DATA PROCESSING AGREEMENT (DPA)

Between	and
the party specified in the relevant document provided by Candis and accepted by Candis Contracting Party	Candis GmbH CityQuartier DomAquarée Karl-Liebknecht-Straße 5 10178 Berlin
– hereinafter: **'the Client'** –	– hereinafter referred to as: **"Contractor"** –

Preamble

This Annex sets out in detail the data protection obligations of the contracting parties arising from the data processing activities described in detail in the contractual relationship under the User Agreement and the General Terms and Conditions. It applies to all activities related to the contractual relationship in which the Contractor's employees or third parties commissioned by the Contractor may come into contact with the Client's personal data.

Annexes 1 and 2 form an integral part of this agreement.

1. Subject matter, duration and specification of the data processing

1.1 The subject matter and duration of the contract, as well as the nature and purpose of the processing, are set out in the Terms of Use. Specifically, the following data form part of the data processing (a detailed list of all data categories can be found in Annex 2):

Type of data	Nature and purpose of data processing	Categories of data subjects
Contact and identification data (e.g. name, business email address, telephone number, postal address, contact details)	Processing for the provision and use of Candis functions, in particular for user management, communication, document processing and assignment to business transactions.	Customers, employees, suppliers, and, where applicable, prospective customers
User and authorisation data (e.g. user ID, role, team, authorisations, profile information, organisational assignment , telephone numbers, email addresses, fax numbers, IP addresses)	Processing for the purposes of authentication, user management and the management of roles, permissions and approval processes within Candis.	Customers, employees, suppliers and, where applicable, prospective customers
Payment and transaction data relating to individuals (e.g. IBAN, BIC, credit card details, transaction data, payment references, and information on senders and recipients)	Processing for the mapping and support of payment, credit card, accounting and transaction processes within Candis.	Customers, employees, suppliers and, where applicable, prospective clients

Type of data	Nature and purpose of data processing	Categories of data subjects
Personal data contained in documents, receipts and emails (e.g. names, contact details, signatures, personal contract details, individuals entertained, email content and attachments)	Processing for the purpose of capturing, managing, extracting, classifying and further processing documents, supporting documents and emails within Candis.	Customers, employees, suppliers and, where applicable, prospective clients
Workflow, approval and communication data relating to individuals (e.g. approval assignments, approvals, rejections, comments, notes and support communications)	Processing for the execution, automation and traceability of invoicing, document and approval processes, as well as for communication relating to the use of Candis.	Customers, employees, suppliers and, where applicable, prospective clients
Personalised analysis, extraction, classification and assignment data (e.g. personalised field and assignment suggestions, recognised relationships, risk characteristics and results of automated approval rules)	Processing for the provision of automated and AI-supported Candis functions, in particular for the extraction, classification, risk assessment, linking and automated processing of personal information.	Customers, employees, suppliers and, where applicable, prospective clients
Log, audit and usage data (e.g. logins, user actions, IP addresses, timestamps, changes to data, audit trail information, log data and usage statistics)	Processing for the provision of automated and AI-supported Candis functions, in particular for the extraction, classification, risk assessment, linking and automated processing of personal information.	Customers, employees, suppliers and, where applicable, prospective clients
Contract and billing data relating to individuals (e.g. contact persons, contact details and personal contract and billing information)	Processing for the purposes of executing, managing and settling the contractual relationship, as well as for customer support.	Customers, employees, suppliers and, where applicable, prospective clients

1.2 The term of this Annex is determined by the term of the Terms of Use, provided that no further obligations arise from the provisions of this Annex.

2. Scope and Responsibility

2.1 The Contractor shall process the data on behalf of the Client. This includes activities specified in the contract and in the scope of services. Under this agreement, the Client is solely responsible for compliance with the statutory provisions of data protection legislation, in particular for the lawfulness of the transfer of data to the Contractor and for the lawfulness of the data processing (‘Data Controller’ within the meaning of Article 4(7) of the EU General Data Protection Regulation (GDPR)).

2.2 Instructions are initially set out in the contract and may subsequently be amended, supplemented or replaced by the Client in writing or in text form by means of individual instructions (individual instruction). Instructions that go beyond the contractually agreed service shall be treated as a request for a change to the service. Verbal instructions must be confirmed in writing or in text form without delay.

2.3 Those authorised to issue instructions are the Client's legal representatives and persons who have been named as contact persons with the relevant authorisation in the underlying quotation, at the time of concluding the contract or subsequently in text form.

2.4 By virtue of this responsibility, the Client may, at any time during the term of the contractual relationship and after its termination, request the rectification, erasure, blocking and disclosure of data.

2.5 The provisions of this agreement shall apply mutatis mutandis where the inspection or maintenance of automated processes or data-processing systems is carried out on behalf of the Client and access to personal data cannot be ruled out.

3. Obligations of the Contractor

3.1 The Contractor may only collect, process or use the data within the scope of the contract and in accordance with the Client's instructions, unless an exception applies within the meaning of Article 28(3)(a) of the GDPR. The Contractor shall inform the Client without delay if it considers that an instruction contravenes applicable laws. The Contractor may suspend implementation of the instruction until it has been confirmed or amended by the Client.

3.2 The Contractor shall organise its internal operations within its area of responsibility in such a way as to meet the specific requirements of data protection. The Contractor shall implement appropriate technical and organisational measures that comply with the requirements of the GDPR (see Article 32 of the GDPR). This includes, in particular:

3.2.1 The ability to ensure the confidentiality, integrity, availability and resilience of the systems and services relating to processing on an ongoing basis,

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

3.2.3 procedures for regularly reviewing, assessing and evaluating the effectiveness of the technical and organisational measures designed to ensure the security of processing.

3.3 Measures in this regard include, in particular, the use of state-of-the-art encryption methods or pseudonymisation.

3.4 At the Client's request, the Contractor shall provide the information required for the overview referred to in Article 30(1) of the GDPR.

3.5 The Contractor shall ensure that employees involved in the processing of data are bound by a duty of confidentiality and have been instructed in the protective provisions of the GDPR. The duty of confidentiality shall continue even after the termination of their employment.

3.6 The Contractor undertakes to fulfil its obligations under Article 37 of the GDPR, such as its obligation to appoint a data protection officer, where required by law.

3.7 The Contractor shall provide the Client with the contact details of the company's data protection officer.
The contact details of the company's data protection officer are: datenschutz@Candis.io

3.8 The Contractor shall notify the Client without delay in the event of serious disruptions to business operations, suspected data breaches or other irregularities in the processing of data. The Contractor shall take the necessary measures to safeguard the data and to minimise any adverse consequences for data subjects, and shall consult with the Client on this matter without delay.

The Contractor shall, to the best of its ability, assist the Client in responding to enquiries and claims from data subjects in accordance with Chapter III of the GDPR, as well as in complying with the obligations set out in Articles 32 to 36 of the GDPR.

In the event that a data subject makes a claim against the Client under Article 82 of the GDPR, the Contractor undertakes to assist the Client in defending against the claim to the best of its ability.

3.9 Upon termination of the data processing, the personal data processed on behalf of the Client shall be deleted in accordance with the contractually agreed rules on deletion and handover, or made available to the Client. Any existing copies shall also be deleted, unless the Contractor is under a legal obligation to retain them further. Data subject to a statutory retention obligation shall be blocked for the duration of the relevant retention period and processed exclusively for this purpose.

3.10 The Contractor must monitor compliance with the aforementioned obligations and provide evidence thereof in an appropriate manner.

3.11 The Contractor shall rectify or erase personal data, or restrict its processing, insofar as the Client so requires within the scope of its authority to issue instructions.

3.12 The Contractor shall not use the data provided for any purposes other than the performance of the contract.

4. Obligations of the Client

4.1 The Client and the Contractor are responsible for complying with the data protection laws applicable to them in respect of the data to be processed.

4.2 The Client must inform the Contractor immediately and in full if, upon reviewing the results of the work, it discovers any errors or irregularities relating to data protection regulations.

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

5. Enquiries from data subjects to the Client

If a data subject contacts the Contractor with requests for rectification, erasure or access, the Contractor shall refer the data subject to the Client, provided that the data subject's details allow the data subject to be identified as relating to the Client. The Contractor shall forward the data subject's request to the Client without delay. The Contractor shall assist the Client to the best of its ability. The Contractor shall not be liable if the Client fails to respond to the data subject's request, or responds incorrectly or out of time.

6. Rights and obligations of supervision

6.1 Before data processing commences, and thereafter at regular intervals, the Client shall verify the technical and organisational measures implemented by the Contractor and shall document the results. To this end, the Client may, at its discretion, obtain self-declarations from the

Contractor, request a certificate from an expert, or, following timely notification, verify the measures in person during normal business hours without disrupting business operations.

6.2 The Contractor undertakes to provide the Client, upon written request or a request in text form, within a reasonable period, with all information necessary for carrying out an audit.

7. Subcontractors

7.1 The Client consents to the use of the additional data processors listed in 7.3.

7.2 The Contractor is entitled to engage further data processors or to replace existing data processors. The Contractor shall inform the Client of this in writing at least four weeks before the intended change and shall update the list of data processors used.
The Client may object to the change in writing to datenschutz@candis.io within four weeks of receiving the notification on data protection grounds. If no objection is raised within this period, the Client's consent to the change shall be deemed to have been given.

7.3 The contractually agreed services or the partial services described below shall be carried out with the involvement of 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 and provision of cloud infrastructure and AI-supported functions (AWS certifications),
Gini GmbH Lyonel-Feininger-Str. 28 80807 Munich	Extraction 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 AI-powered features (AVV & TOM Google)
Intercom R&D Unlimited Company 124 St Stephen's Green Dublin 2, D02 C628 Ireland	Provision of customer service and communication features within Candis. Processing and documentation of support enquiries. (Intercom certifications)
Clever Cloud SAS 4 rue Voltaire 44000 Nantes France	Hosting and provision of individual Candis applications. (Clever Cloud certifications)
BunnyWay d.o.o. Dunajska cesta 165 1000 Ljubljana	Provision of content delivery and edge infrastructure for individual Candis applications. Processing of technical

Name and address of the subcontractor	Description of the partial service
Slovenia	connection and request data in particular to ensure the secure and high-performance delivery of content. (https://bunny.net/blog/bunnynet-achieves-iso-27001-certification/)

7.4 The contractually agreed service shall be 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 parts thereof to a third country requires the prior consent of the client and may only take place if the specific conditions set out in Articles 44 et seq. of the GDPR are met (e.g. an adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

7.5 The Contractor must ensure, in accordance with the contract, that the agreed provisions between the Client and the Contractor also apply to subcontractors. Where several subcontractors are engaged, this shall also apply to the responsibilities between these subcontractors. In particular, the Client must be entitled, where necessary, to carry out appropriate checks and inspections, including on-site, at subcontractors' premises, or to have such checks and inspections carried out by third parties appointed by the Client.

7.6 The contract with the subcontractor must be drawn up in writing, which may also be in electronic format (Article 28(4) and (9) of the GDPR). The transfer of data to the subcontractor is only permitted once the subcontractor has fulfilled the obligations under Article 29 and Article 32(4) of the GDPR regarding persons under their control.

7.7 The Contractor shall be 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 section of the contract.

7.8 A subcontracting relationship does not exist where the Contractor engages third parties in connection with ancillary services to the main service, such as external staff, postal and delivery services, or maintenance.
The Contractor shall enter into agreements with such third parties 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 ensured that the data processed within the scope of the contractual relationship is not used for the general training of the AI/LLM. The use of the data must be strictly limited to the processing purposes specified in the contract. The data processor shall ensure that all AI systems it uses comply with the data protection and data security requirements in accordance with the applicable legal provisions.

8. Duty to provide information

Should the data held by the Contractor be at risk due to attachment or seizure, insolvency or composition proceedings, or other events or measures taken by third parties, the Contractor must inform the Client of this without delay. The Contractor shall immediately inform all relevant parties in this context that sovereignty over and ownership of the data lie exclusively with the Client as the 'controller' within the meaning of the GDPR.

9. Written Form Clause & Applicable Law

9.1 Any amendments or additions to this agreement and all its constituent parts must be set out in a written agreement or in text form and must expressly state that they constitute an amendment or addition to these terms and conditions. This also applies to any waiver of this formal requirement.

9.2 In the event of any inconsistencies, the provisions of this Annex on data protection shall take precedence over the provisions of the contract. Should individual parts of this Annex be invalid, this shall not affect the validity of the remainder of the Annex.

9.3 German law shall apply.

10. Contact

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

Berlin 2026-11-12

_____
Place, Date

Candis GmbH

_____
Company name

Christian Ritosek CEO

_____
Name of signatory, position

Christian Ritosek

_____
Signature

ANNEX 1 TO THE AVV: TECHNICAL AND ORGANISATIONAL PROTECTION MEASURES

A Access control measures for office premises

(Please refer to the documentation from Amazon Web Services here for information on access control measures for server rooms. Amazon Web Services holds ISO 27001 certification, which imposes high security standards on certified organisations with regard to access control measures.)

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

Name Candis Offices
Address CityQuartier DomAquarée, Karl-Liebknecht-Straße 5, 10178 Berlin
Email: info@candis.io
Tel: 030 311 930 40

A.2. Is there a concierge service or a permanently staffed reception area for the building or your offices?

☒ Yes

A.3. Is the building or are the office premises protected by an intruder alarm system (IAS)?

☒ Yes

A.4. Who is notified if the intrusion alarm system is triggered?

☒ contracted security service

A.5. Is the office building or its entrances under video surveillance?

☒ Yes, with video recording – entrances only

A.6. Is the building/office premises fitted with an electronic locking system?

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

A.7. If B.8 is 'yes': What access control technology is used?

☒ RFID

A.8. Is there a mechanical lock for the buildings / office premises?

☒ Yes

A.9. Is the issuing of keys logged, and who issues the keys?

☒ Yes

A.10. Are there official access rules for non-staff members (e.g. visitors) to the office premises?

☒ Yes, non-staff members are met at the entrance or reception by a designated contact person and may only move about the building when accompanied.

Are the documented measures suitable for ensuring a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects?

☒ suitable

B Access and access control measures

B.1. Is there a process in place for issuing user IDs and access authorisations when new staff are recruited, when staff leave the organisation, or in the event of organisational changes?

☒ defined approval process

B.2. Do employees authenticate themselves using a unique identifier with the central directory service?

☒ Yes

B.3. Are there mandatory password policies in place within the organisation?

☒ Yes, and two-factor authentication where offered by the service

---

B.4. How long must the password be, and must it contain special characters?

Length 12 characters, one uppercase letter, one special character

---

B.5. Does the IT system enforce compliance with the above password requirements?

☒ Yes

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

☒ Yes, after one minute

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

☒ The administrator assigns a new initial password

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

☒ Password & multi-factor authentication

B.9. Are the systems on which personal data is processed protected by a firewall?

☒ Yes

B.10. Is the firewall updated regularly?

☒ Yes

B.11. Who administers your firewall?

☒ In-house IT

Are the documented measures suitable for ensuring a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects?

☒ Appropriate

C Measures for securing paper documents, portable data storage media and mobile devices

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

☒ Shredders are available for this purpose, and staff are instructed to use them.

C.2. How are data storage media (USB sticks, hard drives) containing personal data that are no longer required disposed of?

☒ Deletion of the data

C.3. Are mobile data storage devices (e.g. USB sticks) permitted for use within the organisation?

☒ Yes

C.4. Are employees permitted to use personal data storage devices (e.g. USB sticks)?

☒ No, all necessary storage media are provided by the company.

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

☒ Yes

Are the documented measures suitable for ensuring a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects?

☒ suitable

D Measures for secure data transmission

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

☒ via SSL

☒ via TLS 1.2 or higher

D.2. Who manages the keys or certificates?

☒ In-house IT

☒ External service provider (hosting provider using Managed Keys)

D.3. Are the transmission processes logged?

☒ Yes

D.4 Are the logs analysed regularly?

☒ Yes, manual and automated analysis

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

☒ In-house IT

Are the documented measures suitable for ensuring a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects?

☒ suitable

E Backup and contingency plan, virus protection

E.1. Is there a backup plan in place?

☒ Yes

E.2. Is the functionality of the backup and recovery system tested regularly?

☒ Yes

E.3. How often are backups taken of systems on which personal data is stored?

☒ Daily (backup retention period: 12 months)

E.4. On what type of backup media are the backups stored?

☒ Second redundant server

E.5. Where are the backups stored?

☒ A second redundant server located at a different site

E.6. If the backups need to be transported, how is this carried out?

☒ Transported by an IT staff member or a member of senior management

E.7. Are the backups encrypted?

☒ Yes

E.8. Is the backup storage location situated in a separate fire compartment or part of the building from the primary server?

☒ Yes

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

☒ Yes

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

☒ In-house IT

E.11. Is there a contingency plan (e.g. emergency measures in the event of hardware failure, fire, total loss, etc.)?

☒ Yes

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

☒ antivirus software

☒ anti-spyware

☒ spam filter

☒ IDS/IPS

☒ content filters

E.13. Who is responsible for keeping the virus protection, anti-spyware and spam filter up to date?

☒ Internal IT

Are the documented measures suitable for ensuring a level of protection appropriate to the risk, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of data subjects?

☒ suitable

F Further security measures

F.1. Access control

- Alarm system
- Retention period for video footage < 50 days
- Automatic access control system
- Visitors must be accompanied by staff
- Reception with a porter
- The building is used exclusively as an office block

F.2. Access control

- General policy on data protection and/or security
- Anti-virus software
- Using two-factor authentication
- Automatic desktop lock
- Intrusion detection systems
- Login with username and password
- Encryption of laptops and tablets
- Assignment of user rights

F.3. Access control

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

F.4. Segregation of duties

- Definition of database rights
- Logical client separation (software-based)
- Control via an authorisation scheme
- Separation of production and test environments

F.5. Disclosure control

- Email encryption
- Provision via encrypted connections such as SFTP, HTTPS

F.6. Input control

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

F.7. Encryption

- Encrypted access to customer databases
- Encrypted access to customers' servers
- Encrypted access to web portals
- Encryption of email transmission

F.8. Availability (of data)

- Backup and recovery strategy
- Operation of high-availability web servers
- RAID system / hard disk mirroring
- Daily backups
- Uninterruptible Power Supply (UPS)

F.9. System resilience

- Use of hardware firewalls
- Use of intrusion detection systems
- Use of software firewalls
- Installation of the latest security updates on all application servers
- Installation of security updates on all development systems

F.10. Recoverability (of data / of systems)

- Alarm notification in the event of unauthorised access to the server room
- Fire doors
- Fire and smoke detection systems
- Fireproof cabinets
- Fire extinguishers in the server room

F.11. Contract monitoring

- Conclusion of the necessary data processing agreements
- Conclusion of the necessary standard contractual clauses
- Selection of the data processor in accordance with due diligence principles
- Review of the data processor's level of protection (on an ongoing basis)

F.12. Data Protection Management

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

F.13. Incident Response Management

- Documentation of security incidents
- Involvement of data protection officers in security incidents
- Use of firewalls and their regular updating
- Use of antivirus software and its regular updating

ANNEX 2 TO THE AVV: DATA PROCESSING

The Contractor shall store, amongst other things, the following data for the purposes of using CANDIS. Depending on the extent of use by the Client, more or less data will be stored and processed.

a) Transaction information

- Basic information on linked bank accounts, credit cards and PayPal accounts, comprising:
    - Account/card name
    - IBAN, BIC
    - Credit card number
    - PayPal email address
- Individual transactions from linked bank accounts, credit cards and PayPal accounts, comprising:
    - Date

- Amount
- Reference
- Information on the sender's/recipient's account

b) Document details

- Documents and emails sent by the client to the CANDIS email address provided or uploaded manually, consisting of:
  - Email header
  - Email body
  - Email attachments
- Individual document details, consisting of a maximum of:
  - Document layout
  - Amount payable
  - Postcode
  - Account number
  - BIC
  - Company registration number of the invoicing party
  - Customer number
  - Document type
  - Document date
  - Document domain
  - IBAN
  - Invoice number
  - Payment reference
  - Sender's town
  - Sender
  - Sender's name suffix
  - Sender's PO Box
  - Sender's postcode
  - Sender's address
  - Tax number
  - VAT number
  - Website

c) User, employee and authorisation data

This includes, in particular, data relating to the client's users and employees, which can be entered directly into Candis or transmitted via integrations activated by the client, such as:

- First name and surname
- business email address
- User and organisational assignment
- Profile information and, where applicable, profile picture
- Role and permissions
- Team and organisational unit
- Cost centre
- bank details where applicable, in particular the IBAN
- Status and information regarding the use of the user account

d) Master, organisational and accounting data

These include, in particular:

- Business partner and supplier data
- Names and contact details of contact persons
- Addresses
- Payment details
- Cost centres and cost objects
- General ledger accounts
- Tax codes
- Terms of payment
- Organisational and company details
- VAT registration numbers and tax reference numbers
- Other master data required for accounting and financial processes

e) Workflow, approval and communication data

In connection with invoicing, document and approval processes, the following may in particular be processed:

- Assignment to requesters and approvers
- Approval steps and approval status
- Approvals and rejections
- Timestamps and processing status of individual processing steps
- Comments and notes
- Allocations to teams, cost centres and other accounting characteristics
- Support and communication content relating to the use of Candis

f) Analysis, extraction, classification and allocation data

As part of Candis's automated and AI-supported functions, further information and results may be generated from the data provided by the client. These include, in particular:

- extracted document and supporting document information
- classification of documents and document types
- automatically generated field and mapping suggestions
- identified links between invoices, contracts, credit card transactions, expenses and other documents
- results of checks and risk assessments, particularly in relation to IBAN data
- Results and status of automated processing and approval rules

g) Log, audit and usage data

To ensure the security, traceability and functionality of Candis, the following data in particular may be processed:

- User and login information
- Log data
- Audit trail data
- User actions
- Changes to documents and records
- Changes to transactions
- Changes to master and user data
- Changes to roles and permissions
- Timestamps
- Technical device, browser and connection information
- Usage statistics
- Search queries

h) Contract, customer and billing data

In connection with the contractual relationship and billing, the following data in particular may be processed:

- Company name
- Company address
- Contact person
- Email address and other contact details
- Contract and tariff information
- Invoicing and billing information
- Other information required for the administration of the contractual relationship

The lists above are not exhaustive. Which personal data is actually processed depends, in particular, on the data provided by the client, the functions and integrations used, and the configurations made by the client.

Audit trail

Details

FILE NAME	Candis_AVV_1.11 Einzelunterschrift en-GB .docx - 12.11.26, 16:03
STATUS	Signed
STATUS TIMESTAMP	2026/11/12 20:06:14 UTC

Activity

SENT	marius.roth@candis.io **sent** a signature request to: • Christian Ritosek (christian@candis.io)	2026/11/12 15:03:50 UTC
SIGNED	**Signed** by Christian Ritosek (christian@candis.io)	2026/11/12 20:06:14 UTC
COMPLETED	This document has been signed by all signers and is **complete**	2026/11/12 20:06:14 UTC

The email address indicated above for each signer may be associated with a Google Account, and may either be the primary email address or secondary email address associated with that account.