Data Processing Agreement according to Art. 28 GDPR

between

CCV GmbH
Gewerbering 1
84072 Au i. d. Hallertau
Germany

(- the Processor – hereinafter referred to as the Supplier -)

and

(- the Controller - hereinafter referred to as the Client -)

[if applicable: representative according to Art. 27 GDPR:

………………………………………………………………………………………]

1. Subject and duration of the agreement

(1) Subject

The object of the data handling order is defined in the main service agreement(s). The Supplier shall generally perform the following tasks, whereby not all listed services are used by the Client:

1.1 Remote management of terminals

1.2 Subsequent posting of payments for customers in the event of errors

1.3 Provision and operation of an app-based POS system

1.4 Provision and operation of a customer portal "MyCCV”

1.5 Management of gift cards, hosting of gift card data

1.6 Inspection, repair or refurbishment of CCV products

1.7 Provision of customer support

1.8 Provision of a customer portal for transaction reporting

1.9 Processing of transactions

1.10 Payment processing via trust account

1.11 Provision and operation of the CCV-Store

1.12 Sending postal invoices

1.13 Open Application Manager: Development and hosting of payment-related extension modules

(2) Duration

The duration of this contract (term) corresponds to the term of the service agreement.

2. Specification of the Contract Details

(1) Nature and Purpose of the intended Processing of Data

Detailed description of the Subject Matter with regard to the nature and purpose of the services provided by the Supplier:

To 1.1: Software updates, whereby the configuration data and log files of the terminals are processed and stored in the TKS or TMS system.

To 1.2: Documents sent in by customers are subsequently posted manually by Customer Service Direct Business.

To 1.3: Provision of a POS system, hosting of customer and consumer master data, remote maintenance, setup of the POS system, creation of customer master data, on-site service, payment processing via terminal connection, MMS administration with Meraki, sending of receipts to consumer e-mail, employee administration, support service.

To 1.4: "MyCCV" platform for CCV customers to centrally manage CCV products. Central boarding for customers, enabling transaction reports in a DATEV format.

To 1.5: Value added system that allows consumers to sell gift cards and manage gift card data.

To 1.6: Inspection, repair or refurbishment of hardware, backup of device data and log files, updating of software.

To 1.7: Handling of customer enquiries regarding technical and commercial problems and requests. Provision of an upload and download platform for data exchange. Provision of an activation code for the installation of automatic terminals (4eye Tool).

To 1.8: Web service with customer login to monitor transaction data.

To 1.9: Processing of cashless payment transactions in terminals and web shops.

To 1.10: Bundling of payment transactions and payment via CCV trust account incl. monitoring.

To 1.11: Closed App Store "CCV-Store" to provide CCV products and 3rd party applications.

To 1.12: Production and transport of digitally delivered items by classic letter post.

To 1.13: Function modules can be added to extend the scope of services of the payment application. The function modules are developed (OAM interface) and hosted (OAM server).

The undertaking of the contractually agreed Processing of Data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA).

(2) Type of Data

The processing of personal data is subject to the following data types/categories (enumeration/description of data categories):

To 1.1: Salutation, first and last name (title if applicable), address, e-mail address, telephone number, fax number, terminal ID, IP address, signature of consumer.

To 1.2: Salutation, first name and surname (title if applicable), address, card number, car number, account number.

To 1.3: Salutation, first name and surname (title if applicable), address, telephone and fax number, e-mail address, tax identification number, bank details, article details, consumer's signature.

To 1.4: Salutation, first and last name (title if applicable), address, telephone and fax number, e-mail address, IP address, date of birth, contract billing and payment data, bank details, consumer e-mail address, consumer name, copy of customer's identity card, extract from customer's commercial register, VAT ID.

To 1.5: Customer data.

To 1.6: Salutation, first name and surname (title if applicable), address, telephone and fax number, e-mail address, card numbers, account number, IP address, signature, vehicle registration number, article data.

To 1.7: Salutation, first name and surname (title if applicable), address, telephone and fax number, e-mail address, card numbers, account number, IP addresses, date of birth, telephone number, vehicle registration number, signature, article data.

To 1.8: E-mail address, customer number, Terminal ID, VU number.

To 1.9: Salutation, first name and surname (title if applicable), telephone number, card number (like PAN), account number, IP address, vehicle registration number, signature, article data.

To 1.10: Salutation, first and last name (title if applicable), e-mail address, telephone and fax number, signature, payment data (sales data, transaction data, etc.), contract billing data, bank details, contract partner number, contract data, configuration data of the technical interfaces (IP addresses, PC configurations, etc.), configuration data for administration programs and online portals, copy of the customer's ID card, excerpt from the commercial register of the customer, sales VAT ID of the customer.

To 1.11: Salutation, first and last name (title if applicable), address, e-mail address, telephone number, fax number, location data.

To 1.12: Salutation, first and last name (title if applicable), address, contract data, contract billing and payment transaction data, position/function, mandate number.

To 1.13: Salutation, first name and surname (title if applicable), address, e-mail address, telephone number, fax number, terminal ID, IP address, company number, consumer's signature.

(3) Categories of Data Subjects

The categories of data subjects to be processed shall include:

To 1.1: Customer, consumer

To 1.2: Customer

To 1.3: Customer, prospect

To 1.4: Customer, consumer

To 1.5: Customer

To 1.6: Customer, consumer

To 1.7: Customer, consumer

To 1.8: Customer

To 1.9: Customer, consumer

To 1.10: Customer, consumer

To 1.11: Customer, cooperation partner

To 1.12: Customer

To 1.13: Customer, consumer

3. Technical and Organizational Measures

(1) The Supplier shall document the implementation of the technical and organizational measures set out and required prior to the award of the contract prior to commencement of processing, in particular with regard to the actual execution of the contract, and shall hand them over to the Client for inspection. If accepted by the Client, the documented measures become the basis of the order. If the client's inspection/audit reveals a need for adjustment, this must be implemented by mutual agreement.

(2) The Supplier shall establish the security in accordance with Art. 28 Para. 3 lit. c and Art. 32 GDPR in particular in conjunction with Art. 5 Para. 1 and 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 Para. 1 GDPR must be taken into account. [Details in Appendix 1].

(3) The technical and organizational measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client. Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.

(2) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Art. 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

a) The Supplier undertakes to appoint a Data Protection Officer in writing who will carry out his duties in accordance with Art. 38 and 39 GDPR. The Data Protection Officer can be contacted as follows:
E-Mail: datenschutz@ccv.eu
Phone: +49-8752 864 0

b) Confidentiality in accordance with Art. 28 Para. 3 Sentence 2 lit. b, 29 and 32 Para. 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarized with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all technical and organisational measures necessary for this Order or Contract in accordance with Art. 28 Para. 3 Sentence 2 lit. c, Art. 32 GDPR [Details in Appendix 1].

d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.

e) The Client shall be informed immediately of any inspections and measures conducted by the Supervisory Authority, insofar as they relate to this order or contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this order or contract.

f) Insofar as the Client is subject to an inspection by the Supervisory Authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the order or contract data processing by the Supplier, the Supplier shall make every effort to support the Client.

g) The Supplier shall periodically monitor the internal processes and the technical and organizational measures to ensure that processing within his area of responsibility is in accordance with the requirements of applicable Data Protection Law and the protection of the rights of the Data Subject.

h) Verifiability of the technical and organizational measures conducted by the Client as part of the Client's supervisory powers referred to in paragraph 7 of this Agreement.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. However, the Supplier shall be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Client's data, even in the case of outsourced ancillary services.

(2) The Client agrees that the Supplier may commission subcontractors (further processors) to perform the services. Where the Supplier places orders with subcontractors, the Supplier shall become the main Supplier. The Supplier shall inform the Client of any change in the involvement or replacement of subcontractors prior to such change. The Client has the right to object to this. The main Supplier shall also be obliged to impose the obligations arising from this Data Processing Agreement on each subcontractor. The following subcontractors are currently processing relevant data:

Subcontractor	Address	Service
CCV Group B.V.	Westervoortsedijk 55 6827 Arnheim Netherlands	Operating of the backend systems for 1.1 (only TMS; TKS is operated by Supplier), 1.4 and 1.9

PAYONE GmbH	Lyoner Straße 9 60528 Frankfurt Germany	Backend-System for 1.2 and 1.9
Samhammer AG	Zur Kesselschmiede 3 92637 Weiden Germany	Support for 1.7
Volksbank in der Ortenau eG	Okenstraße 7 77652 Offenburg Germany	Provision of the interim account for 1.10
Continum AG	Bismarckallee 7b-d 79098 Freiburg Germany	Computer center for the backend systems for 1.9, 1.11, 1.13
Deutsche Post ePost	Moltkestr. 14 53173 Bonn Germany	Dispatch of postal invoices for 1.12
CCV Lab BVBA	Spinnerijstraat 99 bus 12 8500 Kortrijk Belgium	Provision of the services for 1.3 and 1.5
Concardis GmbH	Helfmann-Park 7 65760 Eschborn Germany	Backend-System for 1.2, 1.9

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors´ commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. Otherwise, the involvement of subcontractors outside the EU/EEA is not permitted.

(5) Further outsourcing by the subcontractor requires the express consent of the main Client (at the minimum in text form). All contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this Agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Art. 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the technical and organizational measures.

(3) Evidence of such measures, which concern not only the specific order or contract, may be provided by compliance with approved Codes of Conduct pursuant to Art. 40 GDPR.

(4) The Supplier may claim remuneration to enable the Client to carry out controls, which go beyond one day.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Art. 32 to 36 GDPR. These include:

a) Ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.
b) The obligation to report a personal data breach immediately to the Client.
c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client for his possibly necessary data protection impact assessment.
e) Supporting the Client with regard to prior consultation of the Supervisory Authority.

(2) The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).

(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.

(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data protection compliant manner as far as possible and reasonable. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request.

(3) Documentation which is used to demonstrate orderly data processing in accordance with the order or contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods as far as possible and reasonable. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Au i. d. Hallertau, ____________________	________________________________
Place, Date	Place, Date
________________________________	________________________________
Stamp, Signatures CCV GmbH	Signature Client

Appendix 1 – Technical and Organizational Measures

1. Confidentiality (Art. 32 Para. 1 lit. b GDPR)

Physical access control

Measures preventing unauthorised persons from gaining access to data processing equipment used to process or use personal data.

- Electronic locking system (chip cards)
- Key provision
- Alarm system
- Visitor regulation by protocoling
- Obligation to wear authorisation cards
- Careful selection of cleaning personnel

Internal access control

Measures to prevent data processing systems from being used by unauthorised persons.

- Assignment of user rights
- Use of secure passwords with expiration time
- Forcing automatic lock mechanisms and complexity requirements
- Locking of external interfaces (USB etc.)
- Use of anti-virus software
- Use of VPN technology

Electronic access control

Measures to ensure that persons authorised to use a data processing system have access only to data covered by their right of access and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after storage.

- Authorization concept
- Administration of rights by system administrator
- Password policy incl. password length and password change
- Secure storage of data media
- Use of document shredders or service providers

Isolation control

Measures to ensure that data collected for different purposes can be processed separately.

- Authorization concept
- Definition of database rights
- Separation of productive and test system

Pseudonymisation and encryption (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

Is carried out and recorded according to legal requirements or at the request of those affected or the Client. Encryption is used with mobile data carriers.

2. Integrity (Art. 32 Para. 1 lit. b GDPR)

Data transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during their electronic transmission or during their transport or storage on data carriers, and to verify and establish the entities to which personal data are to be transmitted by means of data transmission.

- Only encrypted data transmission paths are used
- Only encrypted data carriers are used
- Installation of dedicated lines or VPN tunnels
- Email encryption

Data entry control

Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified or removed in data processing systems.

- Entries are partially automated, manual processing of the data is then not planned
- Use of logging mechanisms such as document management and ticket systems
- Traceability of input, modification and deletion of data by individual usernames (not user groups)
- Allocation of rights to enter, change and delete data on the basis of an authorization concept

3. Availability and Resilience (Art. 32 Para. 1 lit. b GDPR)

Availability control

Measures to ensure that personal data are protected against accidental destruction or loss.

- Storage of data backup at a secure, outsourced location
- Air conditioning in server rooms
- Automatic deletion system in server rooms
- Existing backup and recovery concept
- Contingency plan
- Server room not under sanitary facilities

Rapid recoverability (Art. 32 Para. 1 lit. c GDPR)

Measures to ensure that data access is restored as quickly as possible after an interruption.

- Existing backup and recovery concept
- Cold Standby Systems
- Shadow copies

4. Procedures for regular testing, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

Data Protection-Management

Measures to ensure that the requirements of the GDPR are implemented in a verifiable manner.

- Regular data protection audits
- Internal revision
- Annual Staff Privacy Trainings

Incident-Response-Management

Measures to ensure that, following a malfunctioning, the contracting entity receives information on the malfunctioning in so far as its data are concerned.

- Provision of information by the Contact Center

Data protection-friendly default settings (Art. 25 para. 2 GDPR)

Measures to ensure that personal data are deleted after a specified period.

- Manual software support
- Manual deletion according to legal requirements
- Manual deletion on request

Order control

Measures to ensure that personal data which are processed on instructions can only be processed in accordance with the instructions of the Client.

- Data will not be processed without a concrete order
- Written commitment of employees to data secrecy
- Careful selection of subcontractors
- Data processing agreements concluded with subcontractors