Ver. 2023-10-25

Undervedlegg till Vedlegg 1 Databehandleravtale
Undervedleggene gjelder for Vedlegg 1:

Annexes to DATA PROCESSING AGREEMENT
The Annexes are applicable for Appendix 1:

*ANNEX I*

**List of parties**

**Controller(s):** [*Identity and contact details of the Controller(s), and, where applicable, of the Controller's data protection officer]*

Name: The company specified as the Customer (*NO: Kunde*) on the front page of the Framework Agreement between PayEx and Customer concerning Invoice Services and/or Ledger Services (*NO: Fakturaservice /Reskontroservice*) provided by PayEx to Customer

Address: Ref. to the front page of the Framework Agreement between PayEx and Customer.

Contact person's name, position and contact details: Ref. to the front page of the Framework Agreement between PayEx and Customer.

Name and contact details of data protection officer [*if applicable*]: Information to be provided by Customer on request from PayEx.

**Processor(s):** [*Identity and contact details of the Processor(s) and, where applicable, of the Processor's data protection officer]*

Name: The company or its foreign division specified as PayEx on the front page of the Framework agreement concerning Invoice Services and/or Ledger Services (*NO: Fakturaservice /Reskontroservice*) provided by PayEx to Customer.

Address: Ref. to the front page of the Framework Agreement between PayEx and Customer.

Contact person's name, position and contact details: Ref. to the front page of the Framework Agreement between PayEx and Customer.

| | | |
|---|---|---|
| Contact details of data protection officer: | E-mail: | dpo@payex.com , |
| | Address: | PayEx Sverige AB, att: Dataskyddsombudet, 621 88 Visby, Sweden |
| | Phone: | +46 (0) 8 - 20 24 00 |

*ANNEX II*

**Description of the processing**

*Categories of data subjects whose personal data is processed*

Controller's employees, Controller's customers and thus receivers of invoices, Controllers owners and members of board/management

*Categories of personal data processed*

Authentication information (personal ID number, bank account number), Contact information (Name, address, telephone number, e-mail) Historical information (purchased goods & services), Transaction information (purchased goods & services), Tracking information (IP address, cookies)

*Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

Unless otherwise explicitly instructed by Controller in this DPA, in writing, and accepted by Processor, no special categories of personal data will be processed. Special categories of personal data include racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

*Nature and subject matter of the processing*

Subject matter of the processing is to provide invoice services and related ledger services as further specified in the Agreement between Controller and Processor. Furthermore, Processor needs, as required by law, to know its customers in order to ensure that the Service does not inadvertently support illegal activities and to curb fraud and other misuse of the Service.

Nature of the processing is to perform processing which is necessary for the purpose set forth above, including inter alia recording, organization, structuring, storage, adaptation and alteration, retrieval, consultation, transfer, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

*Purpose(s) for which the personal data is processed on behalf of the Controller*

Is to enable Processor to fulfill its obligations under the Agreement. The Processor may also process all categories of personal data set forth above for the purpose of improving the Service. Furthermore, Processor needs, as required by law, to know its customers in order to ensure that the Service does not inadvertently support illegal activities and to curb fraud and other misuse of the Service.

*Duration of the processing*

The duration of processing is limited to the period of time necessary to provide the Service, unless where otherwise is set forth in the Agreement or in Applicable Law or in Annex V of this DPA.

*Frequency of transfer (e.g. whether the data is transferred on a one-off or continuous basis)*

Continuous basis

*For processing by (sub-) processors, also specify subject matter, nature and duration of the processing*

Please see Appendix IV and V

Processor is entitled to engage Sub-Processors within the EU/EEA as well as outside the EU/EEA, provided that the provisions of the Agreement and this DPA are complied with.

*ANNEX III*

**TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**The Processor shall implement technical and organisational measures to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons. The technical and organisational measures are described below in this Annex.**

## 1. MEASURES FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA

**a) Technical measures for transfer within EU/EEA or to a country with an EU adequacy decision**
The Processor shall have an implemented policy for the use of cryptography, including use of cryptography controls, protection and management of cryptographic keys throughout the lifecycle and availability of encrypted information (as part of the contingency planning). The Processor shall apply cryptographic techniques to ensure the information integrity and confidentiality (e.g. to protect information in transit and at rest). See also section 6, Measures for the protection of data during transmission.

**b) Supplementary measures for transfer to 3rd countries**
In addition to the requirements under 1 a) above, this section is applicable in the case of transfer of personal data to a 3rd country.

All personal data must be encrypted or pseudonymised prior of transfer to prevent unauthorized access.
Keys for decryption and/or for translating pseudonymised personal data to the clear must be kept by Controller or an entrusted party within the EU/EEA. The encryption and/or pseudonymisation must be implemented in such a way that it fulfils the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." Adopted by the European Data Protection Board at any given moment. This is to ensure that the encryption algorithm and its parameterization is implemented to provide robust protection against cryptanalysis performed by the public authorities in the recipient country taking into account:

1. The resources and technical capabilities (e.g. computing power for brute-force attacks) available to them
2. The strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved.
3. That the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities
4. The keys and/or pseudonymisation data are reliably managed following best practices to prevent disclosure or unauthorized access.
5. Assessment of the strength of encryption algorithms, their robustness against cryptanalysis over time.
6. When using pseudonymisation the personal data must be processed in such a manner that the personal data can no longer be attributed to a specific data subject, or be used to single out the data subject in a larger group, without the use of additional information.
7. It is established by means of a thorough analysis of the data in question – taking into account any information that the public authorities of the recipient country may be expected to possess and use - that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

The Processor shall promptly make needed updates to the service needed to continue to be compliant with above requirements.

## 2. MEASURES FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES

The Processor shall process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. The Processor shall have a documented and implemented framework of information security controls to ensure the protection of information and IT-services. The security controls shall ensure protection of the information confidentiality, integrity and availability in transit, in use and at rest throughout its lifecycle and, including following principles:

a) treat information security as an integral part of the overall system design and integrate security controls at different IT-services levels (e.g. application, computer and network level).
b) implement the principle of 'defence in depth' or equivalent, where multiple layers of protection exist (e.g. authentication, segmentation, hardening, authorization, malware protection, logging) to avoid reliance on

one type or method of security control.

c) when a system or a component shall interact with other systems and components, it shall be assumed that these are unsecure.
d) implement the least privilege principle (e.g. only the minimum possible privileges are granted to a user or a process when accessing the system).
e) design and implement a basic functionality for audit trail.

The Processor shall also continuously monitor the effectiveness of the security controls and remediate any found deficiencies promptly.

**3. MEASURES FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT**

The Processor shall have;

- Documented and implemented procedures for managing information security incidents to ensure a quick, effective and structured response to information security incidents.
- An emergency response process for dealing with severe security incidents.
- Business Continuity Plans and Disaster Recovery Plans or equivalent to maintain acceptable service levels in the event of problems which may disrupt the availability of the information or IT-services. The Processor shall regularly test the plans and evaluate the test results for continuous improvement.
- Documented and implemented backup procedures to ensure that the information and IT-services are backed-up and restored within decided time frames. The procedure shall take different risks into consideration (e.g. hardware failure, ransomware). Backups shall be protected.
- Backup images shall be taken and tested regularly in accordance with decided recovery point objective and recovery time objective.

**4. MEASURES FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING**

The Processor shall have a documented and implemented risk management process and assurance program to monitor the control effectivess, identify and manage outstanding information security related risks, to ensure the confidentiality, integrity and availability of the Processor's information.

The Processor shall perform information security follow-up activities (e.g. measurements, reviews, assessments and testing) to ensure that information security controls are effective and are not being bypassed and that deviations and risks are identified (e.g. gap analysis against information security policy and procedures, compliance reviews, IT-service information security risk review, penetration testing, internal and external audits of the IT-services). The Processor shall evaluate the results of the information security follow-up and update their security procedures and implemented controls without undue delays.

It is by default not allowed to use Controller´s personal data for testing activities unless explicit approved by Controller.

**5. MEASURES FOR USERS IDENTIFICATION AND AUTHORISATION**

The Processor shall have documented and implemented procedures for access management. Such procedures should be monitored and audited regularly.

The procedures shall include the following:

a) User accountability: users shall have and use unique user-ids to ensure that users can be identified for the actions performed in the IT-services. The Processor should therefore not use shared accounts in IT-services.
b) Access rights: shall be granted on a 'need-to-know' and least privilege basis and shall be granted, modified or withdrawn in a timely manner.
c) Authorisation: provided access rights shall be subject to documented authorisations.
e) Segregation of duties: conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse.
f) Authentication: authentication methods shall correspond with the sensitivity of the personal data and IT-services.
g) Access recertification: access rights shall be periodically reviewed (at least every 6 months for privileged access) to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.
h) Logging of user activities in IT-services: activities by users shall be logged and monitored. Privileged access shall be subject to stricter enhanced logging and monitoring.

i) Privileged access rights: stronger controls over privileged access shall be applied, e.g. by a strict authorisation process, minimize privileges, apply multi-factor authentication, granular logging, closely supervising accounts, ensure segregation of duties.

## 6. MEASURES FOR THE PROTECTION OF DATA DURING TRANSMISSION

All personal data must be encrypted during transmission. The Processor shall have security controls that can protect against unauthorized traffic interception or interference. Wireless network connection shall be encrypted according to best practice.

The Processor shall have documented and implemented procedures for granting corporate network access to only authorised devices. The Processor should evaluate whether endpoints (e.g. servers, workstations, mobile devices) meet the security standards defined by them before they are granted access to the corporate network.

The Parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure to ensure authentication of both sender and receiver involved in all communication. If transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer.

The encryption of personal data in transit must be implemented in such a way the it fulfils the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." Adopted by the European Data Protection Board at any given moment.

## 7. MEASURES FOR THE PROTECTION OF DATA DURING STORAGE

Additional to all other controls described in this document that apply to information at rest including but not limited to, encryption, authentication/authorization and audit trail, the Processor shall have documented and implemented backup procedures to ensure that the information and IT-services are backed-up and restored within decided time frames. The procedure shall take different risks into consideration (e.g. hardware failure, ransomware). Backups shall be protected. Backup images shall be taken and tested regularly in accordance with decided recovery point objective and recovery time objective.

If personal data is transferred to a 3rd country for storage it must be encrypted prior to transfer in accordance to section. See section 1, Measures for pseudonymisation and encryption of personal data.

## 8. MEASURES FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH PERSONAL DATA ARE PROCESSED

The Processor shall continuously identify physical and environmental threats (e.g. natural disasters, malicious attacks, accidents) and implement adequate controls to mitigate these threats. Physical access to facilities and IT-equipment where Controller's personal data is processed shall be limited to authorized employees. For cloud based hosting the Processor is obligated to utilize established and well known vendors with datacentres within EU.

The Processor shall have a documented and implemented framework of information security controls to ensure the protection of information and IT-services (e.g. 2-factor authentication, intrusion system, fences). All accesses to the premises shall be registered and logged. Data centres require a strict physical access control and additional security arrangements (e.g. guarding, humidity control, fire alarms, temperature control, and redundant electricity supply).

## 9. MEASURES FOR EVENTS LOGGING

The Processor shall have at least a basic system that enables logging of events.

## 10. MEASURES FOR SYSTEM CONFIGURATION, INCLUDING DEFAULT CONFIGURATION

The Processor shall have documented and implemented security configuration baselines of all components (e.g. operating system, databases, network devices). The Processor shall continuously check the technical compliance of IT-services against a defined security baseline (e.g. hardening configuration). Identified deviations shall be assessed and addressed by appropriate measures to address the associated risk.

## 11. MEASURES FOR INTERNAL IT AND IT SECURITY GOVERNANCE AND MANAGEMENTS

The Processor shall have documented and implemented roles and responsibilities for information security, including accountability and responsibility for information security across the organisation. The Processor shall have an individual role appointed with an overall responsibility for the information security management within the organisation (e.g. CISO).

## 12. MEASURES FOR CERTIFICATION / ASSURANCE OF PROCESSES AND PRODUCTS

The Processor shall have implemented an Information Security Management System (ISMS) to ensure that the information security work performed by the Processor is structured, adequate and subject to management review. The ISMS shall comply with common information security standards (e.g. ISO/IEC 27001 or reasonable alternative and include an information security framework (e.g. policy and procedures), that is implemented across the Processor 's organisation, including services provided to Controller. If there are any specific requirements on certification/assurance stipulated by applicable law or regulation or as specified by Controller elsewhere, then these requirements must be fulfilled.

## 13. MEASURES FOR ENSURING DATA MINIMISATION

The Processor shall also ensure to process and store the personal data in accordance with any written Instructions from Controller, documented in writing in the DPA between Processor and Controller.

## 14. MEASURES FOR ENSURING DATA QUALITY

The Controller must ensure there are documented processes and routines to ensure that personal data must be accurate and up to date.

## 15. MEASURES FOR ENSURING LIMITED DATA RETENTION

The Processor shall have procedures for handling data retention and deletion in accordance with Instructions from the Controller.

## 16. MEASURES FOR ALLOWING DATA PORTABILITY AND ENSURING ERASURE

The Processor must be able to support Controller to fulfil its obligations about data portability as described in GDPR.

The Processor shall have documented and implemented procedures to ensure that all Processor storage media devices are securely erased or physically destroyed by using generally accepted methods (e.g. NIST SP 800-88 guidelines for Media Sanitization) for secure information removal.

**……**

Ver. 2023-10-25

*ANNEX IV*

**List of sub-processors**

The Processor has been authorised by Controller to use the following sub-processors. Additions and/or changes to this list are regulated in the DPA including Annex 1 clause 7.7 (a):

**Name:** All sub-processors used by Processor are listed in the matrix below

**Address:** Please see the matrix below

**Contact person's name, position and contact details:** Could be provided by Processor to Controller on written request from Controller.

**Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):** Please see the matrix below

**Categories of data subjects**: Please see the matrix below

**Categories of personal data**: Please see the matrix below

**Retention period of personal data**: Please see the matrix below

**Place of processing**: Please see the matrix below

**Frequency of transfer of personal data**: Please see the matrix below

| Name and address of the Subprocessor | Description of the processing | Categories of Data Subjects | Categories of Personal Data | Retention period of Personal Data | Place of Processing | Frequency of transfer of Personal Data |
|---|---|---|---|---|---|---|
| Postnord Strålfors AB, Terminalvägen 24, 171 73 Solna | Print of invoices*, claims and letters<br><br>***Only applicable for "Invoice Service"** | Controller's customers | Authentication information, Contact information, Transaction Information | 90 days | Sweden | Daily, when invoices, claims and letters are printed |
| Edi solutions AB, Box 9169, 400 94 Göteborg (*Not valid for Ledger service for Receivables* | Integration and restructuring of data files sent by Controller | Controller's customers | Authentication information, Contact information, Transaction Information | Incoming/outgoing files/API, database, backups: 6 months<br><br>E-mail with Set up instructions (including PayEx contact information): deleted | Sweden, Cloud storage servers are located within EU | Daily, when integration is used by client for invoicing or reporting back to clients ERP. |

| | | | | | | |
|---|---|---|---|---|---|---|
| *Lending PxR*) | | | | immediately after Set up is done.<br><br>E-mail from PayEx customers: Microsoft 365 GDPR-standard | (Azure) | |
| 21 Grams, Lumaparksvägen 9, 12125 Stockholm | Distribution of e-invoices B2C* (online banking) and B2B (EDI), digital distribution of claims and letters<br>***Only applicable for "Invoice Service"** | Controller's customers | Authentication information, Contact information, Transaction Information | 90 days | Sweden, Norway, Finland, Denmark, depending on distribution destination | Daily, when invoices, claims and letters are distributed |
| In cases where Controller integrates to PayEx through use of Partner, such Partner will be considered a sub-processor to Processor | See Annex V p. 5. Partner will receive invoice, ledger and/or payment information reports from Processor. | Information listed in Annex II of this DPA | Information listed in Annex II of this DPA | As instructed by Controller to Partner and/or PayEx. | As agreed between Partner and Controller. | Daily |
| Asteria AB Sveavägen 45, 1 tr 111 34 Stockholm | Integration and restructuring of data files sent by Controller | Controller's customers | Authentication information, Contact information, Transaction Information | Incoming/outgoing files/API, database, backups: 6 months<br><br>E-mail with Set up instructions (including PayEx contact information): deleted immediately after Set up is done.<br><br>E-mail from PayEx customers: Microsoft 365 GDPR-standard | Sweden, Cloud storage servers are located within EU (Azure) | Daily, when integration is used by client for invoicing or reporting back to clients ERP. |

Ver. 2023-10-25

| | | | | | | |
|---|---|---|---|---|---|---|
| SpeedLedger AB<br>Fabrikstorget 1<br>412 50 Göteborg<br>(*Not valid for Ledger Service for receivables lending PxR or Invoice service PxR*) | Integration and restructuring of data files sent by Controller | Controller's customers | Authentication information, Contact information, Transaction Information | Incoming/outgoing files/API, database, backups: 6 months<br><br>E-mail with Set up instructions (including PayEx contact information): deleted immediately after Set up is done.<br><br>E-mail from PayEx customers: Microsoft 365 GDPR-standard | Sweden, Cloud storage servers are located within EU (Azure) | Daily, when integration is used by client for invoicing or reporting back to clients ERP. |
| Apix Messaging Oy*<br>(*Only valid for; Ledger service for Receivables Lending PxR Finland*) | Conversion of invoice data formats | Controller's customers | Authentication information, Contact information, Transaction Information | Incoming invoices, database backups: 7 years | Finland, Cloud storage servers are located within EU | Daily, when integration is used by client for invoicing |
| LinkMobility | Storage and distribution of SMS/messaging | Controller's customers | Mobile number and messages | 3 months | EU/EEA | Continuous |
| Mastercard Payment Services (only applicable for Invoice service in Norway) | Storage and invoice hotel | Controller's customers | Information listed in Annex II of this DPA | Mastercard Payment Services GDPR-standard | EU/EEA | Continuous |
| Microsoft Azure<br><br>Microsoft Ireland Operations Limited<br>One Microsoft Place<br>South County Business Park<br>Leopardstown<br>Dublin 18<br>D18 P521<br>Irland | Microsoft Azure is a cloud computing platform. It provides a broad range of cloud services, including compute, analytics, storage and networking. Azure serves as | Information listed in Annex II of this DPA | Information listed in Annex II of this DPA. | Processor has the ability to access, extract and delete data stored. Principles for retention and deletion of data follows the written instructions documented in the DPA between Processor and Controller and as such the Sub-processor has no influence over access, extraction and deletion of data stored. | Microsoft shall store and process Customer Data within the European Union with primary storage location in Microsoft Clod Data Centers in | Continuous |

| | | | | | | |
|---|---|---|---|---|---|---|
| *Please note that Processors use of Sub-processor Microsoft Azure is initiated in steps and that the engagement is expected to be in full use at end of Q4 2024 and that the start date for migration to Microsoft Azure is set to be initiated during Q1-Q3 2024.* | storage location and personal data is accessed, extracted and otherwise processed by Processor to provide the Service described in the Agreement between Controller and Processor. | | | | Gävle & Sandviken, Sweden and secondary (backup) storage location in Microsoft Clod Data Centers in Staffanstorp, Sweden | |
| Efecte AB Drottninggatan 33, 111 51 Stockholm Sweden | Case management | Controller's customers | Authentication information, Contact information, Transaction Information | Cases/tickets are retained for 13 months. | Finland | Ongoing, when end customers contact the Processor's customer service with invoice questions |
| Telia Company Stjärntorget 1, 169 79 Solna Sweden | Customer service via telephone and chat with the Telia ACE software | Controller's customers | Authentication information, Contact information, Transaction Information | Phone calls and chat logs are saved for 90 days. | Sweden | Ongoing, when end customers contact the Processor's customer service with invoice questions |

In addition to the list of sub-processors detailed in this ANNEX IV, Processor is entitled to process personal data within the PayEx Group when such processing is necessary to be able to provide the service in the manner defined in the Agreement. When a PayEx Group company processes personal data on behalf of Processor, each PayEx Group company undertakes to process Personal Data in accordance with Applicable Law, the Agreement and the Customer's instructions set forth in Appendix 1 and Annexes to the DPA between Controller and Processor.

Ver. 2023-10-25

*ANNEX V*

**Controllers instruction to Processor**

1. *Legal ground for processing*

Controller is responsible to ensure that the processing of data in accordance with the Agreement and this DPA is lawful under Applicable law, whether the data subjects have consented to the processing or if there is another legal ground for the processing, and that the personal data covered by this DPA and that Processor processes on behalf of Controller have been collected for specific, explicit and justified purposes, and otherwise in accordance with Applicable Law and that these purposes have been set forth in full and correct in Annex II. Controller will immediately give notice to Processor if the nature of the personal data processed under the Agreement changes.

Controller is further responsible to ensure that Processor does not process other categories of personal data than those set forth in Annex II on the behalf of Controller.

2. *Retention period and storage of Personal Data*

Processor will store personal data only as long as is necessary, ultimately governed by the Agreement as defined in the DPA p. 3.2. Controller has instructed Processor to provide the service in the manner defined in the Agreement. When Controller and Processor no longer have a valid Agreement in place, Processor will only store personal data if required by law or, in other cases, under the defined period of the Agreement, Contract Period, but no longer than to the point where Processor has ceased administration and terminated all cases that are in the ledger, including Claims that are under Monitoring.

Specification in relation to files communicated to Processor through file, CUSIN or API: Controller has agreed to observe Processor regulations and instructions applicable at the time relating to the sending and receiving of files. If a technical description has been prepared and appended to the Agreement, this shall be followed. Processor will store data received from Controller by file or by other electronic communication during a period of 13 months.

Specification in relation to files communicated by Processor to Controller. Storage of reports and created document have a general storage time of 13 months from creation, exemplified below, such as:

| **Report** | **Storage time** |
|---|---|
| Ledger report (Reskontrarapport) | 13 months from creation |
| Invoices created (Skapade fakturor) | 13 months from creation |
| Invoice (Fakturafordringar) | 13 months from creation |
| Surplus, detailed (Slutkund tillgodo, detaljerad) | 13 months from creation |
| Collection payments, detailed (Oplacerade inkassobetalningar, detaljerad) | 13 months from creation |
| Company accounts, detailed (Oplacerade betalningar, detaljerad) | 13 months from creation |
| Impairment report, detailed (Nedskrivningsrapport, detaljerad) | 13 months from creation |
| Impairment report (Nedskrivningsrapport) | 13 months from creation |
| Age analysis (Åldersanalys) | 13 months from creation |

3. *Distribution*

Processor will distribute invoices, claims and other communications described in the Agreement according to instruction received from Controller via API, file or other electronic communication, and distribute invoice as specified in Service Description of the agreement, when applicable. Controller guarantees, as described in section 1. Annex V of this DPA, the legal ground for processing and that Processor can distribute invoices, claims and other communications to data subjects received from Controller.

4. *Invoice Portal (Only applicable for "Invoice Service" based on ledger system PxR)*

Processor will make available invoice information relating to Controller's customers in an Invoice Portal. The Invoice Portal is available to end customers when receiving invoice per e-mail or when a link or integration to the Invoice Portal is established/used by Controller. In the Invoice Portal the end customer can access information about their invoices and follow the status of an invoice (paid/unpaid etc.). The end customer will also have the option to pay their received invoice through use of available payment means in the Invoice Portal. Controller instructs Processor to make available invoice information relating to Controller's customers in an Invoice Portal. Invoice information shall mean produced end customer invoices, reminders and where applicable debt collection notices (note: distribution of debt collection claims will follow the hierarchy described in the Service Description of the Agreement, as described here in section 3 of this Annex V. Invoice information and payment options about such distributed claims will however be available through Invoice Portal). The information in the Invoice Portal will be made available to the end customer according to Controllers instruction to Processor, i.e. when Processor is sending information through use of e-mail addresses (collected and transferred to Processor by Controller through file, CUSIN or API or as otherwise agreed between the Parties) to communicate invoices and other communications/documents/statements/compilations etc. The information in the Invoice Portal will generally be made available through link inclusion (in e-mail for example) or re-direct thereby transferring the end customer without need of identity verification/strong authentication, except in cases where the end customer is required to verify identity when using available payment means in the invoice portal, or when accessing information about a debt collection claim. Furthermore, Controller instructs Processor to make available information, to Controller in the form of reports or through other means as detailed in the Agreement, concerning Controller's customers who chooses to pay through use of available payment means in the Invoice Portal.

5. *Partner*

In scenarios where Controller has an integrated solution to Processor, meaning that Controller has integrated to Processor through use of a Partner (i.e. a separate legal entity providing, amongst others, integration services whereby Controllers ERP/e-commerce-system or similar is integrated to Processor on behalf of Controller), Controller hereby instructs Processor to receive such personal data, as is provided through Partner to Processor on behalf of Controller, as if it was directly received from Controller. Controller further instructs Processor to send invoice-, ledger- and payment reports/information to Partner. Personal data transferred to Partner will contain information listed in Annex II this DPA. For sake of clarity, Partner is considered a sub-processor only in relation to transferal of personal data, as instructed by Controller to Processor, in the form of invoice-, ledger- and payment reports/information.

In scenarios where Controller has a partner solution whereby Controller has a separate agreement with a Financing Partner (for example a Bank providing a financing solution to Controller) and a separate agreement with Processor (concerning invoice, administration and ledger services i.e. *Ledger service for Receivables Lending PxR*), and where Controllers agreement with the Financing Partner requires certain invoice/ledger data to be shared by Processor to such Financing Partner, Controller hereby instructs Processor to receive personal data, as is provided through Financing Partner to Processor on behalf of Controller, as if it was directly received from Controller. Controller further instructs Processor to send invoice-, ledger- and payment reports/information and credit related information to Financing Partner. Personal data transferred to Financing Partner will contain information listed in Annex II of this DPA. Controllers instructions are further detailed in the Service Agreement (section Processing of personal data) between Controller and Processor.

6. *Third-party service providers*

In a scenario where the Controller uses a third party to send/communicate information connected to the Service, Controller is responsible for such third party as for itself. If a third party is appointed by Controller to communicate invoice information, including personal data, via file, CUSIN or API or as otherwise agreed, Controller is responsible for such invoice

information, including personal data, and that the data has been collected in accordance with Applicable Law. If the Controller's agreement with a third party requires Processor to share certain invoice/ledger data with such third party, Controller hereby instructs Processor to receive personal data, provided through the third party to Controller on behalf of Controller, as if it were received directly from Controller. Controller further instructs Processor to send invoice, ledger and payment reports/information as well as credit-related information to such third party. Personal data transferred to third party will include information listed in Annex II to this DPA. Controller's instructions are, in applicable cases, further detailed in the Service Agreement (section regarding personal data) between Controller and Processor.