DATA PROCESSOR AGREEMENTS

BETWEEN

CONTINIA CUSTOMER AND CONTINIA SOFTWARE A/S

Version 1.5 of 14 May 2020

DATA PROCESSOR AGREEMENT

Between

the Continia Customer
(hereinafter referred to as 'the Customer')

Customer Name	
Adresss	
Country	
Company registration (CVR) no	

and

Continia Software A/S
Stigsborgvej 60
9400 Nr. Sundby
Denmark
Company registration (CVR) no.: DK32658083
(hereinafter referred to as 'Continia')

who have entered into the following processor agreement (hereinafter referred to as 'the Agreement') regarding Continia's processing of personal data on behalf of the Customer.

The agreement has been pre-signed on behalf of Continia Software. To enter into this agreement, the Customer must:

1. Complete the agreement with legal name, address and signatory information.
2. Submit the completed and signed agreement via email to dpo@continia.com

1. General

1.1 The Agreement pertains to Continia's obligation to comply with the General Data Protection Regulation (GPRD)(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 Danish Act. Based on GPDR (hereinafter referred to as the General Data Protection Regulation)

1.2 The Agreement contains the requirements in the coming rules of the General Data Protection Regulation that are applicable to processor agreements.

2. Purpose

2.1 Continia is authorized to processes personal data pursuant to the license agreement with The Customer for use right of Continia Software solutions (hereinafter referred to as 'the Main Agreement') in which Continia's processing and the purpose of the processing are described in Appendix 3 - Instructions.

3. The rights and obligations of The Customer

3.1 The Customer is controller of the data that the Customer instructs Continia to process. The Customer is responsible for ensuring that the personal data that the Customer instructs Continia to process may be processed by Continia, including that the processing is necessary and legitimate in relation to the tasks of the Customer.

3.2 The Customer has the rights and obligations that are given to a controller pursuant to the legislation, cf. sections 1.1. and 1.2 of the Agreement.

4. The obligations of Continia

4.1 Continia is processor of the personal data that Continia processes on behalf of The Customer, cf. section 6 and Appendix 3. As processor, Continia has the obligations that are imposed on a processor pursuant to the legislation, cf. sections 1.1 and 1.2. of the Agreement.

4.2 Continia shall only process the personal data entrusted to it according to instructions from The Customer, cf. section 6 and Appendix 3, and only in order to fulfil the Main Agreement.

4.3 As of 25 May 2018, Continia shall maintain a record of the processing of personal data and a record of all personal data breaches.

4.4 Continia shall secure the personal data using technical and organizational security measures, as described in the Security Measures Executive Order and the Security Measures Guidelines (until 25 May 2018) and the General Data Protection Regulation (as of 25 May 2018), cf. Appendix 1 – Security.

4.5 Upon the request of the Customer, Continia shall help to fulfil the Customer's obligations with regard to the rights of the data subject, including responding to requests from citizens about access to own data, the handing over of the citizens' data, rectification and erasure of data, restrictions to processing the citizens' data, and the Customer's obligations relating to notification of the data subject in case of personal data breaches, as of 25 May 2018 pursuant to Chapter III and Article 34 of the General Data Protection Regulation.

4.6 As of 25 May 2018, Continia shall help the Customer comply with its obligations pursuant to Articles 32-36 of the General Data Protection Regulation.

4.7 As of 25 May 2018, Continia shall guarantee that it will provide sufficient expert knowledge, reliability and resources to implement appropriate technical and organizational measures so that Continia's processing of the Customer's personal data meets the requirements of the General Data Protection Regulation and ensures protection of the rights of the data subject.

4.8 Continia is obligated to provide information about the precise addresses where the Customer's personal data are stored, cf. Appendix 2. Continia must keep the Customer updated in case of any changes.

5. Sub-supplier (sub-processor)

5.1 A sub-processor is defined as a sub-supplier to whom Continia has entrusted the processing (in whole or in part) that Continia carries out on behalf of The Customer.

5.2 Without the express written approval of the Customer, Continia may not use other sub-processors than those that are stated in Appendix 2 for processing the personal data that the Customer has entrusted to Continia pursuant to the Main Agreement. This also includes replacing these sub-processors.

5.3 If Continia entrusts the processing of personal data, for which the Customer is controller, to a sub-processor, Continia shall enter into a written (sub-)processor agreement with the sub-processor.

5.4 The (sub-)processor agreement, cf. section 5.3, shall impose the same data protection obligations on the sub-processor that apply to Continia pursuant to the Agreement, including that the sub-processor as of 25 May 2018 shall guarantee that it is capable of providing sufficient expert knowledge, reliability and resources to be able to implement the appropriate technical and organizational measures so that the sub-processor's processing meets the requirements of the General Data Protection Regulation and ensures protection of the rights of the data subject.

5.5 When Continia entrusts the processing of personal data, for which the Customer is controller, to sub-processors, then Continia is responsible to the Customer for the compliance by the sub-processors with their obligations, cf. section 5.3.

5.6 The Customer may, at any given time, demand documentation from Continia about the existence and content of (sub-)processor agreements for Continia's sub-processors in connection with fulfilling obligations to the Customer.

5.7 All communication between the Customer and the sub-processor shall take place via Continia.

5.8 In accordance with the Customer's request, Continia delivers data, including personal data, via the integration module to the business partners chosen by the Customer, including e.g. banks, MobilePay, credit card companies or the like. In order to avoid misunderstandings, it is emphasized that the Customer's other business partners are not considered to be Continia's sub-processors, and the Customer must ensure that separate data processor agreements with such business partners are entered into as Continia is not liable for the processing that takes place at the Customer's other business partners.

6. Instructions

6.1 Continia's processing of personal data on behalf of the Customer shall only take place according to documented instructions of the relevant solutions and services used by the Customer, cf. Appendix 3.

6.2 As of 25 May 2018, Continia shall immediately notify the Customer if an instruction relevant for a solution or service used by the Customer, in Continia's opinion, violates legislation, cf. section 1.2.

7. Technical and organizational security measures

7.1 As of 25 May 2018, cf. Appendix 1, Continia shall implement all necessary technical and organizational security measures that are required for an appropriate level of security.

7.1.1 The measures must be implemented with due regard to the current state of the art, costs of implementation and the nature, scope, context and purposes of the processing and the risk of varying likelihood and severity to the rights and freedoms of natural persons. Continia shall take the category of personal data described in appendix 3 into consideration in the determination of such measures.

7.1.2 Continia warrants towards the Customer that Continia shall implement the suitable technical and organizational measures in such a manner that Continia's processing of personal data meets the requirements of the personal data regulation in force from time to time.

7.1.3 The Parties agree that the provided safeguards as specified in clause 7.1.2 are adequate at the date of conclusion of this Processor Agreement.

7.2 At least once a year, Continia shall review its internal security regulations and guidelines for processing personal data in order to ensure that the necessary security measures are continually observed, cf. sections 7.1 and as well as Appendix 1.

7.3 Continia and its employees are not permitted to obtain information of any kind that does not have significance for the fulfilment of the tasks of those in question.

7.4 Continia is obligated to instruct its employees, who have access to or in another way carry out processing of the Customer's personal data, about Continia's obligations including the provisions on obligation of confidentiality and secrecy, cf. section 9.

7.5 The Processor shall ensure that employees processing personal data for the Processor only process such data in accordance with the Instructions.

7.6 Continia is obligated to inform the Customer immediately about every personal data breach and of

(i) every request for transfer of personal data covered by the Agreement from an authority, unless informing the Customer is explicitly prohibited by law, for example, pursuant to rules intented to ensure the confidentiality of an investigation by a law-enforcing authority,

(ii) other lack of compliance with Continia's and any sub-processor's obligations

regardless of whether this takes place at Continia or at a sub-processor.

7.7 Continia shall maintain a record of all Security Breaches. The record must as a minimum document the following:
- the actual circumstances of the Security Breach;
- the effects of the Security Breach; and
- the remedial measures taken.

7.8 Upon written request, the record must be made available to the Controller or the supervisory authorities.

7.9 Continia may neither publicly nor to a third party communicate about personal data breaches, cf. section 7.6, without prior written agreement with the Customer regarding the content of such communication unless Continia has a legal obligation to provide such communication.

8. Transfers to other countries

8.1 Continia's may not transfer personal data to countries that are not members of the EU (third countries), for example, via a cloud solution or a sub-processor.

9. The obligation of confidentiality and secrecy

9.1 Continia is - during the duration of the Main Agreement and afterwards - subject to full obligation of confidentiality regarding all information with which Continia becomes familiar due to the cooperation. The Agreement entails that the confidentiality provisions in sections 152-152f of the Danish Criminal Code, cf. section 152a of the Danish Criminal Code, shall be applicable.

9.2 As of 25 May 2018, Continia shall ensure that all those who process data covered by the Agreement, including employees, third parties (for example, a repairman) and sub-processors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

10. Monitoring and statements

10.1 Continia is obligated to provide the Customer with the information required so that the Customer can ensure that Continia complies with the obligations resulting from this Agreement.

10.2 Continia shall every year obtain an audit report from an independent expert regarding Continia's compliance with the data security requirements under the Agreement. Continia will free of charge, on request, submit the audit report to the Customer once every year. The audit report shall be prepared in accordance with recognized industry standards ISAE 3402 and shall cover data processing by both Continia and any sub-processors. The ISAE 3402 statement will also be available on www.continia.com.

10.3 In case the Customer and/or relevant public authorities, especially the Danish Data Protection Agency, want to carry out an inspection of the measures mentioned above pursuant to this Agreement, Continia and Continia's sub-suppliers obligate themselves to make time and resources available to do so at no further expense to the Customer.

11. Amendments to the Agreement

11.1 To the extent that changes to legislation, cf. sections 1.1 and 1.2, or related practice give rise to this, Continia is entitled to make amendments to the Agreement with 90 days' notice.

12. Deletion of data

12.1 On termination of the processing services, Continia shall be under obligation, at the Customer's discretion, to erase or return all the personal data to the Customer and to erase existing copies unless EU law or Member State law requires storage of the personal data.

12.2 No later than 90 days before the termination of the Main Agreement, the Customer shall notify Continia in writing about whether all the personal data shall be deleted or returned to customer. Continia shall ensure that any sub-processors also comply with the Customer's notification.

13. Fees and Costs

13.1 The Parties are only entitled to payment for the performance of this Processor Agreement if specifically specified herein or in the agreement(s) on delivery of the Primary Services.

13.2 Regardless of the above requirements, a Party is not entitled to payment for assistance or implementation of changes to the extent that such assistance or change is a direct consequence of the Parties' breach of this Processor Agreement.

14. Change of Instructions

14.1 Before any changes are made to the Instructions, the Parties shall to the widest possible extent discuss and, if possible, agree on, the implementation of the changes, including time and costs of implementation.

14.2 Unless otherwise agreed, the following applies:

14.2.1 Continia shall, without undue delay, execute implementation of changes to the Instructions and ensure that such changes are implemented without undue delay in relation to the nature and scope of the change.

14.2.2 Continia is entitled to payment of all costs directly related to changes to the Instructions, including costs of implementation and increased costs for the delivery of the Primary Services, unless the change is required by law.

14.2.3 An indicative estimate of the time and cost of implementation must be communicated to the Customer without undue delay.

14.2.4 The changes to the Instructions are only considered to apply once the changes have been implemented, provided that the implementation is carried out in accordance with this clause 14.2 and unless Continia explicitly communicates a deviation from this clause.

14.2.5 Continia are exempt from liability for failure to deliver the Primary Services if (including in terms of time) delivery of the Primary Services would be contrary to the changed Instructions or delivery in accordance with the changed Instructions is not possible. This may be the case (i) where the changes cannot be technically, practically or legally implemented, (ii) where Continia explicitly communicates that the changes have to apply before implementation is possible or (iii) during the period until the parties have made any necessary changes to the agreement(s) in accordance with the change procedures herein.

15. Breaches and disputes

15.1 Breaches and disputes are regulated by the Main Agreement.

16. Compensation and insurance

16.1 Questions regarding compensation and insurance are regulated by the Main Agreement.

17. Entry into force and duration

17.1 The Agreement is entered into with the signatures of both parties and remains in force until termination of the Main Agreement or as long as data is processed by Continia or one of its sub-data processors.

18. Requirements as to form

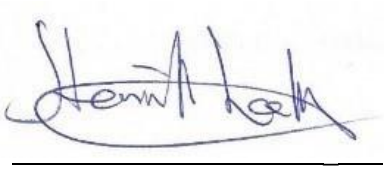
18.1 The Agreement shall be in writing, including in electronic form, at the Customer and Continia.

For the Customer

Date

For Continia

14. May 2020



CEO, Henrik Lærke

Continia Software A/S

History

Version	Change	Date
1.0	Initial Version	19/4/2018
1.1	Updated with AWS	30./4/2018
1.2	Updated with MobilePay Invoice instructions and 10.2, 12.1, 12.2 and 14.2.2 clearifications. 5.8 with clearification on sub-processor and business partner.	1/6/2019
1.3	Data related to licensing removed from Appendix 3, as the description is irrelevant for customer data processing.	27/11/2019
1.4	Descriptions of Mobilepay Invoice and Mobilepay Subscription added	24/02/2020
1.5	Minor update of 17.1	14/5/2020

Appendices

Appendix 1 – Security

Appendix 2 – Information on locations for processing and sub-suppliers (sub-processors)

Appendix 3 – Instructions

Appendix 1 – Security

1. Continia Security Measurements and Controls

Continia have implemented technical and organizational security measures and controls that comply with the ISAE 3402 Information Security assurance standard. The latest audit report can be found on www.continia.com under the TrustCenter.

Security obligations as of 25 May 2018

The Supplier shall carry out the following technical and organizational security measures to ensure a level of security that is appropriate for the agreed processing, cf. Instructions (Appendix 3) and which, therefore, fulfil Article 32 of the General Data Protection Regulation.

The measures are determined based on considerations related to:

1. What is technically feasible (state of the art)

2. The implementation costs

3. The nature, scope, context and purpose of processing, cf. Instructions (Appendix 3)

4. The consequences for the persons in case of personal data breaches

5. The risk that is connected with the processing, including the risk of:

    a) Destruction of personal data

    b) Loss of personal data

    c) Alteration of personal data

    d) Unauthorized disclosure of personal data

    e) Unauthorized access to personal data

Appendix 2 – Information on locations for processing and sub-suppliers (sub-processors)

1. Location or locations for processing.

Continia does not store or process Customer personal data on its own office locations.
All development and access the Customer personal data is done from the 2 Danish Office locations

Continia Software A/S
Stigsborgvej 60 (headquarter)
DK-9400 Nr. Sundby
Denmark

Continia Software A/S
Knabrostræde 30
DK-1210 Copenhagen K.
Denmark

2. Sub-processors

Continia uses the following sub-processors:

Microsoft – Azure Cloud Service located in Dublin, Ireland and Amsterdam, The Netherlands

ABBYY – Cloud OCR Service located in the Nethelands.

Amazon – AWS located in Dublin, Ireland.

Appendix 3 – Instructions

Continia Software is providing this GDPR-compliance document as a matter of convenience only. It's your responsibility to classify the data appropriately and comply with any laws and regulations that are applicable to you. Continia Software disclaims all responsibility towards any claims related to your classification of the data.

Instructions
The Customer hereby instructs Continia to carry out any processing of the Customer's personal data for the solutions and services used by the Customer, whether these are expenses, documents, payments and users handled using the Continia Online Services as a part of the Continia solutions, cf. the Main Agreement. Conitinia Online Services is the part of the Continia solutions that is operated, hosted and managed by Continia as a Cloud service,
Data used by Continia solutions in the customers own installation (on premise(NAV), hosted(NAV), smartphone or any other device) is not covered by this agreement and is not Continia Software's responsibility as data processor.

If Continia entrusts the processing of the Customer's personal data to sub-processors, Continia is responsible for entering into written (sub-)processor agreements with them, cf. section 5.3 of the Agreement.

1.1 Purpose of the processing

Processing of the Customer's personal data shall take place in accordance with the purpose in the Main Agreement.

Continia may not use the personal data for other purposes.

This section describes purpose of data processed and stored, permanent or temporary, with Continia Software and is applicable to the extent relevant in accordance with the Main Agreement.

Data related to Continia Document Capture

Only when using Continia Cloud OCR data is stored with Continia Online Service. Data is necessary to be able to receive and process e-mail and PDF-files.

Flow - Document categories will be exported to Continia Onlince Services for Continia Cloud OCR to be able to receive e-mails. This happens as part of the initial configuration or when the user manually exports them.

E-mails are received by Continia Cloud OCR when sent to the e-mail addresses of the document categories. Afterward, each PDF-file on each e-mail is sent to and processed by ABBYY. When ABBYY has processed PDF-files, the result is downloaded to the Continia Cloud OCR services and removed from ABBYY.

Expiration - Data remains until downloaded to the customer or expire after 180 days.

Content - Data related to document categories. Ex.: Code, Description, Connection Endpoint Code

Data related to e-mails.

Ex: Sender e-mail, Sender name, Subject, Body, all attachments

Sensitivity - Personal data of Sender e-mail and Sender name is considered less sensitive.

The content of e-mail and attachments can potentially be sensitive personal data.

Data related to Continia Expense Management

When using Expense Management, there are multiple integration points where data is sent to and received from NAV to Continia Online Services and to the mobile Expense app.

Flow - Expense users are synchronized to Continia Online Services to allow them to log in to the app and the Expense Portal.

Master Data from NAV is synchronized to Continia Online Services and used when working with expenses and mileage in the app or the Expense Portal.

There are three different ways to process Bank transactions:

1) Bank transactions can be received by Continia Online Services from the bank, on behalf of the Customer. Later, bank transactions are downloaded to the Customer and deleted from Continia Online Services.

2) Bank transactions can be downloaded as a file by the customer, directly from the bank. This file is uploaded to Continia Online Services, which will process it and return it immediately to the customer.

3) Bank transactions can be processed by Continia Document Capture with OCR On-Premise or Continia Cloud OCR. Please refer to the section “Data related to Continia Document Capture” for more details.

The expense app downloads data from Continia Online Services and stores it on the device. When a user creates or updates an existing record in the app, then it is automatically sent to Continia Online Services and made available for download to NAV.

The Expense Portal hosted by Continia Online Services uses data already synchronized to Continia Online Services. When a user creates or updates an existing record, then it is automatically updated with Continia Online Services and made available for download to NAV and to the app.

Expiration - Expense users remain for 180 days or until removed and exported from NAV.

Master Data from NAV remains until removed in NAV or maximum 180 days and the synchronization routine has run in NAV.

Bank transactions received by Continia Online Services from the bank remains until the synchronization routine has run in NAV or for maximum 180 days.

All expenses, mileage, settlements and related data are stored with Continia Online Serives while Status = “Pending Expense User”. When Status is no longer “Pending Expense User” they are removed from Continia Online Services when the synchronization routine has run in NAV or maximum 180 days.

When expense, mileage or settlement is approved, this can trigger an approval notification to the user. Approval notifications are uploaded to Continia Online Services and downloaded to the app when it connects. Approval notification is removed from Continia Online Services after downloading to the app. The approval notification is removed from Continia Online Services if not downloaded by the app within 90 days.

Historical expenses, mileage, and settlements is stored in the app and devices they have been downloaded to. The user can either delete history manually or configure automatic deletion, i.e. after one month. History is also deleted if the app is uninstalled or the phone is reset.

History in the app is not deleted by deleting the user in NAV as there is no way to control that the device and app get connected to the internet.

Content - Data related to expense users.

Data related to master data.

Ex: Expense types, Dimensions, and other configured fields with a look up to a table

Data related to bank transactions. Ex.: Card ID, Card name, Date, Amount, Place of purchase.

Data related to expenses. Ex.: User identification, Expense type, Date, Description, Amount.

Data related to mileage. Ex.: User identification, Date, Address where the user was driving from and to

Data related to settlements. Ex.: User identification, Date, associated expenses and mileage

Sensitivity - Master data is not considered personal sensitive.

All other data is considered personal sensitive.

Data related to Continia Web Approval Portal

The Web Approval Portal works in combination with Continia Document Capture and Continia Expense Management. The Web Approval Portal can either be installed On-Premise or hosted with Continia Software. Only when hosted with Continia Software data is stored with Continia Online Services.

Flow - When a user logs in to the Web Approval Portal, then data is read from NAV using NAV Web Services. When a user accesses a record for approval, then the primary PDF or JPG for that document is uploaded from NAV and displayed to the user.

Expiration - Users remain until removed from the solution in NAV. It is the customers responsibility to manage user from within NAV and synchronize with Continia Online Services.

General approval data (except PDF-files and attachments) related to documents for approval is stored in the cache of the current user and removed when the session of the user expires.

PDF-files and attachments will be stored for 4 hours and removed afterward.

Content - Data related to allowed users. Ex.: Dynamics NAV username, Windows username, E-mail address, Full name

General approval data related to documents for approval. Ex: purchase invoice header and line information, expenses, list of required approvers, approval comments, etc.

PDF-files and attachments: depend on the content of PDF-files and attachments. Typically, at least a copy of the purchase invoice.

Sensitivity - Personal data of users are considered sensitive.

The content of approval data, PDF-files and attachments are considered potentially personal sensitive.

Data related to Continia Payment Management

When using Payment Management, you can create, send and retrieve payment files.

This is accomplished with the use of two external components (dll-files), meaning they are not part of the Microsoft Dynamics NAV software package, but delivered by Continia Software:

1. The Continia Bank Integration Component (CBIC) for creating the file, and

2. The Continia Bank Communication Component (CBCC) for sending the file to the bank and for retrieving status files, inpayment files and account statements.

In Payment Management however, you have the choice to either:

1. Install and use the Continia Bank Integration Component (CBIC) locally, or

2. Use the Continia Bank Integration Component (CBIC) on Continia Online.

The Continia Bank Communication Component (CBCC) is always installed locally.

Depending on your settings above, only Continia Online-installed components is Continia Software's responsibility and therefore relevant for this documentation. Locally installed components, or files saved to a local file-location, is the responsibility of the user.

Flow - Creating the payment file:

When creating payments with Payment Management, an xml-formatted file is created with payment data from Dynamics NAV. The file is then sent to the CBIC component, either installed locally or by using the Continia Online version.

The CBIC component then processes the payment data in the xml-formatted file and creates a new xml-formatted file that fits with the chosen bank's file format. The new file is then sent back to Dynamics NAV.

Sending the payment file:

When sending payments with Payment Management, (the payment file returned by the CBIC component), depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, the payment file generated by the CBIC will be sent to the locally installed CBCC component, which will handle the communication with the bank using the user's Certificate.

2. If the user has selected Manuel Communication, the payment file generated by the CBIC is saved on a user-specific file location. The user must then manually upload the file to the bank either using a SFTP-folder or using the bank's online system, which will handle the communication with the bank.

Retrieving status files, inpayment files and account statements:

When receiving status files, inpayment files and account statements with Payment Management, depending on which setting the user has selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, Dynamic NAV generates a request file and sends the file to the locally installed CBCC, which will handle the communication with the bank using the user's Certificate. Based on the request-file, the CBCC component then retrieves the files requested and sends the files back to Dynamics NAV.

2. If the user has selected Manuel Communication, the files must be manually downloaded, for example using the bank's online system, and afterwards imported into Dynamics NAV using Payment Management feature-specific import actions.

Expiration - Using Continia Bank Integration Component (CBIC):

Creating the payment file: Data is not saved locally, and they expire immediately after the generated xml file is sent back to Dynamics NAV.

Using Continia Bank Communication Component (CBCC):

Creating Certificate: Data is not saved locally, and they expire immediately after the certificate is sent to the bank and secure communication has been established.

Sending the payment file: Data is not saved locally, and they expire immediately after the file is sent to the bank.

Retrieving status files, inpayment files and account statements: Data is not saved locally, and they expire immediately after the retrieved files are sent to Dynamics NAV.

Content - Data related to Creating and Sending Payment file:

Sender Ex.: Bank Reg. No., Account No., Address, CVR, CPR, Amount, Company Name, Company Address, Currency, Bank Name, Bank IBAN, Bank SWIFT, Sender reference.

Recipient Ex.: Name, Address, Account No. Account Reg. No., Bank Name, Bank IBAN, Bank SWIFT, Creditor Number, SE-No., P-No., Receiver Reference.

Creating Certificate Ex.: Sender-id, Signer-id, Receiver-id, Certificate-holder, activation-code.

Data related to Retrieving status files, inpayment files and account statements Ex.:

Bank user information, File reference number from bank, Swift number, IBAN.

Sensitivity - All data is considered personal sensitive.

Data related to Continia Payment Management 365

When using Continia Payment Management 365 you can create, send and retrieve payment files.

This is accomplished with the use of two external components installed on Continia Online, meaning they are not part of the Dynamics 365 Business Central software package, but delivered by Continia Software.

1. The Continia Bank Integration Component (CBIC) for creating the file, and

2. The Continia Bank Communication Component (CBCC) for sending the file to the bank and for retrieving status files, inpayment files and account statements.

Locally installed components, or files saved to a local file-location, are the responsibility of the user.

Flow - Creating the payment file:

When creating payments with Payment Management 365, an xml-formatted file is created with payment data from Dynamics 365 Business Central. The file is then sent to the CBIC component on Continia Online.

The CBIC component then processes the payment data in the xml-formatted file and creates a new xml-formatted file that fits with the chosen bank's file format. The new file is then sent back to Dynamics 365 Business Central.

Sending the payment file:

When sending payments with Payment Management 365, (the payment file returned by the CBIC component), depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, the payment file generated by the CBIC will be sent to the CBCC component on Continia Online, which will handle the communication with the bank using the user's Certificate.

2. If the user has selected Manuel Communication, the payment file generated by the CBIC is saved on a user-specific file location. The user must then manually upload the file to the bank either using a SFTP-folder or using the banks online system, which will handle the communication with the bank.

Retrieving status files, inpayment files and account statements:

When receiving status files, inpayment files and account statements with Payment Management 365, depending on which setting the user have selected when setting up the bank, the following flow is used:

1. If the user has selected Direct Communication, Dynamics 365 Business Central generates a request file and sends the file to the CBCC component on Continia Online, which will handle the communication with the bank using the user's Certificate. Based on the request-file the CBCC component then retrieves the files requested and sends the files back to Dynamics 365 Business Central.

2. If the user has selected Manuel Communication, the files must be manually downloaded, for example using the bank's online system, and afterwards imported into Dynamics 365 Business Central using Payment Management 365 feature-specific import actions.

Expiration - Using Continia Bank Integration Component (CBIC):

Creating the payment file: Data is not saved locally, and they expire immediately after the generated xml file is sent back to Dynamics 365 Business Central.

Using Continia Bank Communication Component (CBCC):

Creating Certificate: Data is not saved locally, and they expire immediately after the certificate is sent to the bank and a secure communication has been established.

Sending the payment file: Data is not saved locally, and they expire immediately after the file is sent to the bank.

Retrieving status files, inpayment files and account statements: Data is not saved locally, and they expire immediately after the retrieved files is sent to Dynamics 365 Business Central.

Content - Data related to Creating and Sending Payment file:

Sender Ex.: Bank Reg. No., Account No., Address, CVR, CPR, Amount, Company Name, Company Address, Currency, Bank Name, Bank IBAN, Bank SWIFT, Sender reference.

Recipient Ex.: Name, Address, Account No. Account Reg. No., Bank Name, Bank IBAN, Bank SWIFT, Creditor Number, SE-No., P-No., Receiver Reference.

Creating Certificate Ex.: Sender-id, Signer-id, Receiver-id, Certificate-holder, activation-code.

Data related to Retrieving status files, inpayment files and account statements Ex.:

Bank user information, File reference number from bank, Swift number, IBAN.

Sensitivity - All data is considered personal sensitive.

Data related to Continia MobilePay 365

When using Continia MobilePay 365 you can create and send collection request to MobilePay Denmark and retrieve status files. This communication is established using Continia Online components.

During communication to MobilePay Denmark, the Customer's MobilePay Business Credentials will be sent to Continia Online. These MobilePay Business Credentials are necessary because the Continia Online component needs to check that the MobilePay Business Credentials are valid, before making any MobilePay collections.

Customer Data will be sent to Continia Online as a part of the collection request.

Flow - When installing the Continia MobilePay 365 extension on Dynamics 365 Business Central, the user will be asked to enter the MobilePay Business Credentials. This happens as a part of the initial configuration of the extension.

Expiration - Business Credentials: MobilePay Business Credentials will be sent to Continia Online when creating a collection request. As soon as the Business Credentials has been validated, they will expire on Continia online.

Customer data: Customer data will be sent to Continia Online as a part of the collection request. The collection request and the related data will not be saved on contina online and expires when the request is sent to MobilePay.

Status files: Callbacks from MobilePay will contain information about the collection request and the Customer. Callbacks will be stored on Continia online until they are collected by Continia MobilePay 365 on Dynamics 365 Business Central. If callbacks are not collected, they will be stored for a maximum of 180 days.

Content - Credentials: Credentials for MobilePay Business.

Customer data: Name, E-mail, Phone No., Amount.

Callback data: Name, E-mail, Phone No., Amount.

Sensitivity - All data is considered personal sensitive.

Data Related to Continia MobilePay Invoice

When using MobilePay Invoice you can create and send invoices as a request for payment to MobilePay Denmark A/S and retrieve status answers and inpayment files.

This is accomplished with the use of an external component installed on Continia Online, meaning it is not part of the Microsoft Dynamics 365 Business Central software package, but delivered by Continia Software:

1. The Continia MobilePay Interface Component.

Below is a description of how MobilePay Invoice communicates with Continia Online.

Flow - Creating the invoice request: When creating an invoice request with MobilePay Invoice, a json-formatted request is created with data from Business Central. The request is then sent via a secure https-protocol to the Continia MobilePay Interface Component on Continia Online.

The Continia MobilePay Interface Component then sends the request to MobilePays API.

Sending the invoice request: When sending invoice request with MobilePay Invoice, the following flow is used:

1. If the user has selected InvoiceDirect, the invoice request generated by the Continia MobilePay Interface Component is send to the MobilePay Portal using the OpenID Certified certification process.

2. If the user has selected InvoiceLink, the invoice request generated by the Continia MobilePay Interface Component is sent to the MobilePay Portal using the OpenID Certified certification process. The MobilePay Portal then creates a Link which is returned to the Continia MobilePay Interface Component and embedded in the invoice and invoice request.

Retrieving status on invoices: Status for the MobilePay Invoices will be sent to Continia Online from MobilePay, they will then await a request from MobilePay Invoice to import the new states of all active payments.

Expiration - Using MobilePay Invoice:

Sign-up: when signing up, data is stored at Continia Online to enable communication with MobilePay.

Sending invoices: When sending invoices, data is stored at Continia Online.

Retrieving Status: When Status of Invoices is imported to MobilePay Invoice, data will be stored at Continia Online.

Content - Data related to Creating and Sending Payment file:

Sign-up: Merchant Id, Client ID, API key, is merchant id registered with another company on Continia Online.

Sender Ex.: Business Central Invoice Id, MobilePay Invoice ID, AccessToken, RefreshToken, Callback url, status.

Data related to Retrieving status on payments:

Error code, error message, Invoice callback id, redirect url for payment.

Sensitivity - All data is considered personal sensitive.

Data related to Continia Mobilepay 365 Subscription

When using MobilePay Subscriptions you can create and send payment agreements and one-off payments as a request for payment to MobilePay Denmark A/S and retrieve status, answers, inpayment files and automatically collect payments as long as the payment agreement is active.

This is accomplished with the use of an external component installed on Continia Online, meaning it is not part of the Microsoft Dynamics 365 Business Central software package, but delivered by Continia Software:

1. The Continia MobilePay Interface Component.

Below is a description of how MobilePay Subscriptions communicates with Continia Online.

Flow - Creating the Payment agreement and One-off payment request: When creating a payment agreement or one-off payment request with MobilePay Subscriptions, a json-formatted request is created with data from Business Central. The request is then sent via a secure https-protocol to the Continia MobilePay Interface Component on Continia Online.

The Continia MobilePay Interface Component then sends the request to MobilePays API.

Sending the Payment Agreement request: When sending Payment agreement request with MobilePay Subscriptions, the following flow is used:

1. The payment agreement request generated by the MobilePay Subscriptions Extension is sent to the MobilePay Portal using Continia Online.

2. The MobilePay Portal creates a Link which is returned to the Continia MobilePay Interface Component, which is returned to Business Central and then used to either send to customer or open inside Business Central and send the payment agreement request directly to the customers mobile phone.

Retrieving status on payment agreements: Status for the MobilePay payment agreement will be sent to Continia Online from MobilePay, Continia Online will then await a request from MobilePay Subscriptions to import the new states of all active payment.

Sending payments: When creating a payment on an existing MobilePay Subscriptions agreement, the following flow is used.

The One-off payment request generated by MobilePay Subscriptions Extension is sent to Continia Online which then sends the request to the MobilePay Portal. The MobilePay Portal then creates a Link which is returned to Continia MobilePay Interface Component, which is returned to Business Central where users are able to open the link in Business Central or send it to the customer for activating the One-off payment making it appear in their MobilePay app.

Recurring payment request generated by the MobilePay Subscriptions Extension is sent to Continia Online which then sends the request to the MobilePay Portal. The payment will be collected unless the customer cancels it.

Retrieving status on payments: Status for the MobilePay One-off payments will be sent to Continia Online from MobilePay. Continia Online will then await a request from MobilePay Subscriptions to import the new status of all active One-off payments.

Status for the MobilePay recurring payments will be sent to Continia Online from MobilePay, Continia Online will then await a request from MobilePay Subscriptions to import the new status of all recurring payments.

Expiration

Using MobilePay Subscriptions:

Sign-up: when signing up, data is stored at Continia Online to enable communication with MobilePay.

Sending payment agreements: when sending payment agreements, data is stored at Continia Online.

Retrieving Status: When States of payment agreements is imported into MobilePay Subscriptions, data will be stored at Continia Online.

Content

Data related to Creating and Sending payment agreement:

Sign-up: Merchant Id, Client ID, Company GUID, AccessToken and RefreshToken, whether the merchant id registered with another company on Continia Online.

Callbacks: Provider Id, API key, configured callback urls.

Data related to Retrieving status on payment agreements:

Agreement-Id, internal-id, transaction-id, timestamp, Status_code, Status_text and

Status. Sensitivity: All data is considered personal sensitive.

1.2 Categories of data subjects

Data regarding the following categories of data subjects are processed:

A) Expense Data for employees submitted by Expense Users

B) Document Data for documents submitted to the Continia solutions.

C) Bank Data created and processed by the Continia solutions.

D) User Data for the users' setup to use the Continia solutions.

E) Usage Data from users/companies using the Continia solutions.