Data Processing Agreement between Continia customer and Continia Software A/S

Version 2.9 of April 3rd, 2025.

DATA PROCESSING AGREEMENT

Between the Continia

Customer

(Hereinafter referred to as 'the controller' or 'the Customer')

Customer Name	
Address	
Country	
Company registration no	

and

Continia Software A/S

Stigsborgvej 60

9400 Nørresundby

Denmark

Company registration (CVR) no.: DK32658083

(Hereinafter referred to as 'the processor' or 'Continia')

Customer and Continia agree that Customer is the controller of Personal Data and Continia is the processor of such data, except when Customer, or the Customer's appointed third party (in most cases the Customer's Microsoft partner) acts as a processor of Personal Data, in which case Continia is a sub-processor. When Continia acts as the processor or sub-processor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its Agreement (including this DPA and any applicable updates), along with the Customer's use of Continia's Services, are Customer's complete documented instructions to Continia for the processing of Personal Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Continia that Customer's instructions, including appointment of Continia as a processor or sub-processor, have been authorized by the relevant controller, and documented in a separate Data Processing Agreement between the parties. For clarification, when Continia acts as a sub-processor any instructions given from the data processor is considered a documented instruction from the controller.

Standard contractual clauses

SECTION I

Clause 1

Purpose and scope

a. The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

b. The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

c. These Clauses apply to the processing of personal data as specified in Annex II.

d. Annexes I to IV are an integral part of the Clauses.

e. These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679.

f. These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679.

Clause 2

Invariability of the Clauses

a. The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them. Such add-on or update shall be made and accepted in writing with a notice period of no less than 30 days, except for change of sub-contractors (Clause 7.7) or other material issues, where the notice period shall be 2 months.

b. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

c. Any modifications or amendments to these Clauses and/or Annexes in accordance with this Clause 2, cf. Clause 7.7(a), shall be informed by way of email and always by notification on the processor´s website (www.continia.com), therefore all controllers are obliged to subscribe to the notification mailing list at https://www.continia.com/legal/trust-center/gdpr-compliance/ while using the data processor‘s

services. All further use of the services is considered an active acceptance of the notified changes or updates.

Clause 3

Interpretation

a. Where these Clauses use the terms defined in Regulation (EU) 2016/679 respectively, those terms shall have the same meaning as in that Regulation.

b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 respectively.

c. These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5 - Optional

Docking clause

a. An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a controller or as a processor, by obtaining written, legally binding, consent from the controller.

b. Once an entity has obtained written consent, and by doing so accepting the terms of the Clauses and Appendices, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a controller or processor in accordance with the written consent.

c. The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause 7

Obligations of the Parties

7.1. Instructions

a. The processor shall process personal data only on documented instructions from the controller, unless required to do so by law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

b. The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 or applicable law.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

a. The processor shall, at a minimum, implement the technical and organisational measures necessary to meet prevailing industry standards and legal requirements. This obligation includes safeguarding the data against security breaches resulting in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to the data (referred to as a "personal data breach"). When determining the appropriate level of security, the processor shall consider factors such as the nature, scope, context, and purpose of processing, as well as the risks posed to the data subjects. With the controller's general consent, the processor is granted the authority to continually assess, update, and adapt these measures to fulfil its obligations efficiently.

b. The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing, and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

The Parties shall be able to demonstrate compliance with these Clauses.

a. The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

b. The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

c. The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

d. The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

a. The processor has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The processor shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 2 months in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The processor provides the controller with the necessary information as described in Clause 2.c, to enable the controller to exercise its right to object. All further use of the services is considered an active acceptance of the changes.

b. Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679.

c. At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secrets or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

d. The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub- processor to fulfil its contractual obligations.

e. The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. International transfers

a. Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679.

b. The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met or equivalent safeguards/framework is in place.

Clause 8

Assistance to the controller

a. The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

b. The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

c. In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

    1. the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
    2. the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
    3. the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
    4. the obligations in Article 32 of Regulation (EU) 2016/679.

d. In Annex III and Clause 7.4 the parties have set out the appropriate processes regarding technical and organisational measures by which the processor is required to assist the controller in application of this clause as well as the scope of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, where applicable, taking into account the nature of processing and the information available to the processor.

9.1. Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

a. in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

b. in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679 shall be stated in the controller's notification, and must at least include:

   1. the nature of the personal data including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
   2. the likely consequences of the personal data breach;
   3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c. in complying, pursuant to Article 34 of Regulation (EU) 2016/679 with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2. Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach.

Such notification shall contain, at least:

a. a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

b. the details of a contact point where more information concerning the personal data breach can be obtained;

c. its likely consequences and the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay, no later than 72 hours.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

a. Without prejudice to any provisions of Regulation (EU) 2016/679 in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

b. The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

   1. the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
   2. the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679.
   3. the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679.

c. The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

d. Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless applicable law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I

List of parties

Controller(s):

Name:

Business Identification Number (e.g., VAT, CVR, KVK, EIN, HR) if applicable:

Address:

Contact person's:

Name:

Position:

Telephone:

E-mail:

Signature and accession date:

*The controller has the option of accepting the terms of this DPA online within Business Central. When accepted by the user in Business Central, the information above is known and stored digitally without having to sign or fill out this section of Annex I.

Processor(s):

Name: Continia Software A/S

Business Identification Number: CVR DK32658083

Address: Stigsborgvej 60, 9400 Nørresundby, Denmark

Contact person:

Name: Inger Ericson

Position: Corporate Counsel/DPO

E-mail: dpo@continia.com

Signature and accession date: 03.04.2025

Henrik Lærke, CEO

ANNEX II

2.1. Description of the processing

Continia will process Personal Data to provide the services and in accordance with the Main Agreement. Continia may not use or store the personal data for other purposes.

Continia may create an anonymous copy of your data, which will therefore never contain information that serves as an identifier to the data subject. The purpose of such a copy is for Continia to make statistics and analysis to improve our products and services.

Data and its processing period are limited to what is necessary to fulfil the nature of the service. It is not possible to predict the extent to which the controller's data will contain personal data, which can range from non-sensitive to sensitive information. Refer to sections 2.2.1 through 2.2.12 for further details on which data subjects and categories apply to each service.

2.2. The nature of, purpose and duration of the processing, including specification of the data subject, personal data categories and location.

This section describes Continia's services, nature of the purposes, categories of data subjects and types of data to be processed with Continia Software as applicable to the extent relevant in accordance with the Main Agreement.

Prior to transmitting or processing sensitive data, either by the controller or their end-users, via Continia services, the controller is responsible for ensuring that suitable safeguards are in place.

Applicable from the 2nd of April 2024: Initial phase of data processing segmentation by geographical location (Europe/Australia) is available and applicable for new customers running version 24 of Continia services and supported Business Central versions as following:

For new on-premises customers using version 24 of Continia Services and supported Business Central versions: Customers have the option to choose between data processing in Europe or Australia, as applicable to each relevant service. Detailed information on each service and relevant sub-processor can be found in section 2.2.5 - 2.2.7, section 2.2.11 - 2.2.12 and Annex IV.

For new cloud-based customers located in Australia and New Zealand using version 24 of Continia Services and Business Central: Customer data is automatically processed and stored in Australia as applicable to each relevant service. Detailed information on each service and relevant sub-processor can be found in section 2.2.5 - 2.2.7, section 2.2.11 - 2.2.12 and Annex IV.

For new cloud-based customers using version 24 of Continia Services and Business Central: Europe serves as the default data center location for customers in the following countries: Austria, Belgium, Canada, Czechia, Denmark, Faroe Islands, Finland, France, Germany, Greenland, Iceland, India, Italy, Mexico, Netherlands, Norway, Spain, Sweden, Switzerland, United Kingdom, and United States. For customers in all

other countries, there is an option to choose either Europe or Australia as the primary data processing location, if applicable to the specific service. Detailed information on each service and relevant sub-processor can be found in section 2.2.5 - 2.2.7, section 2.2.11 - 2.2.12 and Annex IV.

2.2.1. Support Services

1. Nature of processing

While performing support services, Continia may obtain access to personal data, either through support cases created in Zendesk, through direct access to customer systems, as the recipient of e-mails, file transfers, or other ways. Continia will use and otherwise support services data only to provide support services in accordance with controllers' documented instructions.

For purposes of this DPA, "to provide" Support Services consists of:

a. Delivering the support services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services. For clarification, providing technical support will include making improvements to the underlying Continia products and services subscribed to or utilized by the customer based on issues identified during delivery of support services.
b. Troubleshooting (preventing, detecting, investigating, mitigating, and repairing issues, including security incidents and problems identified during delivery of support services).

2. Data subjects

a. End users
b. Business partners
c. Potentially other data subjects obtained within submitted e-mails, PDF-files, XML-files, and other files

3. Categories of personal data

a. Name, title, email address
b. Any form of personal data shared as a part of the support case, but out of control or influence of Continia

4. Sensitive data (special categories of personal data)

Continia does not anticipate that this type of processing will include any form of sensitive data but cannot be excluded since it is out of the control or influence of Continia.

5. Retention

Continia stores closed/solved tickets for up to 5 years, all tickets are automatically deleted on the date of 5 years from last activity.

6. Sub-processors

Zendesk: Provides platform and hosting of Continia's support cases.

2.2.2. Professional Services

1. Nature of processing

While performing professional services, Continia may obtain access to personal data, either through direct access to customer systems, as the recipient of e-mails, file transfers, or other ways. Continia will use and otherwise process professional services data, only to provide professional services in accordance with controllers' documented instructions.

For purposes of this DPA, "to provide" Professional Services consists of:

a. Delivering the professional services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services. For clarification, providing technical support will include making improvements to the underlying Continia products and services subscribed to or utilized by the customer based on issues identified during delivery of professional services.
b. Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including security incidents and problems identified during delivery of professional services).

2. Data subjects

a. End users
b. Business partners
c. Potentially other data subjects obtained within submitted e-mails, PDF-files, XML-files, and other files

3. Categories of personal data

a. Name, title, email address
b. Any form of personal data within the controller's environment, but out of control or influence of Continia

4. Sensitive data (special categories of personal data)

Continia does not anticipate that this type of processing will include any form of sensitive data but cannot be excluded since it is out of the control or influence of Continia.

5. Retention

Continia will retain data until the business purposes, for which the data was collected or transferred, have been fulfilled or earlier upon the customer's request. Once fulfilled only essential personal information, such as contact names and email, will be stored in a project summary, while all other data is permanently deleted.

6. Sub-processors

Microsoft (**Azure**)**:** Provides platform and hosting services related to storing project data.

Microsoft (**Microsoft 365**)**:** Provides platform and hosting services related to storing project data.

2.2.3. Continia Core

1. Nature of processing

Personal data is transmitted to the Continia Online Service via APIs from Business Central. This data, which includes account information, support details, and more, enables us to provide the services to which you've subscribed.

Within the framework of Continia Core, Continia assumes the role of a controller in relation to this data.

2. Data subjects

a. End users
b. Business partners

3. Categories of personal data

a. Name, title, email address
b. Credit card number if paying for the services via credit card

4. Sensitive data (special categories of personal data)

None

5. Retention

Continia retains data from Continia Core for the duration of the service provision, and for the time that is necessary to document our business relationship or as required by law.

6. Sub-processors

Microsoft (Azure): Provides platform and hosting services related to Continia Online Services

2.2.4. PartnerZone

1. Nature of processing

Continia processes data regarding Partners and End Users to provide the requested services, comply with legal obligations, document business relationship, and fulfill compliance requirements. This includes using data to perform KYC/KYB (Know Your Customer/Know Your Business) and ongoing monitoring for compliance.

2. Data subjects

a. Microsoft Partner employees
b. Other users created in Partner Zone (end users)

3. Categories of personal data

a. Name and email address

4. Sensitive data (special categories of personal data)

None

5. Retention

Continia retains data from PartnerZone for the duration of the service, as long as necessary to document the business relationship, meet compliance requirements, or as required by law

6. Sub-processors

Microsoft (Azure): Provides platform and hosting services related to PartnerZone.

2.2.5. Personal data related to Document Capture

1. Nature of processing

Personal data is transferred to Continia Online Service by APIs from Business Central or by sending e-mails to dedicated e-mail addresses (AWS service) in Continia Online with attachments for processing. PDF-files are processed by either ABBYY (not applicable for customer data processed in Australia) or Microsoft as a sub-processor whereafter the result is downloaded to Continia Online. Processed data is downloaded from Continia Online by the customer either manually or automatically from Business Central.

2. Data subjects

a. Employees
b. Business partners
c. Potentially other data subjects within submitted e-mails, PDF-files, XML-files, and other files

3. Categories of personal data

a. Contact name and email information (sender name/email address, receiver name/email address, email body).
b. Potentially other information within submitted emails, PDF-files, XML-files and other files

4. Sensitive data (special categories of personal data)

E-mail body, PDF-files, XML-files, and other files can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

E-mails, PDF-files, and XML-files are stored until downloaded to Business Central or deleted after 180 days. Backup is stored for 90 days.

6. Sub-processors

AWS: Provides technical platform and services to receive incoming emails from the customer with PDF and XML attachments for processing.

ABBYY: Provides OCR services of customer data (PDF-files). This service is not applicable to customer data processed in Australia.

Microsoft (**Azure**)**:** Provides OCR services of customer data (PDF-files), and platform and hosting services related to Continia Online Services.

2.2.6. Personal Data related to Continia Expense Management

1. Nature of processing

Personal data is transferred to/from Continia Online Service and Expense App, Expense Portal, Business Central, card transaction provider, or by sending e-mails to dedicated e-mail addresses in Continia Online Services with attachments for processing. Images of receipts and PDF-files are processed by Klippa as a sub-processor.

2. Data subjects

a. Employees
b. Expense users
c. Credit card holders (when processing and importing bank transactions)
d. Potentially other data subjects obtained within submitted e-mails, PDF-files, XML-files, and other files

3. Categories of personal data

a. Name, e-mail, home address of expense user
b. E-mail information (sender name/e-mail address, receiver name/e-mail address, e-mail body, attachments)
c. Expense/Mileage/Per diem information and attachments
d. Card transaction data (when processing and importing bank transactions)
e. Business Central user-id
f. Potentially other information obtained within submitted e-mails, PDF-files, and other files

4. Sensitive data (**special categories of personal data**)

E-mail body, PDF-files, XML-files, and other files can potentially contain sensitive data, but beyond the control or influence of Continia**.**

5. Retention

Transactional data are stored until downloaded to Business Central or deleted after 180 days. Backup is stored for 90 days.

Customer can configure Expense Management to save transactional data for up to 12 months, to enable Expense users to view historical data. In that case, data will be stored during the chosen period and deleted automatically at the time of expiration. History in the app is not deleted by deleting the user in Business Central as there is no way to control that the device and app get connected to the internet, and the responsibility relating erasure from mobile devices lies with the controller.

6. Sub-processors

AWS: Provides technical platform and services to receive incoming emails related to expenses.

Klippa: Provides Continia AI Receipt Scanner in order to process customer data (OCR services regarding pictures of receipts or PDF-files). Data processed by Klippa occurs within the EU. For Customers who have chosen Australia as their geographical location, Continia offers the option to instruct Klippa processing to be deactivated upon request.

Microsoft (**Azure**)**:** Provides platform and hosting services related to Continia Online Services.

7. Geographical specifications

Customers that have instructed data processing to take place in Australia: All bank transaction data relevant to Expense Management, received from banks or credit card providers, is initially processed by Continia within the EU. This processing time is limited to the shortest time possible before the data is returned to the customer's preferred geographical location. Typically, for most transactions, this transfer occurs within the first hour. However, in cases where the transaction is not associated with an active agreement, it may be stored for a maximum period of 180 days before it is deleted.

2.2.7. Personal Data related to Continia Web Approval Portal

1. Nature of processing

The Web Approval Portal works in combination with Continia Document Capture and Expense Management and can either be installed on-premises or hosted with Continia as part of Continia Online Services. Processing of personal data will only take place when hosted with Continia. Personal data is transferred to/from Continia Online Service and Business Central.

2. Data subjects

a. Employees, Approvers, Purchasers, Expense users
b. Credit card holders (when processing and importing bank transactions)
c. Business partners
d. Potentially other data subjects obtained within submitted e-mails, PDF-files, XML-files, and other files

3. Categories of personal data

a. Name, e-mail, Business Central user-id
b. Expense/Mileage/Per diem information and attachments.
c. Potentially other information obtained within submitted e-mails, PDF-files, and other files

4. Sensitive data (special categories of personal data)

E-mail body, PDF-files, XML-files, and other files can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

User access data are stored in Continia Online Services until removed from the solution in Business Central and synchronized to Continia Online Services by the customer.

All other relevant data (such as PDF, receipt images, etc.) are stored in the cache of the user and removed when the session of the user expires. Files such as PDF, receipt images, etc. may be stored for up to 48 hours to increase general application performance.

6. Sub-processors

Microsoft (Azure): Provides platform and hosting services related to Continia Online Services.

7. Geographical specifications

For Business Central customers in North America and Oceania, data processing will occur in the regional datacenter corresponding to the location of their Business Central instance:

USA Datacenter: Covers Antigua and Barbuda, The Bahamas, Barbados, Belize, Canada, Costa Rica, Cuba, Dominica, Dominican Republic, El Salvador, Grenada, Guatemala, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Trinidad and Tobago, and the United States.

Australia Datacenter: Covers Australia, Fiji, Kiribati, Marshall Islands, Micronesia, Nauru, New Zealand, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

Europe Datacenter: Covers all other regions.

2.2.8. Personal Data related to Continia Payment Management

1. Nature of processing

Personal data is transferred to/from Continia Online Service by APIs from Business Central, and by sending or downloading data from payment institutions and payment service providers.
Older versions (Business Central v. 14) of Continia Payment Management can use either Continia Online Services or the local CBIC (Continia Banking Integration Component) for converting file formats. When using the older versions of Business Central with the local CBIC, there is no transfer or processing of personal data.

2. Data subjects

a. Employees working with Payment Management
b. Bank certificate owners
c. Potentially other data subjects obtained within submitted payment and bank account transaction data

3. Categories of personal data

a. Name and e-mail
b. Business Central user-id
c. Personal identification number (DK CPR-nr.) and phone number (only when using NemKonto-payments)
d. Information obtained within payment and bank account transaction data (such as identification information, contact details, bank account information, payment instructions, etc.)

4. Sensitive data (special categories of personal data)

Payment and bank account transaction data can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

In general, payment data and transaction data are transferred directly (in-memory process within Continia Online Services) to the payment institution or payment service provider instructed by the customer, and therefore data is not stored by Continia Online Service.

However, for some payment institutions and payment service providers Continia is required to store the payment and transactional data to document finance related activities. This data can be stored for up to 4 years.

6. Sub-processors

Microsoft (Azure): Provides platform and hosting services related to Continia Online Services.

2.2.9. Personal Data related to Continia Banking

1. Nature of processing

The Personal Data in Banking is transferred to/from Continia Online Service by APIs from Business Central, and by sending or downloading data from payment institutions and payment service providers.

2. Data subjects

a. Employees working with Banking
b. Bank certificate owners
c. Potentially other data subjects obtained within submitted payment and bank account transaction data

3. Categories of personal data

a. Name and e-mail
b. Business Central user-id

c. Personal identification number information obtained within payment and bank account transaction data (such as identification information, contact details, bank account information, payment instructions, etc.)

4. Sensitive data (special categories of personal data)

Payment and bank account transaction data can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

In general, payment data and transaction data are transferred directly (in-memory process within Continia Online Services) to and from the payment institution or payment service provider instructed by the customer, and therefore data is not stored by Continia Online Service.

However, for some payment institutions and payment service providers, Continia is required to store the payment and transactional data to document finance related activities. This data can be stored for up to 4 years.

6. Sub-processors

Microsoft (Azure): Provides platform and hosting services related to Continia Online Services.

2.2.10. Personal Data related to Collection Management

1. Nature of processing

Personal data is transferred to/from Continia Online Service by APIs from Business Central, and by sending or downloading data from collection providers.

2. Data subjects

a. Individuals receiving the payment collection
b. Potentially other data subjects obtained within submitted collection data

3. Categories of personal data

a. Name, e-mail, phone number, home address
b. Bank account information or personal identification number (e.g., DK CPR) when creating collection agreements
c. Potentially other information obtained within submitted collection data

4. Sensitive data (special categories of personal data)

Collection data can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

Personal collection data and transaction data is transferred directly (in-memory process within Continia Online Services) to the collection provider instructed by the customer. Personal data is not stored by Continia Online Service.

6. Sub-processors

Microsoft (**Azure**)**:** Provides platform and hosting services related to Continia Online Services.

2.2.11. Personal Data related to Document Output

1. Nature of processing

Personal data is transferred to/from Continia Online Service by APIs from Business Central. Personal data will be potential data subjects within printed/e-mailed PDF-files, and only relevant when using Continia Online Services for signing PDF-files, merging PDF-files, applying background to PDF-files, etc.

2. Data subjects

a. Data subjects potentially obtained within PDF-files
b. Signing certificate owners (when using PDF signing functionality)

3. Categories of personal data

Information potentially obtained within submitted PDF-files.

4. Sensitive data (**special categories of personal data**)

PDF-files can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

Personal data within PDF-files is never stored but only processed (in-memory process within Continia Online Services), and then returned to Business Central

6. Sub-processors

Microsoft (**Azure**)**:** Provides platform and hosting services related to Continia Online Services

2.2.12. Personal Data related to Continia Delivery Network

1. Nature of processing

The Continia Delivery Network is used when subscribing to the service in Continia Document Capture or Document Output. Personal data is transferred to/from Continia Online Service by APIs and Business Central, or from incoming business documents via the connected electronic network.

2. Data subjects

a. Employees
b. Business partners
c. Potentially other data subjects obtained within submitted XML-files

3. Categories of personal data

a. Contact name, email, and phone number
b. Information obtained in submitted business documents

4. Sensitive data (special categories of personal data)

Business documents can potentially contain sensitive data, but beyond the control or influence of Continia.

5. Retention

Business documents are stored until downloaded to Business Central or deleted after 180 days. Backup is stored for 90 days.

6. Sub-processors

Tickstar: Provides platform and services to the Peppol eDelivery Network, such as sending and receiving business documents.
KMD: Provides platform and services provider to the Danish NemHandel, such as sending and receiving business documents.
Microsoft (Azure): Provides platform and hosting services related to Continia Online Services.

ANNEX III

3.1. Measures regarding security of processing

The processor shall primarily assist the controller in ensuring an adequate level of processing security, in accordance with Article 32 GDPR as well as Clause 7.4. by implementing technical and organisational measures to establish the necessary level of data security and ensure that it is updated as technical and legal requirements evolve.

Controller may request information on the processor's implemented technical and organisational security measures, such as the latest copy of the processors ISAE 3402 Type II Assurance Report performed by an independent auditor.

3.2. Direct Assistance to the Controller

The processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the controller directly in accordance with Clause 8 by the following:

a. The processor shall upon request make the necessary information available to the controller necessary for the controller to comply with Clause 8.

b. If necessary, the processor shall assist the controller in identifying the relevant personal data in connection with the fulfilment of the controller's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR.

c. If necessary, the processor shall - in the form of technical or organisational measures - assist the controller in observing requests for rectification or deletion in accordance with Articles 16 and 17 GDPR.

Any costs incurred by the Processor in connection with the above stated assistance will be payable by the Controller pursuant to an agreed fee scheme.

3.3. Procedures for the controller's audits, including inspections, of the processing of personal data being performed by the processor

The controller or the controller's representative shall have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the processor, including physical facilities as well as systems used for and related to the processing.

Such an inspection shall be performed, when the controller has assessed and determined that the current certifications held by the processor are insufficient and has duly informed the processor in writing.

As a rule, any inspection or audit must be notified by the controller to the processor with at least 1 months' notice and all costs incurred by the processor are payable by the controller.

The processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

3.4. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The processor shall, on the basis of an assessment of the risks to the rights and freedoms of the data subjects related to the specific processing activities to be carried out by sub-processor, determine how the processor will audit sub-processors' compliance with the GDPR, or applicable data protection provisions and any Clauses which the processor has agreed with the sub-processor.

Further, the processor shall determine how often and to what extent the processor will audit those sub-processors and implement these audits in the processor's technical and organisational measures to ensure that those sub-processors comply with the GDPR, or applicable data protection provisions and any Clauses which the data processor has agreed with the sub-processor.

3.5. Procedure for assessing and implementing measures derived from subsequent instructions from the controller to the processor

The controller has, as stated in Clause 7.1, the right to issue subsequent instructions to the processor throughout the duration of the processing of personal data. In such an event the controller must convey these instructions to the processor by either contacting the processors contact person as stated in Annex I or contact the processor through dpo@continia.com.

The processor will then assess the received instructions in order to determine whether the processor is able or willing to implement the measures contained in the subsequent instruction. The processor will implement measures that are required by law to which the processor is subject within a reasonable time frame.

The processor however retains the right to refuse implementing instructions that the processor either deems to exceed measures required by law to which the processor is subject, or are based on requirements that originate from third country legislation.

In any such event as described above or in the event that the provisions of Clause 10 for whatever reason become applicable and the controller decides to terminate the contract between the controller and the processor the conditions of termination stated in the Main Agreement will apply.

ANNEX IV

List of sub-processors

The controller has authorised the use of the following sub-processors:

Name: Microsoft Ireland Operations Ltd.

Address: One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing:

a) **Azure**: Ireland - applicable for all controllers not specifying another geo location.

b) **Azure**: Australia - Only applicable for new customers that have purchased Continia Services after the 2nd of April 2024 and have Continia version 24 and supported Business Central versions and have instructed processing in this geo location.

c) **Microsoft 365:** EU

Name: ABBYY Europe GmbH

Address: Landsberger Str. 300 80687 Munich, Germany

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing: The Netherlands

Name: Amazon Web Services EMEA SARL

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing:

a) Ireland – applicable for all controllers not specifying another geo location.

b) Australia – Only applicable for new customers that have purchased Continia Services after the 2nd of April 2024 and have Continia version 24 and supported Business Central versions and have instructed processing in this geo location.

Name: Tickstar AB

Address: Triewaldsgränd 2, SE-111 29 Stockholm, Sweden

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing:

a) Ireland – applicable for all controllers not specifying another geo location.

b) Australia – only applicable for controllers that have instructed processing in this geo location.

Name: Klippa App B.V.

Address: Lübeckweg 2, 9723 HE Groningen, The Netherlands

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing: Ireland

Name: KMD A/S

Address: Lautrupparken 40-42, 2750 Ballerup, Denmark

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing: Denmark (support within the EU may be utilized)

Name: Zendesk, Inc.

Address: 989 Marker St, San Fransisco, CA 94103, USA

See Annex II for details of the processing description regarding the relevant Continia service.

Country of processing: Germany