ORDER PROCESSING AGREEMENT (AVV)

Between	and
	Candis GmbH
	CityQuartier DomAquarée
	Karl-Liebknecht-Strasse 5
	10178 Berlin
– following: **“client”** –	– following: **"contractor"** –

Preamble

This appendix specifies the data protection obligations of the contracting parties, which arise from the order processing described in detail in the contractual relationship in the user agreement and the general terms and conditions. It applies to all activities that are related to the contractual relationship and in which the contractor's employees or third parties commissioned by the contractor may come into contact with the client's personal data.

Appendices 1 and 2 are part of this agreement.

1. Subject, duration and specification of order processing

1.1 The user agreement determines the subject matter and duration of the order as well as the type and purpose of the processing. In particular, the following data is part of the data processing:

Type of data	Type and purpose of data processing	Categories of data subjects
Bank data (account details, PIN / password, bank transaction data, credit card numbers, Paypal email addresses, [contractual partner and contractual data of the customer, if applicable, type of contract, if applicable, data from third parties from the account overview: name, IBAN, purpose of transfer, amount])	Processing for the purpose of fulfilling the contract and guaranteeing the CANDIS functions. Processing to operate the accounting software (web app and mobile app), offering and ensuring the optional credit card function	Customers, employees, suppliers, if applicable, interested parties
Company data (name, address, contact person, VAT ID, telephone numbers, email addresses, fax numbers, IPs)	Processing for the purpose of fulfilling the contract and guaranteeing the CANDIS functions.	Customers, employees, suppliers, if applicable, interested parties

1.2 The term of this appendix depends on the term of the contract, unless the provisions of this appendix result in additional obligations.

2. Scope and responsibility

2.1 The contractor processes the data on behalf of the client. This includes activities that are specified in the contract and the service description. Within the scope of this agreement, the client is solely responsible for compliance with the legal provisions of data protection laws, in particular for the lawfulness of the data transfer to the contractor and for the lawfulness of data processing ("controller" within the meaning of Article 4 No. 7 of the EU General Data Protection Regulation (GDPR).

2.2 Instructions are initially set out in the contract and can then be changed, supplemented or replaced by the client in written form or in text form with individual instructions (individual instructions). Instructions that go beyond the contractually agreed service are treated as a request for a change in service. Oral instructions must be confirmed immediately in writing or in text form.

2.3 Due to this responsibility, the client can request the correction, deletion, blocking and release of data at any time during the term of the contractual relationship and after its termination.

2.4 The contents of this agreement apply accordingly if the testing or maintenance of automated procedures or data processing systems is carried out on behalf of the customer and access to personal data cannot be excluded.

3. Obligations of the contractor

3.1 The contractor may only collect, process or use the data within the scope of the contract and the instructions of the client, unless there is an exceptional case within the meaning of Article 28 Paragraph 3 a) GDPR. The contractor will inform the client immediately if he believes that an instruction violates applicable laws. The contractor may suspend the implementation of the instructions until they have been confirmed or changed by the client.

3.2 Within his area of responsibility, the contractor will design the internal organization in such a way that it meets the special requirements of data protection. The contractor will take appropriate technical and organizational measures that meet the requirements of the GDPR (Article 32 GDPR). This includes in particular:

3.2.1 The ability to ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services related to the processing,

3.2.2 the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident,

3.2.3 Procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing.

3.3 Measures for this include, in particular, the use of state-of-the-art encryption procedures or pseudonymization.

3.4 At the request of the client, the contractor will provide the information necessary for the overview in accordance with Art. 30 Para. 1 GDPR.

3.5 The contractor ensures that the employees involved in processing the data are obliged to maintain confidentiality and have been instructed in the protective provisions of the GDPR. The confidentiality obligation continues even after the work has ended.

3.6 The contractor guarantees that it will comply with its obligations under Art. 37 GDPR, such as its obligation to appoint a data protection officer, to the extent required by law.

3.7 The contractor informs the client of the contact details of the company data protection officer. The contact details of the company data protection officer are: datenschutz@candis.io

3.8 The contractor will inform the client immediately in the event of serious disruptions to operations, suspected data protection violations or other irregularities in the processing of the data. He takes the necessary measures to secure the data and to reduce possible adverse consequences for those affected and immediately discusses this with the client.

The contractor supports the client to the extent possible in fulfilling the requests and claims of data subjects in accordance with Chapter III of the GDPR as well as in complying with the obligations specified in Articles 32 to 36 GDPR.

If a claim is made against the client by a data subject with regard to any claims in accordance with Art. 82 GDPR, the contractor undertakes to support the client in defending the claim to the extent possible.

3.9 Data media provided and all copies or reproductions made thereof remain the property of the client. The contractor must store these carefully so that they are not accessible to third parties. The contractor is obliged to provide the client with information at any time as far as the data and documents are concerned. The contractor undertakes the data protection-compliant destruction of test and reject material based on an individual order from the client. In special cases to be determined by the client, storage or handover takes place. Furthermore, the contractor reserves the right to continue to securely store corresponding data sets in accordance with its legal retention obligations (such as the principles for the proper management and storage of books, records and documents in electronic form and for data access, GoBD for short) for up to 10 years preserve.

3.10 The fulfillment of the aforementioned obligations must be checked by the contractor and proven in an appropriate manner.

3.11 The contractor will correct, delete or block the contractual data if the client instructs this. The contractor undertakes the data protection-compliant destruction of data carriers and other materials based on an individual order from the client, unless already agreed in the contract. In special cases to be determined by the client, storage or handover takes place.

3.12 Data, data carriers and all other materials must either be returned or deleted after the end of the order at the client's request. If additional costs arise due to different requirements for the release or deletion of the data, these will be borne by the client.

3.13 The contractor does not use the data provided for any purposes other than fulfilling the contract.

4. Obligations of the client

4.1 The client and contractor are responsible for compliance with the data protection laws relevant to them with regard to the data to be processed.

4.2 The client must inform the contractor immediately and completely if he discovers errors or irregularities with regard to data protection regulations when checking the order results.

4.3 The client is responsible for the information obligations resulting from Articles 33 and 34 of the GDPR.

4.4 The client determines the measures to return the data carriers provided and/or delete the stored data after termination of the contractual relationship by contract or by instruction.

5. Inquiries from those affected to the clients

If a data subject contacts the contractor with requests for correction, deletion or information, the contractor will refer the data subject to the client, provided that an assignment to the client is possible according to the information provided by the data subject. The contractor will immediately forward the data subject's request to the client. The contractor supports the client within the scope of his possibilities. The contractor is not liable if the request of the person concerned is not answered by the client, not answered correctly or not on time.

6. Control rights and obligations

6.1 Before starting data processing and then regularly, the client checks the contractor's technical and organizational measures and documents the result. For this purpose, the client can, at his own discretion, obtain information from the contractor, have a certificate from an expert presented to him or, after registering in good time, can convince himself personally during normal business hours without disrupting operations.

6.2 The contractor undertakes to provide the client with all information required to carry out an inspection within a reasonable period of time upon written request or request in text form.

7. Subcontractors

7.1 The use of subcontractors as additional processors is only permitted if the client has given prior consent.

7.2 Before engaging additional subcontractors or replacing listed subcontractors, the contractor will inform the client by updating the list of commissioned subcontractors. The client can object to the change - within a reasonable period of time - for important reasons - in writing to the office named by the contractor: datenschutz@candis.io.

7.3 The contractually agreed services or the partial services described below are carried out using the following subcontractors:

Name and address of the subcontractor	Description of the partial service
Amazon Web Services EMEA Sàrl 5 Rue Plaetis L-2338 Luxembourg	Hosting in the Frankfurt data zone in Germany (Certifications AWS)
Gini GmbH Lyonel-Feininger-Str. 28 80807 Munich	Recognition of relevant information from PDFs and scanned text documents (Tom Gini)
Mailjet SAS 13-13 bis, rue de l'Aubrac, 75012 Paris, France	Sending notification emails (AVV & TOM Mailjet)
Google Cloud EMEA 70 Sir John Rogerson's Quay Dublin 2 Ireland	Provision of automated document type differentiation (AVV & TOM Google)

7.4 The contractually agreed service is provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any relocation of the service or partial work to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 ff. GDPR are met (e.g. adequacy decision by the Commission, standard data protection clauses, approved rules of conduct).

7.5 The contractor must contractually ensure that the agreed regulations between the client and the contractor also apply to subcontractors. If several subcontractors are used, this also applies to the responsibilities between these subcontractors. In particular, the client must be entitled, if necessary, to carry out appropriate checks and inspections, including on-site, with subcontractors or to have them carried out by third parties commissioned by him.

7.6 The contract with the subcontractor must be drawn up in writing, which can also be done in an electronic format (Art. 28 Para. 4 and Para. 9 GDPR). The forwarding of data to the subcontractor is only permitted if the subcontractor has fulfilled the obligations under Article 29 and Article 32 Paragraph 4 GDPR with regard to subordinated persons.

7.7 The Contractor is liable to the Client for ensuring that the Subcontractor complies with the data protection obligations contractually imposed on it by the Contractor in accordance with this Contract Section.

7.8 A subcontractor relationship does not exist if the contractor commissions third parties to provide an additional service to the main service, such as external personnel, postal and shipping services or maintenance.
The contractor will enter into agreements with this third party to the extent necessary to ensure adequate data protection.

7.9 The use of artificial intelligence (AI) and large language models (LLM) by the contractor is only permitted if it is guaranteed that the data processed as part of the contractual relationship

is not used for general training of the AI/LLM. The use of the data must be strictly limited to the processing purposes specified in the contract. The processor ensures that all AI systems it uses meet the data protection and data security requirements in accordance with applicable legal regulations.

8. Information obligations

If the contractor's data is endangered by seizure or confiscation, by insolvency or settlement proceedings or by other events or measures by third parties, the contractor must inform the client immediately. The contractor will immediately inform everyone responsible in this context that the sovereignty and ownership of the data lies exclusively with the client as the “responsible party” within the meaning of the GDPR.

9. Written form clause & applicable law

9.1 Changes and additions to this agreement and all of its components require a written agreement or agreement in text form and an express reference to the fact that it is a change or addition to these conditions. This also applies to the waiver of this formal requirement.

9.2 In the event of any contradictions, the provisions of this data protection appendix take precedence over the provisions of the contract. If individual parts of this system are ineffective, this will not affect the effectiveness of the rest of the system.

9.3 German law applies.

10. Contact person

10.1 Contact person at the contractor:
Data Protection Department,
datenschutz@candis.io, +49 030 311 930 40

Berlin, 19 / 11 / 2024
place, date

Candis GmbH
Company name

Christian Ritosek, CEO
Name of the signatory, position


Signature

APPENDIX 1: TECHNICAL AND ORGANIZATIONAL PROTECTION MEASURES

A Access control measures to office spaces

(Please refer to the Amazon Web Services documentation for information on access control measures to the server rooms here. Amazon Web Services has ISO27001 certification, which sets high security standards for those certified with regard to access control measures.)

A.1. Locations of client workstations from which personal data is accessed.

Name	Office Candis
Address	CityQuartier DomAquarée, Karl-Liebknecht-Straße 5, 10178 Berlin
E-mail:	info@CANDIS.io
Tel:	030 311 930 40

A.2. Is there a doorman service/permanent reception area for the building or your offices?

☒ Yes

A.3. Is the building or the office rooms secured with an alarm system (EMA)?

☒ Yes

A.4. Who will be informed when the EMA triggers?

☒ assigned security service

A.5. Are the office building and its entrances under video surveillance?

☒ yes, with image recording – access only

A.6. Does the building/office rooms have an electronic locking system?

☒ yes, but only the entrance to the offices/office floor, not the building as a whole.

A.7. If B.8 yes: Which access technology is used?

☒ RFID

A.8. Is there a mechanical lock for the building/office space?

☒ Yes

A.9. Is key issuance logged, who issues the keys?

☒ Yes

A.10. Are there official access regulations for non-company people (e.g. visitors) to the office space?

☒ Yes, people from outside the company will be picked up at the entrance or reception by the contact person and are only allowed to move around the building with an escort.

Are the documented measures suitable for a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of those affected to ensure?

☒ appropriate

B Access and access control measures

B.1. Is there a process for assigning user IDs and access authorizations when hiring and leaving employees or in the event of organizational changes?

☒ defined release process

B.2. Do employees authenticate themselves to the central directory service using an individual identifier?

☒ Yes

B.3. Are there mandatory password parameters in the company?

☒ Yes

B.4. How long does the password have to be and does it have to contain special characters?

Long 12, a capital letter, a special character

B.5. Does the IT system force the user to comply with the password requirements mentioned above?

☒ Yes

B.6. Does the screen lock when the user is inactive? If yes, after how many minutes?

☒ Yes, after a minute

B.7. What measures do you take if a password is lost, forgotten or spied on?

☒ Admin assigns new initial password

B.8. How is authentication carried out for remote access?

☒Password

B.9. Are the systems on which personal data is processed secured via a firewall?

☒ Yes

B.10. Is the firewall updated regularly?

☒ Yes

B.11. Who administers your firewall?

☒ own IT

Are the documented measures suitable for a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of those affected to ensure?

☒ appropriate

C Measures to secure paper documents, mobile data carriers and mobile devices

C.1. How are paper documents containing personal data (e.g. printouts/files/correspondence) that are no longer needed disposed of?

☒ Shredders are available for this purpose and are required to be used.

C.2. How are data carriers (USB sticks, hard drives) on which personal data is stored that are no longer needed disposed of?

☒ Delete the data

C.3. Can mobile data media be used in the company (e.g. USB sticks)?

☒ Yes

C.4. Are employees allowed to use private storage media (e.g. USB sticks)?

☒ No, all required storage media is provided by the company.

C.5. Is personal data encrypted on mobile devices?

☒ Yes

Are the documented measures suitable for a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of those affected to ensure?

☒ appropriate

D Measures for secure data transmission

D.1. Is the transfer of personal data consistently encrypted?

☒ per SSL

☒ per TSL 1.2

D.2. Who manages the keys or certificates?

☒ own IT

☒ External service provider (hoster through managed keys)

D.3. Are the transfer processes logged?

☒ Yes

D.4 Are the protocols evaluated regularly?

☒ Yes, manual and automated evaluation

D.5. Who is responsible for the company's network connection?

☒ Own IT

Are the documented measures suitable for a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of those affected to ensure?

☒ appropriate

E backup and emergency concept, virus protection

E.1. Is there a backup concept?

☒ Yes

E.2. Is the backup restore functionality tested regularly?

☒ Yes

E.3. At what frequency are backups of systems on which personal data is stored?

☒ Daily (backup retention period: 12 months)

E.4. What kind of backup media are the backups stored on?

☒ Second redundant server

E.5. Where are the backups kept?

☒ Second redundant server is in a different location

E.6. In the case of transporting the backups: How is this carried out?

☒ Accompanied by an MA from IT / management

E.7. Are the backups encrypted?

☒ Yes

E.8. Are the backups stored in a separate fire compartment or part of the building from the primary server?

☒ Yes

E.9. Is there a documented process for software or patch management?

☒ Yes

E.10. Who is responsible for software and patch management?

☒ Own IT

E.11. Is there an emergency concept (e.g. emergency measures in the event of hardware defects / fire / total loss, etc.)?

☒ Yes

E.12. Are the IT systems technically protected against data loss/unauthorized data access? Yes, by means of constantly updated

☒ Virus protection

☒ Anti-Spyware

☒ Spam filter

☒ IDS/IPS

☒ Content Filter

E.13. Who is responsible for current virus protection, anti-spyware and spam filters?

☒ Internal IT

Are the documented measures suitable for a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs, the nature, scope, circumstances and purposes of the processing as well as the different probability of occurrence and severity of the risk for the rights and freedoms of those affected to ensure?

☒ appropriate

F Other safety measures

Q.1. Access control

- Alarm system
- Retention period for image material < 50 days
- Automatic access control system
- Visitors only when accompanied by employees
- Reception with porter
- Building is purely an office building

Q.2. Access control

- General Policy Privacy and/or Security
- Anti-virus software
- Application of 2-factor authentication
- Automatic desktop barrier
- Intrusion Detection Systeme
- Login with username and password
- Encryption of notebooks/tablets
- Assignment of user rights

Q.3. Access control

- Differentiated permissions (applications)
- Differentiated permissions (data)
- Management of user rights by administrators

Q.4. Separation control

- Determination of database rights
- Logical client separation (software side)
- Control via an authorization concept
- Separation of productive and test environments

Q.5. Transfer control

- Email encryption
- Delivery via encrypted connections such as sftp, https

Q.6. Input control

- Technical logging of data changes
- Granting rights to process data

Q.7. Encryption

- Encrypted access to customer databases
- Encrypted access to customer servers
- Encrypted access to web portals
- Encryption of the transport of emails

Q.8. Availability (of data)

- Backup & recovery concept
- Operation of high availability web servers
- RAID system / hard drive mirroring
- Daily backups
- Uninterruptible power supply (UPS)

Q.9. Resilience (of systems)

- Use of hardware firewalls
- Use of intrusion detection systems
- Use of software firewalls
- Installing current security updates on all application servers
- Installing security updates on all developer systems

Q.10. Recoverability (of data / systems)

- Alarm message in the event of unauthorized access to the server room
- Fire doors

- Fire and smoke alarm systems
- Fireproof cabinets
- Fire extinguisher in the server room

Q.11. Order control

- Conclusion of the necessary order processing agreements
- Conclusion of the necessary standard contractual clauses
- Selection of the contractor based on due diligence aspects
- Review of the contractor's level of protection (continuous)

Q.12. Data protection management

- Appointment of an external data protection officer
- Use of software solutions for data protection management
- Training employees on data protection
- Obligation of employees to maintain confidentiality

F.13. Incident-Response-Management

- Documentation of security incidents
- Involvement of data protection officers in security incidents
- Use of firewall and its regular updating
- Use of virus scanners and their regular updates

APPENDIX 2: DATA PROCESSING

The contractor stores, among other things, the following data for the purpose of using CANDIS. Depending on the level of use by the client, more or less data is stored and processed.

a) The Transaction Information

- Basic information of linked bank accounts, credit cards and PayPal accounts, consisting of:
    - Account/card name
    - IBAN, BIC
    - Credit card number
    - PayPal email address
- Individual transactions of linked bank accounts, credit cards and PayPal accounts, consisting of:
    - Datum
    - sum
    - Purpose of use
    - Sender/recipient account information

b) Receipt information

- Receipts and emails that are sent by the client to the CANDIS email address provided or uploaded manually, consisting of:
    - E-Mail Header
    - E-Mail Body
    - Email attachments
- Individual document information, consisting of a maximum of:
    - Document layout
    - Payable amount
    - Postal code
    - Account number
    - BIC
    - Company registration number of the invoice issuer
    - Customer number
    - Document type
    - Document date
    - Document domain
    - IBAN
    - Invoice number
    - Purpose of use
    - Sender city
    - Sender
    - Sender name suffix
    - Sender mailbox
    - Sender zip code
    - Return address
    - Tax number
    - VAT ID
    - Website

c) Other information

- Comments
- Search inputs
- Information about invited users (name, email address)

d) Billing information

- Business
- Address
- Contact person (email address)
- Billing Information

e) Usage behavior

- Log dating
- Usage statistics

Titel	AVV Englisch
Dateiname	EN_AUFTRAGSVERARB...VV__1.10___1_.pdf
Dokument-ID	cd40ae543e3fe3e679467bc3c46db90e1b5d04eb
Datumsformat für Prüfprotokoll	DD / MM / YYYY
Status	Unterzeichnet

Dokumentverlauf

GESENDET	**11 / 11 / 2024** 13:47:36 UTC	Von marius.roth@candis.io zur Signatur an Christian Ritosek (christian@candis.io) versandt IP: 217.235.213.112
ANGESEHEN	**19 / 11 / 2024** 09:33:35 UTC	Von Christian Ritosek (christian@candis.io) angesehen IP: 46.189.30.170
UNTERZEICHNET	**19 / 11 / 2024** 09:33:42 UTC	Von Christian Ritosek (christian@candis.io) unterzeichnet IP: 46.189.30.170
ABGESCHLOSSEN	**19 / 11 / 2024** 09:33:42 UTC	Das Dokument wurde abgeschlossen.