**

**2.1 Input control**

The entry, modification and deletion of (personal) data is always logged. The logging is checked regularly.

Employees are obliged to work with their own accounts at all times. Accounts may not be shared with other employees. Accordingly, it is always traceable who has entered, changed or deleted data.

**2.2 Passing control**

Personal data will only be passed on to the extent necessary for the provision of the respective contractual services.

All employees are instructed with regard to the permissible use of data and the modalities of disclosure of data.

All transmissions are comprehensively documented and there are detailed data flow overviews and retention and deletion concepts.

As far as possible, data is transmitted to recipients in encrypted form.

Employees are prohibited from using private data carriers for business purposes.

**3 Availability and resilience**

Data on server systems is backed up incrementally at least daily and fully weekly. The backup media is encrypted. The import of backups is tested regularly.

All relevant IT systems have an uninterruptible power supply. There is a fire alarm system and a CO2 extinguishing system in the data center. All server systems are subject to monitoring, which immediately triggers notifications to an administrator in the event of malfunctions.

There is an emergency plan in place, which also includes a recovery plan.

**4 Information security and data protection management system**

**4.1 Information security and data protection management system**

plazz AG has implemented a comprehensive information security and data protection management system. Responsibilities in the areas of information security and data protection are clearly assigned and documented.

There are guidelines on information security and data protection that ensure the implementation of the objectives of the information security and data protection management system. The effectiveness of the management system and in accordance with the guidelines is regularly evaluated with regard to its effectiveness and adjustments are made if necessary.

An expert data protection officer has been appointed and an information security and data protection team has also been set up to plan, implement, evaluate and make adjustments to all measures in the areas of information security and data protection. The information security and data protection team reports directly to the management.

**4.2 Training and Employee Engagement**

All employees at plazz AG are regularly trained in data protection and information security. Supplementary awareness measures are carried out regularly.

All employees are also obliged to data protection and confidentiality. The obligation is valid beyond the end of the employment at plazz AG.

**4.3 Transparency of data processing**

The transparency of data processing is of crucial importance against the background of plazz AG's business model. Plazz AG is absolutely aware of this importance and attaches great importance to providing comprehensive and clearly understandable information to those affected. There is comprehensive documentation of data processing and the data protection information is regularly checked and updated if necessary. There is a formalised process for processing and responding to enquiries from data subjects, and compliance with the relevant deadlines is always guaranteed.

**4.4 Service Provider Management (Order Control)**

When commissioning processors, an audit is carried out initially and then regularly and an agreement on order processing is concluded in accordance with data protection regulations. Processors are carefully selected, in particular with regard to ensuring an appropriate level of information security and data protection.

All processors are obliged to delete personal data at all times on the instructions of the controller and at the latest upon termination of the contract. It is guaranteed that plazz AG's retention and deletion concept is also implemented accordingly by processors.

**4.5 Dealing with Information Security and Data Protection Incidents**

Plazz AG has implemented a guideline for dealing with information security and/or data protection incidents, which defines standardized processes for dealing with potential information security and/or data protection incidents. The information security officer and data protection officer are always informed and involved. All potential information security and/or data protection incidents are documented and each incident is analyzed to determine whether and what measures can be taken to rule out similar incidents in the future.

Firewalls and spam filters are used and continuously updated.

All employees are instructed to report potential incidents to the information security and privacy team, even if there is the slightest suspicion. Plazz AG always guarantees timely reporting if there are legal reporting obligations in the event of an information security and/or data protection incident.

**4.6 Privacy by Design und Privacy by Default**

Already during the development or further development of both the business model in general and the software platform of plazz AG, care is taken to ensure that the principles of data economy and data minimization are taken into account.

Only the personal data that is absolutely necessary for the respective purpose is collected. During each processing operation, it is continuously checked whether there is a need for the processing of personal data or whether anonymisation can be carried out.

##### Appendix 2 – Subcontractors

|  |  |
| --- | --- |
| Subcontractor | Description of service |
| Microsoft Ireland Operations Limited  70 Sir John Rogerson's Quay  Dublin 2  Irland | Office Services  (Data-Center Amsterdam & Dublin) |
| Google Commerce Limited  Gordon House  Barrow Street  Dublin 4  Ireland | Hosting of the application and the backend when using cloud deployment  Backups  (Data-Center Frankfurt) |
| Freshworks GmbH  Alte Jakobstraße 85/86  10179 Berlin  Deutschland | Ticketsystem and IT Helpdesk  (Data-Center EU – Frankfurt a. M.) |
| 3Q GmbH  Kurfürstendamm 102  10711 Berlin  Deutschland | Streaming and hosting of media-data  (Data-Center EU) |
| Sendbird  400 1st Ave.  San Mateo, CA  94401, USA | Chat and textmessages aswell as comments  (Data-Center EU Frankfurt) |
| Agora  2804 Mission College Blvd. Santa Clara, CA  USA 95054 | Conferencing, Live-Streaming |
| Mailgun  Technologies, Inc. 112  E Pecan St #1135  San Antonio, TX 78205  legal@mailgun.com | E-Mail Service  (Data-Center EU) |
| MongoDB  1633 Broadway 38th Floor New York, NY 10019 United States | Content Management, Database  (Data-Center EU Frankfurt) |

##### Appendix 3 – Persons authorised to issue instructions

The following persons are authorised to issue and receive instructions:

Stefan Benischke – Technical Manager

Stefan Heinz – Head of Productboard

Nicole Sauter – Customer Support

Berra Eksen- Sales

##### Appendix 4 – Contact details of the Data Protection Officer

Data security officer:

Jonas Jöck & Julia Pudenz externally from Juno

E-Mail: [datenschutz@plazz.ag](mailto:datenschutz@plazz.ag)

Phone: +49 361 34 94 789 0