Agreement

Processing of personal data on behalf of a controller in accordance with Article 28 EU General Data Protection Regulation (GDPR)

(***)

Note: *please insert name and address of contract partner*

– hereinafter referred to as **"Controller"** –

and

cadooz GmbH

Osterbekstrasse 90b

22083 Hamburg, Germany

– hereinafter referred to as **"Processor"** –

– each a "**Party**" –

– referred to collectively as "the **Parties**" –

herewith conclude the following agreement ("Agreement") pertaining to the processing of the Controller's personal data by the Processor:

Section 1 General

1. The subject of this Agreement is the processing of personal data in connection with the orders over the Quickorder function, to be carried out by the Processor for the Controller on the basis of the order transaction of[date of order transaction] .

2. This Agreement contains a written request to carry out contract data processing within the meaning of Article 28(3) of the General Data Protection Regulation ("GDPR"), and gives concrete form to the rights and obligations incumbent on the Parties pursuant to the GDPR and the respective national data protection legislation insofar as the Processor processes personal data on the Controller's behalf. This Agreement shall apply to all activities, which are related to the orders over the Quickorder function during the course of which the Processor's employees or employees of third parties engaged by the Processor ("Sub Processors") come into contact with the Controller's personal data.

3. Each Party shall comply with the obligations arising for it from the respective applicable data protection law.

Section 2 Scope and Purpose of Processing

1. The data shall be processed solely for the provision of the contractual services of the orders over the Quickorder function in the Incentive Mall

2. The data subjects, the categories of personal data, and the purpose and scope of the processing on behalf are described in **Appendix 1**.

3. The scope of those data categories specified in **Appendix 1,** which are subject of the Agreement, may be supplemented or amended by the Parties at any time; special provisions may likewise be expressly agreed in individual cases.

Section 3 Controller Obligations

1. Within the scope of this Agreement, the Controller is the "Controller" within the meaning of Article 4(7) GDPR.

2. The Controller is solely responsible for assessing the lawfulness of the data processing activities pursuant to Article 6(1) GDPR and for complying with the rights of data subjects pursuant to Articles 12 to 22 GDPR. In particular, the Controller is responsible for fulfilling its statutory information and transparency obligations towards its end-customers and, furthermore, for ensuring that there is a lawful and effective legal basis (e.g. consent) for the processing of the Controller's personal data. Should third parties assert claims against the Processor based on data processing, he Controller shall indemnify the Processor against all such claims upon first request. This shall not apply if the Processor has intentionally or grossly negligently violated this Agreement and/or applicable law.

3. The Controller shall be responsible for providing the Processor with data in good time for the performance of the service in the required quality and only to the extent required.

4. The Controller has the right to issue additional instructions at any time. Should these additional instructions go beyond the contractual obligations arising in the orders over the Quickorder function in the Incentive Mall, the Controller shall bear the necessary and reasonable additional costs incurred thereby; the Processor is entitled to request payment in advance. The Processor may refuse to carry out additional or modified data processing activities if these would significantly increase its workload or if the Processor refuses to pay in advance or reimburse additional costs.

5. The Controller shall notify the Processor without undue delay if it notices any errors or irregularities arising in connection with the Processor's processing of the data.

6. The Controller shall be responsible for the information obligations arising from Articles 33 and 34 GDPR vis-à-vis the supervisory authority or any data subject in the event of a personal data breach.

Section 4
Processor Obligations

1. The Processor shall process the data solely within the scope of the Agreements concluded and in accordance with the Controller's documented instructions. The same applies to the transfer of personal data to a third country or an international organization unless the Processor is obliged to process this personal data. In such a case, the Processor shall inform

the Controller of this legal obligation before processing the data unless the applicable law forbids this in the public interest.

2. The Processor shall notify the Controller without undue delay if it believes that an instruction given by the Controller violates applicable law. In such cases, the Processor shall be entitled to suspend the execution thereof until the instruction is confirmed or modified by the Controller.

3. The Processor shall guarantee that the persons authorized to process the personal data have been bound to secrecy or are subject to an appropriate statutory confidentiality undertaking. Furthermore, all persons who are able to access the Controller's personal data must be bound to secrecy and instructed on their data protection obligations.

4. Pursuant to Art. 28(3) e) GDPR, the Processor shall, insofar as this is possible, assist the Controller with the implementation of suitable technical and organizational measures so that the Controller can fulfill its obligations towards the data subject pursuant to Chapter III GDPR, e.g. information and communication with the data subject, the rectification or erasure of data, restrictions on processing, the right to data portability, and the right to object.

5. As specified in Art. 28(1) GDPR, the Processor shall provide sufficient guarantees regarding the technical and organizational measures implemented in order to guarantee that the data is processed in compliance with the GDPR while upholding the data subject's rights. The Contract Processor shall implement suitable technical and organizational measures that meet the specifications in Art. 32 GDPR in order to guarantee an appropriate level of protection against risk.

5. The Processor shall not transfer the data outside the European Economic Area without the Controller's prior written consent unless it has taken the steps necessary to ensure that the transfer is in compliance with Art. 44ff. GDPR.

6. The measures currently implemented by the Processor are described in **Appendix 2** to this Agreement.
   These technical and organizational measures are subject to technical progress and further developments. The Processor shall be permitted to implement adequate alternative measures insofar it is ensured that the contractually agreed level of protection is maintained. Significant changes shall be agreed with the Controller.

7. Pursuant to Art. 28(3) f) GDPR, the Contract Processor shall cooperate with the performance of the data protection impact assessment specified in Art. 35 GDPR and the prior consultation with the supervisory authorities specified in Art. 36 GDPR.

8. The Processor is aware that the Controller is obliged to maintain extensive documentation of all personal data breaches and, if applicable, to report these to the supervisory authorities and the data subject within 72 hours. If such breaches have occurred, the

Processor shall assist the Controller with the fulfillment of its reporting obligations in accordance with Art. 28(3) f) GDPR.

Section 5 Relationships with Sub Processors (Sub Processors)

1. The Controller grants its general consent to the engagement of Sub Processors as additional processors within the meaning of the GDPR, provided

   a) the Processor notifies the Controller in advance of any intended change with respect to the engagement of any additional Sub Processor or the replacement of an existing Sub Processor;
   b) the Processor enters into a written agreement with the Sub Processor which ensures that the level of data protection is at least as high as the level specified in this Agreement;
   c) the statutory provisions of Art. 44ff. GDPR are complied with when subcontracting relationships are established with Sub Processors that are not domiciled in Germany, a member state of the European Union or another state that is a party to the Agreement on the European Economic Area ("Third Countries").
   d) the Processor remains responsible for any violations of this Agreement which are caused by actions (acts, tolerance or omissions) of any Sub Processor engaged.

2. The Processor shall use the Sub Processors specified in **Appendix 3** to this Agreement; their use shall be deemed to have been approved when the Agreement was signed.

3. The Controller is entitled to object to the appointment or replacement of a Sub Processor by the Processor before such a Sub Processor is appointed or replaced if this objection is based on legitimate reasons related to data protection. In this event, the Processor shall either refrain from appointing or replacing its additional processor; alternatively, where this is not possible, the Controller may suspend or terminate this Agreement (notwithstanding any fees that are incurred by the Controller before the Agreement is suspended or terminated).

Section 6 Supervisory Powers

1. The Controller has the right to monitor the Processor's and Sub Processors' compliance with the statutory data protection regulations and/or the contractual provisions agreed by the Parties and/or the instructions given by the Controller at any time and to the extent necessary. To this end, the Controller may (1) obtain voluntary information from the Processor and (2) request the Processor to submit an expert assessment testifying to the Processor's compliance with the applicable data protection standards. Following a written request by the Processor, evidence that the applicable data protection standards (including but not limited to the technical and organizational measures specified in **Appendix 2**) are being complied with may be provided by submitting the current audit report. Any disclosure of confidential information relating to internal security procedures is excluded.

2. The Processor guarantees that upon receiving a written request, it shall (i) hold a meeting with the Controller's security team to discuss any questions relating to data protection or data security that the Controller may have, or (ii) fill out a questionnaire provided by the Controller or a third party acting on the Controller's behalf relating to the Processor's compliance with the application data protection legislation, whereby the Processor is not obliged to disclose information that can be correctly classified as confidential information relating to the Processor's business operations. This shall not affect the Controller's rights pursuant to section 6.1.

3. Controlled attempts to penetrate the computer systems and networks of the Processor and/or its Sub Processors with the aim of identifying any weak points (penetration test) shall constitute part of the annual audit of the Processor and its Sub Processors. Any disclosure of confidential information relating to internal security procedures is ruled out.

Section 7 Liability

1. If a data subject suffers damages as a result of the contractual data processing activities and consequently claims compensation from the Controller, the Processor shall be liable to the Controller according to its share in the responsibility for the damage caused within the context of the internal relationship if

    a. the Processor culpably failed to meet the obligations incumbent on it as the Contract Processor pursuant to this Agreement, the GDPR or other data protection legislation applicable to the contractual data processing activities, or

    b. the Processor culpably failed to follow the instructions legally issued by the Controller or acted culpably against these instructions.

2. If a data subject suffers damages as a result of the contractual data processing activities and consequently claims compensation from the Processor although the Processor is not responsible for the damages, the Controller shall waive the Processor's liability within the context of the internal relationship.

3. Otherwise the provisions in Article 82 GDPR shall apply.

Section 8 Duration and Termination

1. The Agreement shall remain valid for as long as the Processor is processing personal data on behalf of the Controller's in accordance with this Agreement. This does not affect the right to terminate the Agreement without notice for good cause remains unaffected.

2. Upon termination or expiration of the Contract or upon request of the Controller, the Processor shall, at the Controller's discretion, destroy or return to the Controller all data in its possession or under its control. This requirement shall not apply to the extent that the Processor is required by applicable law to retain part or all of the personal data, or relates

to personal data that was archived on back-up systems and must be safely isolated and protected from any further processing unless this is required by law.

_____	_____
Place, (date)	Hamburg, (date)
_____	_____
(*)	cadooz GmbH

Appendix 1: OBJECT OF COMMISSIONED DATA PROCESSING

[PLEASE CHECK THE FOLLOWING POINTS, INCLUDE 1-2 SENTENCES ON THE SERVICES IN SECTION 1, AND CHECK THE CORRESPONDING POINTS IN SECTIONS 2 AND 3 IN ACCORDANCE WITH THE CONTROLLER AGREEMENT AND SERVICE (E.G. CADOOZCARD PLUS)]

1. Object of commissioned data processing

The Processor shall provide the following services which are the subject of this processing on behalf:

The transaction and Selling of vouchers over the Quickorder function

2. Types of personal data

The following types/categories of data are the object of the contract processing activities:

- ☒ Personal master data
- ☒ Communication data (e.g. phone number, email address)
- ☐ Contract master data (contractual relationship, interest in products and/or a contract)
- ☐ Customer history
- ☒ Contract billing and payment data
- ☒ Bank data (account number, bank code or IBAN)
- ☐ Planning and control data
- ☐ Reported data (from third parties, e.g. credit bureaus, or from public directories)
- ☐ Special types of personal data

3. Categories of data subject

The following categories of data subjects are affected by the contract processing activities:

- ☒ Customers
- ☒ Interested parties
- ☐ Subscribers
- ☐ Employees
- ☐ Suppliers
- ☐ Sales representatives
- ☐ Contacts
- ☐ Minors
- ☐ Retailers

Appendix 2: TECHNICAL AND ORGANIZATIONAL MEASURES (TOM)

The minimum technical and organizational measures designed to guarantee data protection and data security that must be implemented and continually maintained by the Processor are specified below. The objective is to guarantee in particular the confidentiality, integrity and availability of the information processed by CADOOZ.

1. Pseudonymization and encryption of personal data (Art. 32 (1a) GDPR)

- **Pseudonymization**

  The processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures.

  Description of the measures taken:

  The provision of the contractually agreed services (e.g. handling and processing of orders; support and other services) requires the processing of personal data. The purposes of the processing activity cannot be achieved by pseudonymization, i.e. without a direct reference to the person.

- **Encryption**

  Use of procedures and algorithms that convert the content of personal data into a non-readable form using digital and/or electronic codes or keys. Symmetric or asymmetric encryption technology may be considered:

  Description of the measures taken:

  ☒ Encryption of

  - ☐ Mobile data media
  - ☒ Data media in laptops
  - ☐ Data on data media

  ☒ Protection of data during electronic transfer

  - ☒ Establishment of dedicated lines and/or VPN tunnels
  - ☒ Disclosure of data in anonymized form (e.g. reports)
  - ☒ Encrypted transfer (e.g. HTTPS, SSL, SSH, [algorithm], [number]-bit keys)
  - ☒ Email encryption
  - ☒ Encryption of data

2. Measures to ensure the confidentiality, integrity, availability and reliability of the systems (Art. 32 (1b) GDPR)

- **Access control with respect to premises**

  Unauthorized persons must not be allowed access to data processing systems that are used to process or use data.

  Description of the measures taken:

  ☒ Alarm system

  ☒ Securing of building shafts

  ☒ Rules for visitors

  ☒ Identity check at the reception

☒ Automatic access control system

☒ Locking system with code locks

☒ Lockable cabinets

☒for offices

☒ for the server room/rooms

☒ Video surveillance of access points

☒ Light barriers / motion sensors

☒ Security locks

☒ Access card rules

☒ Logging of visitors / visitor log

☒ Obligation for visitors to carry a visitor badge

☒ Careful selection of cleaning staff

☒ Obligation for employees to carry a badge

Measures to protect the server room:

☒ Security locks

☒ Automatic access control system

☒ Logging of visitors / service providers (e.g. providers of maintenance services)

- **Access control with respect to systems**

  Unauthorized persons must be prevented from using data processing systems.

  Description of the measures taken:

  ☒ Allocation of user access rights

  ☒ Creation of user profiles

  ☒ Password policy

  ☒ Automatic expiration of passwords after a certain period of time

  ☒ Password quality (special characters, length)

  ☒ Authentication with user name / password

  ☒ Automatic locking of computers after a specified period of inactivity

  ☒ Automatic logout from programs after a specified period of inactivity

  ☒ Allocation of user profiles to IT systems

  ☒ Housing locks

  ☒ Use of VPN technology

  ☒ Blocking of external interfaces (USB, etc.), possibly approval management

  ☒ Use of intrusion detection systems

  ☒ Use of central smartphone administration software (e.g. for the remote erasure of data)

  ☒ Use of antivirus software

  ☒ Use of a hardware firewall

  ☒ Use of a software firewall

  ☒ Use of personal storage media is prohibited

- **Access control with respect to specific data**

  It must be ensured that the persons authorized to use a data processing system can only access data that they are authorized to access. There must be no way to read, copy, alter or remove personal data without authorization during their processing or use or after they have been recorded.

  Description of the measures taken:

☒ Authorization concept

☒ Management of rights by the system administrator

☒ Number of administrators reduced to the lowest possible number

☒ Logging of access to applications, in particular with respect to the input, alteration and erasure of data

☒ Logging of failed login attempts

☒ Secure storage of data media

☒ Physical erasure of data media before they are used again

☒ Proper destruction of data media by external service providers

☒ Use of document shredders and/or service providers (where possible with privacy seal accreditation)

☒ Logging of the destruction of data

☒ Employees have been placed under the obligation to treat data as confidential and to comply with data protection regulations

-

- **Separation control**

  It must be possible to separately process data that were collected for different purposes.

  Description of the measures taken:

  ☒ Physically separate storage on separate systems or data media

  ☒ Logical Controller separation (through software)

  ☒ Creation of an authorization concept

  ☒ Addition of purpose attributes / data fields to data sets

  ☒ Definition of database rights

  ☒ Separation of operational and testing systems

- **Disclosure control**

  It must be ensured that personal data cannot be read, copied, altered or removed without authorization during their electronic transfer or during transport or while they are being recorded on data media. It must be possible to verify (including subsequently) to which bodies personal data is supposed to be transferred using data communication equipment.

  Description of the measures taken:

  ☒ Documentation of the recipients of data

  ☒ Rules for the safe and confidential decommissioning of devices containing data media (hardware) before they are passed on

  ☒ Logging (e.g. in the directory of processing activities)

  ☒ Email encryption

  ☒ Storage on SFTP server

- **Input control**

It must be ensured that it is possible to subsequently verify and establish whether and by whom personal data was entered into, altered in, or removed from data processing systems.

Description of the measures taken:

☒ Transparent input, alteration and erasure of data

☒ by individual user names (not user groups)

☒ Assignment of rights for the input, alteration and erasure of data based on an authorization concept

3. Availability control and the ability to restore access in a timely manner (point (c) of Article 32 GDPR)

Personal data must be protected against accidental destruction or loss.

Description of the measures taken:

☒ Uninterruptible power supply (UPS)

☒ Air conditioning in server rooms

☒ Devices to monitor the temperature and humidity in server rooms

☒ Surge protector power strips in server rooms

☒ Fire and smoke detection systems

☒ Fire extinguishers in server rooms

☒ Alarm signal in the event of unauthorized access to server rooms

☒ Emergency plan (backup and recovery concept)

☒ Virus protection / firewall

☒ Storage of data backups at a secure, external location

4. Procedures for the regular review, assessment and evaluation of the technical/organizational measures (Art. 32 (1d) GDPR; Art. 25. (1) GDPR)

- **Assignment control**

  It must be ensured that personal data being processed on behalf of the Controller can only be processed in accordance with the Controller's instructions.
  Description of the measures taken:

  ☒ Selection of the Processor based on due diligence criteria (in particular with respect to data security)

  ☒ Prior review and documentation of the security measures implemented at the Processor's company

  ☒ Written instructions to the Processor (e.g. in a data processing contract) within the meaning of Art. 28 GDPR

  ☒ The Processor has appointed a data protection officer

  ☒ The Controller has been granted effective rights to inspect the Processor's work

- **IT emergency management**

  ☒ Emergency manual is available

☒ Responsibilities for responses and response times have been defined

- **Data protection through technological design and "privacy by default" settings**

  ☒ Selection of "privacy-friendly" technology in the procurement process

- **Data protection management**

  ☒ Appointment in writing of a data protection officer

  ☒ Monthly review of access rights by the IT security officer (Euronet Group)

  ☒ The data protection officer will be included in any data protection impact assessment

  ☒ Employees and data protection: GDPR training (on location) and the obligation to take regular WOMBAT security tests

  ☒ Employees have been placed under the obligation to treat data as confidential and to comply with data protection regulations

  ☒ Maintenance of directories of processing activities as specified in Art. 30(1) GDPR

Contact data of the data protection officer of cadooz GmbH:

Yago Amat Martinez
Cadooz GmbH
22083 Hamburg, Germany
datenschutz@cadooz.de

Appendix 3: APPROVED SUBPROCESSORS (ADDITIONAL PROCESSORS) ACCORDING TO SECTION 5.2 of the Agreement

[PLEASE CHECK CONTROLLER AGREEMENT TO ASCERTAIN WHICH SUB PROCESSORS ARE USED TO PROVIDE THE RESPECTIVE SERVICES. PLEASE DELETE THOSE THAT DO NOT APPLY]

Sub Processor	**Address/country**	**Service**
transact Elektronische Zahlungssysteme GmbH	Fraunhoferstrasse 10 82152 Martinsried	Services with respect to redemption and questions relating to orders
PVS Fulfillment-Service GmbH	Heinz-Nixdorf-Strasse 2 74172 Neckarsulm	Sending of rewards
Fulfillers	Frankfurter Strasse 2 65527 Niederhausen	Service provider for clearing and service
VERITAS DATA GmbH	Bunsenstrasse 20 64293 Darmstadt	Service provider for clearing and IT service (landing page)
s!ncNOVATION GmbH	Hammerbrücker Strasse 3 08223 Falkenstein	Service provider in the area of producing the cadoozCardBC
PAV Card GmbH	Hamburger Strasse 6 22952 Lütjensee	Service provider in the area of producing the cadoozCard / cadoozCardBC
Wirecard Card Solutions Ltd.	Grainger Chambers 3-5 Hood Street Newcastle upon Tyne NE1 6JQ (UK)	Service provider in the area of the financial management (banking license) of the cadoozCard
gevekom GmbH	Altplauen 19 01187 Dresden	Services relating to the processing of support queries