data processing agreement (DPA)

between

as the controller (hereinafter referred to as the "client")

and

plazz AG
Bahnhofstraße 5a
D-99084 Erfurt

as the processor (hereinafter referred to as the "contractor")

Preamble

This agreement ensures that plazz AG, as a service provider for event and community platforms, processes personal data securely, transparently, and in accordance with the General Data Protection Regulation (GDPR) within the scope of its cooperation with the client. It serves to protect the data concerned and to ensure a clear and trusting division of tasks between both parties.

§ 1 Definitions

For terms used in this agreement for which Art. 4 GDPR provides a definition, this legal definition in the version applicable at the time of conclusion of the contract also applies to this contract.

§ 2 Information on the competent data protection supervisory authority

(1) The competent data protection supervisory authority for the contractor is:

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit
Häßlerstrasse 8
D - 99096 Erfurt

(2) Upon request, the client shall inform the contractor of its competent data protection supervisory authority.

(3) The client and the contractor shall cooperate with the data protection supervisory authority in the performance of its duties upon request.

§ 3 Subject matter of the contract

(1) The contractor shall provide services for the client in the area of event & community platforms on the basis of the contract for DEAL/offer number 202_/____ commissioned on _____(“Main Contract"). In this context, the contractor and its employees or agents appointed by the contractor shall have access to personal data and shall process such data exclusively on behalf of and in accordance

with the instructions of the client. The scope and purpose of data processing by the contractor are set out in the main contract (and, if available, in the associated service description) and in ***Appendix 1*** to this contract. The client shall ensure that the processing of personal data is carried out in accordance with the applicable data protection regulations.

(2) The parties conclude this agreement to specify their mutual rights and obligations under data protection law. In case of doubt, the provisions of this contract shall take precedence over the provisions of the main contract.

(3) The term of this contract is based on the term of the main contract, unless obligations arising from the following provisions extend beyond the term of the main contract. Termination rights arising from this contract remain unaffected by the above provision.

(4) This agreement shall remain valid beyond the end of the main contract for as long as the contractor has personal data that has been provided to it by the client or that it has collected for the client. This also applies to subsequent contracts between the parties, regardless of a different DEAL number, provided that these contracts relate to the same subject matter and nothing to the contrary has been agreed.

(5) The contractually agreed data processing shall be carried out exclusively in a Member State of the European Union or another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the specific requirements of Art. 44 ff. GDPR are met.

§ 4 Right to issue instructions

(1) The contractor may only process data within the scope of the main contract and in accordance with the client's instructions. If the contractor is obliged to carry out further processing under the law of the European Union or the member states to which it is subject, it shall inform the client of these legal requirements prior to processing, provided that it is legally permitted to do so.

(2) The client's instructions are initially specified in this contract and may subsequently be amended, supplemented, or replaced by the client in writing or in text form by means of individual instructions (individual instructions). The client is entitled to issue such instructions at any time. This includes instructions regarding the correction and deletion of data as well as the restriction of processing. The persons or departments authorized to issue instructions are listed in ***Appendix 4***. In the event of a change or long-term absence of the named persons, the successor or representative must be named to the contractual partner in writing without delay. If a contractual partner does not name any persons or departments authorized to issue instructions, all documented instructions issued within its area of responsibility shall be deemed to have been accepted by it and to be binding.

(3) All instructions issued must be documented by both the client and the contractor. Instructions that go beyond the services agreed in the main contract shall be treated as a request for a change in services. Provisions regarding any remuneration for additional expenses incurred by the contractor as a result of supplementary instructions from the client remain unaffected.

(4) If the contractor believes that an instruction from the client violates data protection regulations, it must immediately notify the client. The contractor is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the client. The contractor may refuse to execute an instruction that is obviously unlawful.

§ 5 Type of data processed, group of data subjects

Within the scope of the performance of the main contract, the contractor shall, depending on the scope of the order, be given access to the personal data of the data subjects specified in more detail in ***Appendix 1***. This data includes the special categories of personal data listed in ***Appendix 1*** and marked as such.

§ 6 Protective measures of the contractor

(1) The contractor is obliged to comply with the statutory provisions on data protection and not to pass on information obtained from the client's area to third parties or to grant them access to it without appropriate instructions. Paper documents and data must be secured against access by unauthorized persons, taking into account the state of the art.

(2) The contractor shall organize its internal operations within its area of responsibility in such a way that they meet the specific requirements of data protection. The contractor guarantees that it has taken all necessary technical and organizational measures to adequately protect the client's data in accordance with Art. 32 GDPR, in particular at least the measures listed in ***Appendix 2***. If special categories of personal data are also processed, the contractor shall additionally take the appropriate and specific measures resulting from Section 22 (2) BDSG, which are specified in more detail in ***Appendix 2***. At the request of the client, the contractor shall disclose the details of the measures to be taken and the implementation of the measures.

The contractor reserves the right to improve the security measures taken, ensuring that the contractually agreed level of protection is not fallen short of and that the client is informed immediately of any significant changes.

(3) The data protection officer at the contractor is: ***PRILUTIONS Rechtsanwaltsgesellschaft mbH, based in 99090 Erfurt***. The contractor shall publish the contact details of the data protection officer on its website and communicate them to the data protection supervisory authority. Any change in the person of the data protection officer must be communicated to the client without delay.

(4) Persons employed in data processing by the contractor are prohibited from processing personal data without authorization. The contractor shall impose a corresponding obligation on all persons entrusted by it with the processing and fulfillment of this contract (hereinafter referred to as employees) (confidentiality obligation, Art. 28 (3) subparagraph 1 sentence 2 lit. b GDPR), instruct them on the special data protection obligations arising from this contract and the existing obligation to follow instructions and adhere to the purpose limitation, and ensure compliance with the aforementioned obligation with due care. These obligations must be formulated in such a way that they remain in force even after the termination of this contract or the employment relationship between the employee and the contractor. The client shall be provided with appropriate evidence of the employees' obligations upon request.

§ 7 Contractor's information obligations

(1) In the event of disruptions to processing activities, suspected data protection violations or breaches of the contractor's contractual obligations, or suspected other security-related incidents at the contractor, among persons employed by the contractor within the scope of the contract, or by third parties, the contractor shall inform the client immediately in writing or in text form. The same applies to audits of the contractor by the data protection supervisory authority that concern processing or circumstances relevant to the client. The notification of a breach of the protection of personal data shall contain the following information, as far as possible:

a) a description of the nature of the personal data breach, including, where possible, the categories and number of data subjects concerned, the categories and number of personal data records concerned

b) a description of the likely consequences of the breach

c) a description of the measures taken or proposed by the contractor to remedy the breach and, where applicable, measures to mitigate its possible adverse effects

(2) The contractor shall immediately take the necessary measures to secure the affected data and mitigate any possible adverse consequences for the person(s) concerned, inform the client thereof, request further instructions from the client, and provide the client with further information at any time if the client's data is affected by a breach pursuant to paragraph 1.

(3) If the client's data held by the contractor is endangered by seizure or confiscation, by insolvency or composition proceedings, or by other events or measures taken by third parties, the contractor shall inform the client immediately, unless prohibited from doing so by court or official order. In this context, the contractor shall immediately inform all competent authorities that the client has sole decision-making authority over the data.

(4) The contractor shall inform the client immediately of any significant changes to the security measures pursuant to Section 6 (2).

(5) The contractor shall maintain a record of all categories of processing activities carried out on behalf of the client, containing all information in accordance with Art. 30 (2) GDPR. The record shall be made available to the client upon request.

(6) The contractor shall cooperate to an appropriate extent in the preparation of the procedure directory by the client, in the preparation of a data protection impact assessment pursuant to Art. 35 GDPR, and, if necessary, in the prior consultation of the data protection supervisory authorities pursuant to Art. 36 GDPR. The contractor shall provide the client with the necessary information in an appropriate manner.

§ 8 Control rights of the client

(1) The client shall satisfy itself of the contractor's technical and organizational measures before commencing data processing and thereafter on a regular basis. To this end, it may, for example, obtain information from the contractor, request existing expert opinions, certifications, or internal audits, or, if possible, personally review the contractor's technical and organizational measures after timely consultation during normal business hours or have them reviewed by a competent third party, provided that this third party is not in a competitive relationship with the contractor. The client shall only carry out checks to the extent necessary and shall not disproportionately disrupt the contractor's business operations in doing so.

(2) The contractor undertakes to provide the client, upon verbal or written request, with all information and evidence necessary to carry out an inspection of the contractor's technical and organizational measures in accordance with ***Appendix 2*** within a reasonable period of time.

(3) The client shall document the results of the checks it has carried out and communicate them to the contractor. If the client discovers any errors or irregularities, particularly when checking the results of orders, it shall inform the contractor immediately. If the inspection reveals circumstances that require changes to the prescribed procedure in order to be avoided in future, the client shall inform the contractor of the necessary procedural changes without delay.

(4) Upon request, the contractor shall provide the client with a comprehensive and up-to-date data protection and security concept for order processing and for persons with access rights.

(5) The contractor shall, upon request, provide the client with evidence of the employees' obligations in accordance with Section 6 (4).

Section 9 Use of subcontractors

(1) In order to always offer our customers the best possible services, plazz AG works with carefully selected subcontractors. These are selected according to strict data protection requirements in order to ensure a high level of security and reliability. Within the framework of this cooperation, the contractually agreed services or the partial services described below are performed with the involvement of the subcontractors listed in ***Appendix 3***. The contractor is authorized within the scope of its contractual obligations to establish further subcontracting relationships with subcontractors ("subcontracting relationship"). These are bound by a contract or other legal instrument under Union law or the law of the Member State concerned to comply with the same data protection obligations as those set out in the data processing agreement between the client and the contractor in accordance with Art. 28 (3) GDPR. In particular, sufficient guarantees must be provided to ensure that appropriate technical and organizational measures are taken to ensure that the processing is carried out in accordance with the requirements of the GDPR. If the further processor fails to comply with its data protection obligations, the contractor shall be liable to the client for the compliance of this subcontractor with its obligations. The contractor shall ensure that the requirements of Chapter 5 of the GDPR are complied with when transferring data to third countries, in particular that adequacy decisions or standard contractual clauses (SCC) including a transfer impact assessment are in place, and shall provide evidence of this to the client upon request.

Before establishing further subcontracting relationships, the contractor shall inform the client in writing with four weeks' notice. The client may only object to the change for good cause. The objection must be made within 14 calendar days and must expressly state all important reasons. An important reason on the part of the contractor shall be deemed to exist in particular if the subcontractor is not based in a country that is a member of the EU/EEA or for which the Commission has issued an adequacy decision pursuant to Art. 45 GDPR.

(2) A subcontractor relationship within the meaning of these provisions does not exist if the contractor commissions third parties to provide services that are to be regarded as purely ancillary services. These include, for example, postal, transport, and shipping services, cleaning services, telecommunications services without any specific connection to services provided by the contractor for the client, and security services. Maintenance and testing services constitute subcontractor relationships within the meaning of paragraph 1 insofar as they are provided for IT systems that are also used in connection with the provision of services for the client.

§ 10 Requests and rights of data subjects

(1) The contractor shall support the client with appropriate technical and organizational measures in fulfilling the client's obligations under Articles 12–22 and 32 and 36 of the GDPR.

(2) If a data subject asserts rights, such as the right to information, correction, or deletion of their data, directly against the contractor, the contractor shall not respond independently, but shall immediately refer the data subject to the client and await the client's instructions.

§ 11 Liability

(1) The client and contractor shall be liable to data subjects in accordance with the provisions of Art. 82 GDPR. The contractor shall coordinate any fulfillment of liability claims with the client.

(2) The contractor shall indemnify the client against all claims asserted by data subjects against the client due to a breach of an obligation imposed on the contractor by the GDPR or due to non-compliance with or breach of an obligation set out in this agreement or an instruction issued separately by the client.

(3) The parties shall indemnify each other if/to the extent that one party proves that it is in no way responsible for the circumstance that caused the damage to a data subject. In all other respects, Art. 82 (5) GDPR shall apply.

(4) Unless otherwise specified above, liability under this agreement shall be the same as that under the main agreement.

§ 12 Costs

(1) Insofar as the contractor supports the client in fulfilling its data protection obligations in accordance with this contract, this support shall generally be provided without separate remuneration.

(2) However, in the following cases, the contractor may demand reasonable remuneration for its expenses:

a) Support in creating and maintaining the record of processing activities in accordance with Art. 30 (1) GDPR, as well as in creating a data protection impact assessment in accordance with Art. 35 GDPR and prior consultation with the data protection supervisory authority in accordance with Art. 36 GDPR (§ 7).

b) Carrying out or supporting checks by the client in accordance with § 8.

c) Support in processing requests from data subjects in accordance with § 10.

(3) Remuneration may only be demanded if the expenditure incurred exceeds the usual amount and is not covered by the contractor's general contractual obligations. The amount of remuneration shall be based on the contractor's standard hourly rates, unless otherwise agreed between the parties.

(4) The contractor shall inform the client of the costs incurred before providing any chargeable support services and shall obtain written or textual consent.

§ 13 Extraordinary right of termination

In the case of minor breaches that are neither intentional nor grossly negligent, the contractor shall first be given the opportunity to remedy the defect within a reasonable period of time. If the breach is not remedied within this period, the client may take further measures, including extraordinary termination.

Irrespective of this, the client has the right to terminate the main contract in whole or in part without notice if the contractor fails to fulfill its contractual obligations, intentionally or grossly negligently violates the provisions of the GDPR, or is unable or unwilling to carry out an instruction from the client.

§ 14 Termination of the main contract

(1) Upon termination of the main contract or at any time upon request, the contractor shall return to the client all documents in paper form, data, and data carriers provided to it or, at the client's request, delete them, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany. The obligation to surrender or destroy also applies to any data backups held by the contractor.

The contractor shall keep documented evidence of proper deletion.

(2) The client has the right to check the complete and contractually compliant return or deletion of the data by the contractor in an appropriate manner or to have it checked by a competent third party, provided that this third party is not in a competitive relationship with the contractor.

(3) The contractor is obliged to treat the information that has become known to it in connection with the main contract as confidential even after the end of the main contract.

§ 15 Final provisions

(1) The parties agree that the contractor has no right of retention with regard to the data to be processed and the associated data carriers.

(2) Amendments and supplements to this contract, the declaration of termination, and the amendment of this clause must be made in writing to be effective (§ 126 (1), (2) BGB). The replacement of the written form by the electronic form (§§ 126 (3), 126 a BGB) or the text form (§ 126 b BGB) is excluded. The priority of individual contractual agreements remains unaffected by this.

(3) Should individual provisions of this agreement be or become wholly or partially legally invalid or unenforceable, this shall not affect the validity of the remaining provisions.

(4) This agreement is governed by German law. The exclusive place of jurisdiction is Erfurt.

Appendices

Appendix 1 – Description of the persons/groups of persons affected and the particularly sensitive data/data categories

Appendix 2 – Technical and organizational measures taken by the contractor

Appendix 3 – Approved subcontractors

Appendix 4 – Persons authorized to issue instructions

Signatures

Place, date	Place, date
Client, represented by	Contractor, represented by Jürgen Mayer - CEO plazz AG

Appendix 1 – Description of Affected Persons/Groups of Affected Persons and Particularly Sensitive Data/Data Categories

Affected Persons:

- Project participants (organizers, speakers, sponsors, exhibitors)
- Visitors/Participants
- Employees and freelancers, alumni
- (Association/Committee) members
- Customers
- Suppliers/Service providers
- Business partners

Personal Data/Data Categories:

The following personal data is processed when collected by the client (*voluntary information* provided by the client):

- Master data (ID, first name, last name, date of birth)
- Contact data (address, email address, phone number)
- Access data (user ID, password)
- Employment data (company, position, city, group affiliation, personnel number)
- Travel data (travel date, ID card number for flight bookings, travel time)
- Tracking data (e.g., app crashes, opt-out available, (individual) app usage – if desired by the client)
- Image and video data (profile picture, photos and videos)
- Own user-generated content (e.g., notes)
- Shared user-generated content (communication data such as submitted reviews, chat messages, appointments stored in the app, posts and likes)
- Other data (description texts, clothing size, _____)

Special Categories of Personal Data:

The following special categories of personal data are processed when collected by the client (*voluntary information* provided by the client):

- Religion, disabilities, allergies/intolerances
- _____

Appendix 2 – Technical and Organizational Measures of the Processor

The following document presents a detailed directory of technical and organizational measures (TOM) implemented by the processor to protect the contractual personal data. These measures collectively serve the protection objectives of confidentiality, integrity, availability, and resilience of systems, which is why the repeated listing of cross-functional measures has been omitted.

1. Physical Access Control

Physical access control refers to measures that ensure only authorized persons have access to premises or facilities where personal data is processed, in order to avoid risks from physical access by third parties. The following section explains the specific measures and strategies implemented by the processor to ensure effective physical access control:

- ➢ Logging and escorting of all visitors
- ➢ Careful selection of cleaning personnel
- ➢ Documentation of access rights
- ➢ Documented procedure for granting/revoking access rights
- ➢ Access rights to "server room" limited to IT Ops
- ➢ Alarm system
- ➢ Intercom system with camera
- ➢ Video surveillance of entrances (doors and windows)
- ➢ Security of building shafts
- ➢ Doors with external knob
- ➢ Transponder system for entrance and side doors
- ➢ Definition of security zones/restricted areas
- ➢ Closed-shop operation for data processing and telecommunications systems
- ➢ Automatic access control
- ➢ Key management policy
- ➢ Reception/Front desk

2. System Access Control

System access control deals with securing digital resources and ensures that only authorized persons have access to specific data, systems, or applications. This prevents unauthorized access to personal data and ensures that it cannot be read, copied, modified, or deleted. The following section explains the specific measures and strategies implemented by the processor to ensure reliable system access control:

- ➢ Assignment of user rights
- ➢ Documentation of access authorizations
- ➢ Password history to prevent reuse of old passwords
- ➢ Password policy (regular changes, minimum length, complexity)

- ➢ Login with biometric data
- ➢ Individual assignment of passwords / Central password assignment (for initial login)
- ➢ Limited number of attempts
- ➢ Encrypted storage and transmission of passwords
- ➢ Secure storage of administration passwords
- ➢ Secure storage of keys for cryptographic procedures
- ➢ Authentication with username/password
- ➢ Two-factor authentication / Participant identification
- ➢ Logging of system usage and log analysis
- ➢ Automatic screen lock during work interruptions (password protected)
- ➢ Use of VPN technology
- ➢ Automatic logging of all activities on data processing systems
- ➢ Access control systems in rooms with IT systems
- ➢ Security locks
- ➢ Use of anti-virus software (server / mobile devices / clients)
- ➢ Encryption of data carriers in laptops/notebooks/tablets and smartphones
- ➢ Laptops locked away outside business hours
- ➢ Use of a hardware firewall
- ➢ Use of a software firewall
- ➢ BIOS protection (separate password)

3. Data Access Control

The main objective of data access control is to ensure that data is not only protected from unauthorized access, but also that authorized users receive exactly the access they need – no more and no less. This section presents the procedures and technologies used by the processor to ensure this granular control and monitoring of data access:

- ➢ Authorization concepts and need-based access rights (profiles, roles, transactions, and objects)
- ➢ Documentation of access authorizations
- ➢ Annual review of access rights through internal system audit
- ➢ Rights management by IT Ops
- ➢ Number of administrators reduced to the "necessary minimum"
- ➢ Password policy (regular changes, minimum length, complexity)
- ➢ Logging of access to applications, especially for data entry, modification, and deletion
- ➢ Physical deletion of data carriers before reuse
- ➢ Data protection-compliant destruction of data carriers
- ➢ Encryption of data carriers
- ➢ Prohibition of mobile external data carriers
- ➢ Secure storage of data carriers outside business hours (locked away)
- ➢ Differentiation of access authorization for files, application programs, and servers/IT

- ➢ Differentiation of processing options into read, modify, delete
- ➢ Testing and approval of application software before use
- ➢ Document shredder
- ➢ Data protection safe

4. Transfer Control/Transmission Control

Transfer control or transmission control ensures that personal data is always protected during transfer between different entities or when disclosed to third parties, and is only transmitted in accordance with applicable data protection regulations. This not only prevents unintentional data leaks but also ensures that data is only shared with those who are authorized to receive it. The following section discusses the mechanisms, policies, and technologies implemented by the processor to ensure secure and compliant data transmission:

- ➢ Authorization concept for network shares and access permissions to folders and files for individual user groups (annual review)
- ➢ Setup of dedicated lines or VPN tunnels
- ➢ Documentation of data recipients and time periods of planned transfer or agreed deletion deadlines
- ➢ Use of security mechanisms for data transmission (all protocols secured via VPN/IPsec, email with S/MIME or PGP, SFTP)
- ➢ Data protection-compliant destruction of data carriers
- ➢ Written data protection obligations from external service providers
- ➢ Supervision of external service providers during their activities
- ➢ Use of firewall, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Virtual Private Network (VPN), content filter
- ➢ IT systems are located in locked rooms / Locking of server consoles
- ➢ Password change after disclosure to an external party
- ➢ Exclusively case-by-case and approved releases for remote maintenance
- ➢ Contractually regulated measures for data/information protection during remote maintenance
- ➢ Revocation of access authorizations when an employee leaves
- ➢ Use of signature procedures
- ➢ Care in selection of transport personnel and vehicles
- ➢ Overview of regular retrieval and transmission processes
- ➢ Personal handover with protocol
- ➢ Secure transport container

5. Input Control

Input control serves to ensure that when data is entered, modified, or deleted, it always remains traceable who entered or modified which data at what time. This section highlights the processes and technologies used by the processor to control the input and verification of data and to ensure its quality and integrity:

- ➢ Traceability of data entry, modification, and deletion through log data, tickets, and usernames
- ➢ Assignment of rights for data entry, modification, and deletion based on an authorization concept
- ➢ Overview of which programs can be used to enter, modify, or delete which data
- ➢ Use of malware protection with automatic updates
- ➢ Regular and timely updates for operating systems and application systems
- ➢ Separate storage of data and programs (directories)
- ➢ Verification of integrity and installation of received programs
- ➢ Complete network documentation
- ➢ Documentation of maintenance, remote maintenance, and repair work
- ➢ Permanent verification of remote maintenance work through continuous recording of remote sessions
- ➢ Data protection-compliant deletion of written data carriers before reuse
- ➢ Retention of forms from which data was transferred to automated processing

6. Order Control/Contract Compliance Control

Order control, also known as contract compliance control, ensures that the processing of personal data by third parties is in accordance with applicable data protection regulations and agreed contractual obligations. It ensures that external partners do not use or modify data on their own authority and that data protection standards are consistently maintained. The following section explains the measures and strategies used by the processor to ensure compliant and secure data processing in the contractual relationship:

- ➢ Formalized order placement
- ➢ Strict selection of service providers
- ➢ Prior review of documentation of security measures taken by the processor
- ➢ Ongoing monitoring of the processor and their activities
- ➢ Change management process for changes in procedures/program changes by the processor
- ➢ Remote maintenance/remote administration only after event trigger from client (logging)
- ➢ Written instructions to the processor (e.g., through data processing agreement)
- ➢ Obligation of processor employees to data secrecy
- ➢ Ensuring destruction of data after completion of the order
- ➢ Effective control rights agreed with the processor
- ➢ Regulation on the use of additional subcontractors

7. Availability Control/Recoverability

Availability control focuses on ensuring that data and systems are accessible at all times, especially when needed, while being protected from unintentional or malicious impairments, whether through technical failures, natural disasters, or targeted attacks. This is not only about protection against data loss, but also about the rapid recovery of data and systems in the event of a failure. This section presents the measures and techniques implemented by the processor to ensure continuous data availability and minimize risks:

- ➢ Uninterruptible power supply (UPS)
- ➢ Surge protection filters
- ➢ Backup data center
- ➢ Emergency and crisis management (BCM)
- ➢ Air conditioning in server rooms
- ➢ Devices for monitoring temperature and humidity in server rooms
- ➢ Protective power strips in server rooms
- ➢ Fire and smoke detection systems
- ➢ Fire extinguishers in server rooms
- ➢ Alert system for alarms within server rooms
- ➢ On-call service in case of disaster
- ➢ Archive policy with restricted access to archive area
- ➢ Creation of a backup & recovery concept
- ➢ Daily and weekly data backup
- ➢ Creation and testing of backup procedures
- ➢ Documentation of backup procedures
- ➢ Hard drive mirroring using RAID procedures
- ➢ Video surveillance in server room
- ➢ Testing of data recovery
- ➢ Storage of data backups at a secure, off-site location
- ➢ Server rooms not located below sanitary facilities
- ➢ Compliance with legal retention periods
- ➢ Testing of recovery

8. Data Separation Control/Multi-Tenancy Control

Data separation control ensures that data sets are isolated from each other according to their specific processing purpose. This not only ensures the preservation of confidentiality and integrity of data, but also compliance with data protection regulations and the avoidance of conflicts of interest. This section describes how the processor implements specific mechanisms and procedures to ensure clear separation of data according to their respective processing purposes:

- ➢ Logical multi-tenant separation (software-based)
- ➢ File separation
- ➢ Creation of an authorization concept
- ➢ Definition of database rights
- ➢ Separation of production and test systems
- ➢ Separation of test and routine programs
- ➢ Separation of test and production data
- ➢ Physical separation (systems/databases/data carriers) available
- ➢ Multi-tenant capability of relevant applications available

9. Organizational Control

The goal of organizational control is to adapt the internal company structure to meet the specific requirements of data protection. The focus is on ensuring that the organization designs its processes and procedures to comply with data protection regulations, rather than adapting data protection to the existing structure. The following section explains the specific measures and strategies implemented by the processor to ensure effective organizational control:

- ➢ Written regulations on operation and procedures of data processing
- ➢ Employees are obligated not to incorporate information from client data sets into other projects/purposes
- ➢ Holiday and sick leave coverage for management and IT managers
- ➢ Written program release procedure
- ➢ Separation of functions in IT area
- ➢ Reconciliation and control procedures
- ➢ Determination and definition of current state of technology
- ➢ Assessment of likelihood and severity of risk to the rights and freedoms of natural persons
- ➢ Evidence of regular employee training on data protection
- ➢ Expert Data Protection Officer appointed in writing (law firm)
- ➢ Data protection policy
- ➢ Documented process for detecting and reporting security incidents/data breaches (including reporting obligation to supervisory authority)
- ➢ Documentation of data breaches and security incidents
- ➢ Formal process and responsibilities for follow-up of security incidents and data breaches

***Appendix 3* – approved subcontractor**

subcontractor	**adress**	**affected platform**	**service**	**Server location**
Microsoft Ireland Operations Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland	all products	Data processing on the Office 365 platform Backups	data centre in Amsterdam & Dublin
Google Commerce Limited	Gordon House, Barrow Street 4, Dublin 4, Ireland	MEA-Frontend MEA-Backend Polario	hosting of the application and backend when using cloud deployment Backups hosting of tracking tools	data centre in Frankfurt
all-inkl.com	Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland	MEA-Frontend MEA-Backend Registr-Frontend Frontende of Pre-Event-Page Web-modules	deployment of interfaces hosting of the formula tool	data centre in Dresden
Freshworks GmbH	Alte Jakobstraße 85/86, 10179 Berlin, Deutschland	all products	ticket system and IT helpdesk	data centre in Frankfurt
3Q GmbH	Kurfürstendamm 102, 10711 Berlin, Deutschland	MEA Polario	streaming and hosting of media data (recordings)	data centre within the EU
Sendbird	400 1st Ave,San Mateo, CA 94401, USA	Polario	chat, text messages and comments	data centre in Frankfurt
MongoDB	1633 Broadway, 38th Floor, New York, NY 10019, USA	Polario	database hosting	data centre in Frankfurt
SINCH Mailjet	Office Location, Paris HQ,43 rue de Dunkerque, 75010 Paris, France	MEA Polario	e-mail services	data centre within the EU
Slido	Sli.do s.r.o.,Vajnorská 100/A, 831 04 Bratislava, Slovakia	MEA Polario	surveys	data centre within the EU

Appendix 4 – Persons authorized to issue instructions

<u>Persons/department of the client authorized to issue instructions:</u>

serial number:	1
name:	
organizational unit:	
contact details:	

serial number:	2
name:	
organizational unit:	
contact details:	

<u>Departments of the contractor authorized to issue instructions:</u>

serial number:	1
name:	project manager **Customer Support**
organizational unit:	**Nicole Sauter**
contact details:	**support@plazz.ag**