Ver. 2023-10-25

Bilag til Databehandleraftale
Bilagene gælder for Bilag 1:

BILAG I

LISTE OVER PARTER

Dataansvarlig(e): [Identitet og kontaktoplysninger for den eller de dataansvarlige og, hvor det er relevant, for den dataansvarliges databeskyttelsesrådgiver]

Navn: Virksomheden angivet som Kunde på forsiden af Rammeaftalen mellem PayEx og Kunden vedrørende Fakturaservice og/eller Reskontroservice leveret af PayEx til Kunden.

Adresse: Ref. til forsiden af Rammeaftalen mellem PayEx og Kunden.

Kontaktpersonens navn, stilling og kontaktoplysninger: Ref. til forsiden af Rammeaftalen mellem PayEx og Kunden.

Navn og kontaktoplysninger på den databeskyttelsesansvarlige [*hvis relevant*]: Oplysninger skal gives af Kunden efter anmodning fra PayEx.

Databehandler(e): *[Identitet og kontaktoplysninger for databehandleren eller databehandlerne og, hvor det er relevant, for databehandlerens databeskyttelsesrådgiver]*

Navn: Virksomheden eller dens udenlandske afdeling angivet som PayEx på forsiden af Rammeaftalen vedrørende Fakturaservice og/eller Reskontroservice leveret af PayEx til Kunden.

Adresse: Ref. til forsiden af Rammeaftalen mellem PayEx og Kunden.

Kontaktpersonens navn, stilling og kontaktoplysninger: Ref. til forsiden af Rammeaftalen mellem Databehandler og Kunden

Kontaktoplysninger databeskyttelsesrådgiver (DPO):

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

BILAG II

BESKRIVELSE AF BEHANDLINGEN

Kategorier af registrerede, hvis personoplysninger behandles

Dataansvarligs medarbejdere, Dataansvarligs kunder og dermed fakturamodtagere, Dataansvarligs ejere og medlemmer af bestyrelse/ledelse

Kategorier af personoplysninger, der behandles

Godkendelsesoplysninger (personligt id-nummer, bankkontonummer), kontaktoplysninger (navn, adresse, telefonnummer, e-mail) Historiske oplysninger (købte varer og tjenester), Transaktionsoplysninger (købte varer og tjenester), sporingsoplysninger (IP-adresse, cookies)

Følsomme oplysninger, der behandles (hvis relevant) og anvendte begrænsninger eller garantier, der fuldt ud tager hensyn til oplysningernes art og de involverede risici, f.eks. streng formålsbegrænsning, adgangsbegrænsninger (herunder kun adgang for personale, der har fulgt en specialuddannelse), registrering af adgangen til oplysningerne, begrænsninger for videreoverførsel eller yderligere sikkerhedsforanstaltninger.

Medmindre andet udtrykkeligt er oplyst af den Dataansvarlige i denne DPA, skriftligt og accepteret af Databehandleren, vil der ikke blive behandlet særlige kategorier af personoplysninger. Særlige kategorier af personoplysninger omfatter race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger eller fagforeningsmedlemskab og behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, data vedrørende helbred eller data vedrørende en fysisk persons sexliv eller seksuelle orientering.

Behandlingens art

Årsagen (*ENG: Subject matter*) til behandlingen er at levere fakturatjenester og relaterede finanstjenester som nærmere specificeret i Aftalen mellem Dataansvarlig og Databehandler. Ydermere skal Databehandleren, som påkrævet ved lov, kende sine kunder for at sikre, at Tjenesten ikke utilsigtet understøtter ulovlige aktiviteter og for at bremse svindel og andet misbrug af Tjenesten.

Karakteren (*ENG: Nature of the processing)* af behandlingen er at udføre behandling, som er nødvendig til det ovenfor anførte formål, herunder blandt andet registrering, organisering, strukturering, lagring, tilpasning og ændring, genfinding, konsultation, overførsel, brug, videregivelse ved transmission, formidling eller anden tilgængeliggørelse , justering eller kombination, begrænsning, sletning eller ødelæggelse.

Formål, hvortil personoplysningerne behandles på vegne af den dataansvarlige

Er at gøre det muligt for Databehandler at opfylde sine forpligtelser i henhold til Aftalen. Databehandleren kan behandle alle kategorier af personoplysninger anført ovenfor med det formål at forbedre Tjenesten. Ydermere skal Databehandleren, som påkrævet ved lov, kende sine kunder for at sikre, at Tjenesten ikke utilsigtet understøtter ulovlige aktiviteter og for at bremse svindel og andet misbrug af Tjenesten.

Behandlingens varighed

Varigheden af behandlingen er begrænset til det tidsrum, der er nødvendigt for at levere Tjenesten, medmindre andet er angivet i Aftalen, i Gældende Lovgivning eller i Bilag V til denne DPA.

Hyppighed af overførsel (f.eks. om data overføres på engangsbasis eller kontinuerligt)

Kontinuerlig basis

Ved behandling af (under)databehandlere angives også behandlingens genstand, art og varighed.

Se venligst bilag IV

Databehandler er berettiget til at engagere underdatabehandlere inden for EU/EØS såvel som uden for EU/EØS, forudsat at bestemmelserne i Aftalen og denne DPA overholdes.

BILAG III

TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER, HERUNDER TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF DATASIKKERHEDEN

Databehandleren skal implementere tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau under hensyntagen til behandlingens art, omfang, kontekst og formål samt risiciene for fysiske personers rettigheder og frihedsrettigheder. De tekniske og organisatoriske foranstaltninger er beskrevet nedenfor i dette bilag.

1. FORANSTALTNINGER TIL PSEUDONYMERING OG KRYPTERING AF PERSONOPLYSNINGER

a) Tekniske foranstaltninger til overførsel inden for EU/EØS eller til et land med en EU-beslutning om tilstrækkelighed

Databehandleren skal have en implementeret politik for brugen af kryptering og krypteringskontrol, beskyttelse og styring af krypteringsnøgler gennem hele livscyklussen og tilgængeligheden af krypteret information (som en del af beredskabsplanlægningen). Databehandleren skal anvende krypteringsteknik for at sikre informationers integritet og hemmeligholdelse (f.eks. for at beskytte information under dataudveksling og data i hvile). Se også afsnit 6, Foranstaltninger til beskyttelse af data under transmission.

b) Supplerende foranstaltninger ved overførsel af personoplysninger til tredjeland

Ud over kravene under 1 a) ovenfor, er dette afsnit gældende i tilfælde af overførsel af personoplysninger til et tredjeland (land uden for EU).

Al data, der omfatter persondatadata, skal være krypteret eller pseudonymiseret før overførsel for at forhindre uautoriseret adgang. Nøgler til dekryptering og/eller til oversættelse af pseudonymiserede personoplysninger til det klare skal opbevares af den dataansvarlige eller en betroet part inden for EU/EØS. Krypteringen og/eller pseudonymiseringen skal implementeres på en sådan måde, at den opfylder "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." i den til enhver tid gældende form der er vedtaget af Det Europæiske Databeskyttelsesråd. Dette er for at sikre, at krypteringsalgoritmen og dens parametre er implementeret for at give robust beskyttelse mod krypteringsanalyse udført af de offentlige myndigheder i modtagerlandet under hensyntagen til:

1. De ressourcer og tekniske muligheder (f.eks. computerkraft til "brute-force"angreb) til rådighed for dem
2. Styrken af krypteringen og nøglelængden tager højde for den specifikke tidsperiode, hvor fortroligheden af de krypterede personoplysninger skal bevares.
3. At krypteringsalgoritmen er implementeret korrekt og af korrekt vedligeholdt software uden kendte sårbarheder
4. Nøglerne og/eller pseudonymiseringsdata administreres pålideligt efter bedste praksis for at forhindre offentliggørelse eller uautoriseret adgang.
5. Vurdering af styrken af krypteringsalgoritmer, deres robusthed over for kryptoanalyse over tid.
6. Ved brug af pseudonymisering skal personoplysningerne behandles på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret, eller bruges til at udskille den registrerede i en større gruppe uden brug af yderligere oplysninger.
7. Det er konstateret ved en grundig analyse af de pågældende data – under hensyntagen til enhver information, som modtagerlandets offentlige myndigheder må forventes at besidde og anvende – at de pseudonymiserede personoplysninger ikke kan henføres til en identificeret eller identificerbar fysisk person, selv hvis der krydshenvises til sådanne oplysninger.

Databehandleren skal straks foretage de nødvendige opdateringer til den service, der er nødvendig for fortsat at være i overensstemmelse med ovenstående krav.

2. FORANSTALTNINGER TIL SIKRING AF LØBENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG -TJENESTER

Databehandleren skal behandle personoplysninger på en måde, der sikrer passende sikkerhed af personoplysningerne, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, ødelæggelse eller beskadigelse, ved brug af passende tekniske eller organisatoriske foranstaltninger. Databehandleren skal have en dokumenteret og implementeret ramme for informationssikkerhedskontrol for at sikre beskyttelse af information og IT-tjenester.

Sikkerhedskontrollen skal sikre beskyttelse af oplysningernes fortrolighed, integritet og tilgængelighed under transit, i brug og i hvile i hele dens livscyklus, og herunder følgende principper:

a) behandle informationssikkerhed som en integreret del af det overordnede systemdesign og integrere sikkerhedskontrol på forskellige it-serviceniveauer (f.eks. applikations-, computer- og netværksniveau).
b) implementere princippet om "defence in depth" eller tilsvarende, hvor der findes flere beskyttelseslag (f.eks. authentication, segmentation, hardening, authorization, malware protection, logging) for at undgå afhængighed af én type eller metode til sikkerhedskontrol.
c) når et system eller en komponent skal interagere med andre systemer og komponenter, skal det antages, at disse er usikre.
d) implementere princippet om færrest privilegier (least privilege principle) (f.eks. gives kun de lavest mulige privilegier til en bruger eller en proces, når man får adgang til systemet).
e) designe og implementere en grundlæggende funktionalitet til revisionsspor.

Databehandleren skal også løbende overvåge effektiviteten af sikkerhedskontrollen og afhjælpe eventuelle fundne mangler omgående.

3. FORANSTALTNINGER TIL SIKRING AF EVNEN TIL AT GENOPRETTE TILGÆNGELIGHEDEN AF OG ADGANGEN TIL PERSONOPLYSNINGER RETTIDIGT I TILFÆLDE AF EN FYSISK ELLER TEKNISK HÆNDELSE

Databehandleren skal have;

- Dokumenterede og implementerede procedurer for håndtering af informationssikkerhedshændelser der sikre hurtig, effektiv og struktureret reaktion på informationssikkerhedshændelser.
- En nødberedskabsproces til håndtering af alvorlige sikkerhedshændelser
- Planer for fortsættelse af driften og genetablering efter en katastrofe, eller tilsvarende for at opretholde acceptable serviceniveauer i tilfælde af problemer, der kan forstyrre tilgængeligheden af informationen eller IT-tjenesterne. Databehandleren skal regelmæssigt teste planerne og evaluere testresultaterne med henblik på løbende forbedring.
- Dokumenterede og implementerede backup-procedurer for at sikre, at informationen og IT-services sikkerhedskopieres og gendannes inden for fastsatte tidsrammer. Proceduren skal tage forskellige risici i betragtning (f.eks. hardware fejl, ransomware). Sikkerhedskopier skal beskyttes.
- Sikkerhedskopier i overensstemmelse med det besluttede "recovery point objective" og "recovery time objective".

4. PROCESSER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER FOR AT GARANTERE BEHANDLINGSSIKKERHEDEN

Databehandleren skal have en dokumenteret og implementeret risikostyringsproces og et sikringsprogram til at overvåge kontroleffektiviteten, identificere og håndtere udestående informationssikkerhedsrelaterede risici for at sikre fortroligheden, integriteten og tilgængeligheden af databehandlerens oplysninger.

Databehandleren skal udføre informationssikkerhedsopfølgningsaktiviteter (f.eks. målinger, anmeldelser, vurderinger og test) for at sikre, at informationssikkerhedskontroller er effektive og ikke omgås, samt, at afvigelser og risici identificeres (f.eks. GAP-analyse i forhold til informationssikkerhedspolitik og -procedurer, compliancegennemgange, IT-serviceinformationssikkerhedsrisikogennemgang, penetrationstest, interne og eksterne revisioner af IT-tjenesterne). Databehandleren skal evaluere resultaterne af informationssikkerhedsopfølgningen samt opdatere deres sikkerhedsprocedurer og implementerede kontroller uden unødig forsinkelse.

Det er som udgangspunkt ikke tilladt, at bruge den dataansvarliges personlige data til testaktiviteter, medmindre den er udtrykkeligt godkendt af den dataansvarlige.

5. FORANSTALTNINGER VEDRØRENDE BRUGERIDENTIFIKATION OG -GODKENDELSE

Databehandleren skal have dokumenterede og implementerede procedurer for adgangsstyring. Sådanne procedurer bør overvåges og revideres regelmæssigt.

Procedurerne skal omfatte følgende:

a) Brugeransvar: Brugere skal have og bruge unikke bruger-id'er for at sikre, at brugere kan identificeres for de handlinger, der udføres i IT-systemer. Databehandleren skal derfor ikke anvende delte konti i IT-tjenester.
b) Adgangsrettigheder: skal gives på et "need-to-know" og "least privilege" basis og skal tildeles, ændres eller

trækkes tilbage rettidigt.
c) Autorisation: tildelte adgangsrettigheder skal være underlagt dokumenterede autorisationer.
e) Opdeling af opgaver: modstridende pligter og ansvarsområder er adskilt for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug.
f) Godkendelse: godkendelsesmetoder skal svare til følsomheden af persondata og IT-tjenester.
g) Tildeling af adgangsrettigheder: adgangsrettigheder skal revideres med jævne mellemrum (mindst hver 6. måned for privilegeret adgang) for at sikre, at brugere ikke har unødvendige rettigheder, og at adgangsrettigheder trækkes tilbage, når de ikke længere er nødvendige.
h) Logning af brugeraktiviteter i IT-tjenester: brugernes aktiviteter skal logges og overvåges. Privilegeret adgang skal være underlagt et højt niveau af logging og overvågning.
i) Privilegerede adgangsrettigheder: øget kontrol over privilegeret adgang skal anvendes, f.eks. ved en streng autorisationsproces, minimere rettigheder, anvende multi-faktor autentificering, granulær logning, overvågning af konti, sikre adskillelse af opgaver.

6. FORANSTALTNINGER TIL BESKYTTELSE AF DATA UNDER OVERFØRSEL

Al personlig data skal være krypteret under overførsel. Databehandleren skal have en sikkerhedskontrol, der kan beskytte mod uautoriseret trafikaflytning eller interferens. Trådløs netværksforbindelse skal være krypteret i overensstemmelse med bedste praksis.

Databehandleren skal have dokumenterede og implementerede procedurer for, kun at give virksomhedens netværksadgang til autoriserede enheder. Databehandleren bør vurdere, om slutpunkter (f.eks. servere, arbejdsstationer, mobile enheder) opfylder de sikkerhedsstandarder, som er defineret af dem, før de får adgang til virksomhedens netværk.

De parter, der er involveret i kommunikationen, er enige om en troværdig "public-key certification authority" eller infrastruktur for at sikre godkendelse af både afsendere og modtagere der er involveret i kommunikation. Hvis transportkryptering ikke i sig selv giver passende sikkerhed på grund af erfaring med sårbarheder i infrastrukturen eller den anvendte software, krypteres personlige data også end-to-end på applikationslaget.

Krypteringen af personoplysninger i transit skal implementeres på en sådan måde, at den opfylder "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data." vedtaget af Det Europæiske Databeskyttelsesråd til enhver tid.

7. FORANSTALTNINGER TIL BESKYTTELSE AF DATA UNDER LAGRING

Ud over de kontroller der er beskrevet i dette dokument, der gælder for information i hvile, inklusive, men ikke begrænset til, kryptering, autentificering/autorisation og revisionsspor, skal Databehandleren have dokumenterede og implementerede sikkerhedskopieringsprocedurer der sikre, at oplysningerne i IT-systemer sikkerhedskopieres og kan genskabes inden for bestemte tidsrammer. Proceduren skal tage forskellige risici i betragtning (f.eks. hardware fejl, ransomware). Sikkerhedskopier skal beskyttes. Sikkerhedskopier skal tages og testes regelmæssigt i overensstemmelse med det besluttede "recovery point objective" og "recovery time objective".

Hvis personoplysninger overføres til et tredjeland (land uden for EU) til opbevaring, skal de krypteres inden overførsel i henhold til afsnit 1, Foranstaltninger til pseudonymisering og kryptering af personoplysninger.

8. FORANSTALTNINGER TIL SIKRING AF FYSISK SIKKERHED PÅ STEDER, HVOR PERSONOPLYSNINGER BEHANDLES

Databehandleren skal løbende identificere fysiske og miljømæssige trusler (f.eks. naturkatastrofer, ondsindede angreb, ulykker) og implementere passende kontroller for at afbøde disse trusler. Fysisk adgang til faciliteter og it-udstyr, hvor dataansvarliges personoplysninger behandles, skal være begrænset til autoriserede medarbejdere. Til cloudbaseret hosting er processoren forpligtet til at benytte etablerede og velkendte leverandører med datacentre inden for EU.

Databehandleren skal have en dokumenteret og implementeret ramme for informationssikkerhedskontroller for at sikre beskyttelsen af information og it-tjenester (f.eks. 2-factor godkendelse, indbrudssikring, hegn). Al adgang til lokaler skal registreres og logges. Datacentre kræver en streng fysisk adgangskontrol og vidtrækkende sikkerhedsanordninger (f.eks. vagt, fugtkontrol, brandalarmer, temperaturkontrol og nødstrømanlæg).

9. FORANSTALTNINGER TIL SIKRING AF LOGNING AF BEGIVENHEDER

Databehandleren skal som minimum have et system til logning af hændelser.

10. FORANSTALTNINGER TIL SIKRING AF SYSTEMKONFIGURATION, HERUNDER STANDARDKONFIGURATION

Databehandleren skal have dokumenterede og implementerede en grundlæggende sikkerhedskonfigurationfor alle komponenter (f.eks. operativsystem, databaser, netværksenheder). Databehandleren skal løbende kontrollere IT-systemers tekniske overensstemmelse i forhold til en defineret minimumsikkerhed(f.eks. "hardening configuration"). Identificerede afvigelser skal vurderes og afhjælpes med passende foranstaltninger for at imødegå den mulige risiko.

11. FORANSTALTNINGER TIL INTERN FORVALTNING OG FORVALTNING AF IT OG IT-SIKKERHED

Databehandleren skal have dokumenterede og implementerede roller og stå til regnskab for informationssikkerhed, herunder være ansvarligfor og have ansvar for informationssikkerhed på tværs af organisationen. Databehandleren skal have en individuel rolle udpeget med et overordnet ansvar for informationssikkerhedsstyringen i organisationen (f.eks. CISO).

12. FORANSTALTNINGER TIL CERTIFICERING/SIKRING AF PROCESSER OG PRODUKTER

Databehandleren skal have implementeret et informationssikkerhedsstyringssystem (ISMS) for at sikre, at det informationssikkerhedsarbejde, som databehandleren udfører, er struktureret, tilstrækkeligt og underlagt ledelsesgennemgang. ISMS'et skal overholde fælles informationssikkerhedsstandarder (f.eks. ISO/IEC 27001 eller et rimeligt alternativ og omfatte en informationssikkerhedsramme (f.eks. politik og procedurer), der er implementeret på tværs af Databehandlerens organisation, herunder tjenester leveret til den dataansvarlige. Hvis der er eventuelle specifikke krav til certificering/sikkerhed fastsat af gældende lov eller regulering eller som specificeret af den registeransvarlige andetsteds, så skal disse krav være opfyldt.

13. FORANSTALTNINGER TIL SIKRING AF DATAMINIMERING

Databehandleren skal også sørge for at behandle og opbevare personoplysningerne i overensstemmelse med eventuelle skriftlige instruktioner fra dataansvarlig, dokumenteret skriftligt i DPA (Databehandleraftale) mellem databehandler og dataansvarlig.

14. FORANSTALTNINGER TIL SIKRING AF DATAKVALITET

Den dataansvarlige skal sikre, at der er dokumenterede processer og rutiner for at sikre, at persondata er korrekte og ajourførte.

15. FORANSTALTNINGER TIL SIKRING AF BEGRÆNSET DATALAGRING

Databehandleren skal have procedurer for håndtering af dataopbevaring og sletning i overensstemmelse med anvisninger fra den dataansvarlige.

16. FORANSTALTNINGER TIL MULIGGØRELSE AF DATAPORTABILITET OG SIKRING AF SLETNING

Databehandleren skal kunne støtte den dataansvarlige med at opfylde sine forpligtelser om dataportabilitet som beskrevet i GDPR.

Databehandleren skal have dokumenterede og implementerede procedurer der sikre, at alle Databehandlerens lagringsmedieenheder er sikkert slettet eller fysisk destrueret ved at bruge almindeligt accepterede metoder (f.eks. NIST SP 800-88 retningslinjer for medierensning) til sikker fjernelse af information.

……

Ver. 2023-10-25

BILAG IV

LISTE OVER UNDERDATABEHANDLERE

Den dataansvarlige har givet tilladelse til, at følgende underdatabehandlere anvendes. Tilføjelser og/eller ændringer til denne liste er reguleret i DPA inklusive bilag 1, punkt 7.7 (a):

Navn: Alle underdatabehandlere, der bruges af Databehandlere, er angivet i matrixen nedenfor

Adresse: Se venligst matrixen nedenfor

Kontaktpersonens navn, stilling og kontaktoplysninger: Kan leveres på forespørgsel

Beskrivelse af behandlingen (herunder en klar ansvarsfordeling, hvis flere underdatabehandlere er godkendt): Se venligst matrixen nedenfor

Underdatabehandlerens navn og adresse	**Beskrivelse af behandlingen**	**Kategorier af registrerede**	**Kategorier af personlige data**	**Opbevaringsperiode for personlige data**	**Behandlingssted**	**Hyppighed af overførsel af personlige data**
Postnord Strålfors AB, Terminalvägen 24, 171 73 Solna, Sverige	Udskrivning af fakturaer*, krav og breve ***Gælder kun for "Fakturaservice"**	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	90 dage	Sverige	Dagligt, når fakturaer, krav og breve udskrives
Edi solutions AB, Box 9169, 400 94 Göteborg, Sverige (Ikke gyldig for Reskontroservice med finansiering PxR)	Integration og omstrukturering af datafiler sendt af Dataansvarlig.	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Indgående/udgående filer/API, database, backups: 6 måneder E-mail med opsætningsinstruktioner (inklusive PayEx-kontaktoplysninger): slettes umiddelbart efter opsætningen er udført. E-mail fra PayEx-kunder: Microsoft 365 GDPR-standard	Sverige, Cloud-servere er placeret inden for EU (Azure)	Dagligt, når integration bruges af klienten til fakturering eller tilbagerapportering til klientens ERP.

Ver. 2023-10-25

21 Grams, Lumaparksvägen 9, 12125 Stockholm, Sverige	Distribution af e-fakturaer B2C* (netbank) og B2B (EDI), digital distribution af krav og breve ***Gælder kun for "Fakturaservice"**	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	90 dage	Sverige, Norge, Finland, Danmark, afhængig af distributionsdestination	Dagligt, når fakturaer, krav og breve sendes
I tilfælde, hvor den Dataansvarlige integrerer til PayEx gennem brug af Partner, vil en sådan Partner blive betragtet som en underdatabehandler til Databehandleren	Se Bilag V p. 5. Partner vil modtage faktura-, finans- og/eller betalingsoplysninger fra Databehandleren.	Oplysninger anført i Bilag II til denne DPA.	Oplysninger anført i Bilag II til denne DPA.	Som instrueret af Dataansvarlig til Partner og/eller PayEx.	Som aftalt mellem Partner og Dataansvarlig.	Daglig
Asteria AB Sveavägen 45, 1 tr 111 34 Stockholm, Sverige	Integration og omstrukturering af datafiler sendt af Dataansvarlig.	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Indgående/udgående filer/API, database, backups: 6 måneder E-mail med opsætningsinstruktioner (inklusive PayEx-kontaktoplysninger): slettes umiddelbart efter opsætningen er udført. E-mail fra PayEx-kunder: Microsoft 365 GDPR-standard	Sverige, Cloud-servere er placeret inden for EU (Azure)	Dagligt, når integration bruges af klienten til fakturering eller tilbagerapportering til klientens ERP.
SpeedLedger AB Fabrikstorget 1 412 50 Göteborg. Sverige (Ikke gyldig for Reskontroservice med finansiering PxR eller Fakturaservice PxR)	Integration og omstrukturering af datafiler sendt af Dataansvarlig.	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Indgående/udgående filer/API, database, backups: 6 måneder E-mail med opsætningsinstruktioner (inklusive PayEx-kontaktoplysninger): slettes umiddelbart efter opsætningen er udført. E-mail fra PayEx-kunder: Microsoft 365 GDPR-standard	Sverige, Cloud-servere er placeret inden for EU (Azure)	Dagligt, når integration bruges af klienten til fakturering eller tilbagerapportering til klientens ERP.

Ver. 2023-10-25

Apix Messaging Oy* (Gælder kun for; *Puitesopimus Reskontrapalvelu, Framework Agreement Ledger Service Finland for Customers with Invoice Discounting through Financing Partner*)	Konvertering af fakturadataformater	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Indgående fakturaer, database backup: 7 år	Finland, Cloud-servere er placeret inden for EU (Azure)	Dagligt, når integration bruges af klienten til fakturering
LinkMobility	Opbevaring og distribution af SMS/besked	Dataansvarligs kunder	Mobilnummer og beskeder	Tre måneder	EU/EEA	Kontinuerlig basis
Mastercard Payment Services (*Gælder kun for; Fakturaservice Norge*)	Opbevaring og fakturahotel	Dataansvarligs kunder	Oplysninger anført i Bilag II til denne DPA.	Mastercard Payment Services GDPR-standard	EU/EEA	Kontinuerlig basis
Microsoft Azure Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Irland (*Bemærk venligst, at Databehandlers brug af Underdatabehandleren Microsoft Azure påbegyndes i trin, og at engagementet forventes at være i fuld brug ved udgangen af 4. kvartal 2024, og at startdatoen for migrering til Microsoft Azure er sat til at blive initieret i løbet af 1.-3. kvartal 2024*.)	Microsoft Azure er en cloud computing-platform. Det leverer en bred vifte af cloud-tjenester, herunder databehandling, analyse, lagring og netværk. Azure fungerer som lagringssted, og persondata tilgås, udtrækkes og på anden måde behandles af Databehandler for at levere den Tjeneste der er beskrevet i Aftalen mellem den Dataansvarlige og Databehandler.	Oplysninger anført i Bilag II til denne DPA.	Oplysninger anført i Bilag II til denne DPA.	Databehandler har mulighed for at få adgang til, udtrække og slette lagrede data. Principper for opbevaring og sletning af data følger de skriftlige instruktioner, der er dokumenteret i DPA mellem Databehandler og Dataansvarlig, og som sådan har Underdatabehandleren ingen indflydelse på adgang, udtræk og sletning af lagrede data.	Microsoft skal gemme og behandle kundedata inden for Den Europæiske Union med primær lagerplacering i Microsoft Clod Data Centers i Gävle & Sandviken, Sverige og sekundær (backup) lagerplacering i Microsoft Clod Data Centers i Staffanstorp, Sverige	Kontinuerlig basis

Ver. 2023-10-25

Efecte AB Drottninggatan 33, 111 51 Stockholm Sverige	Sagsbehandling	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Sager/tickets gemmes i 13 måneder	Finland	Løbende, når slutkunder kontakter Databehandleres kundeservice med fakturaspørgsmål.
Telia Company Stjärntorget 1, 169 79 Solna Sverige	Kundeservice via telefon og chat med Telia ACE-softwaren	Dataansvarligs kunder	Godkendelsesoplysninger, kontaktoplysninger, transaktionsoplysninger	Telefonopkald og chatlogs gemmes i 90 dage.	Sverige	Løbende, når slutkunder kontakter Databehandleres kundeservice med fakturaspørgsmål.

Ud over listen over underdatabehandlere beskrevet i dette BILAG IV, er Databehandleren berettiget til at behandle personoplysninger inden for PayEx-koncernen, når en sådan behandling er nødvendig for at kunne levere tjenesten på den måde, der er defineret i Aftalen. Når en virksomhed i PayEx-koncernen behandler personoplysninger på vegne af Databehandler, forpligter hver virksomhed i PayEx-koncernen sig til at behandle personoplysninger i overensstemmelse med gældende lov, Aftalen og Kundens instruktioner angivet i Bilag 1 og underbilag till Bilag 1 til DPA mellem Dataansvarlig og Databehandler.

Ver. 2023-10-25

BILAG V

DATAANSVARLIGES INSTRUKTION TIL DATABEHANDLER

1. *Retlige grundlag for behandling*

Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af data i overensstemmelse med Aftalen og denne DPA er lovlig i henhold til Gældende Lovgivning, uanset om de registrerede har givet samtykke til behandlingen, eller hvis der er en anden retlige grund for behandlingen, og at de personoplysninger, der er omfattet af denne DPA, og at Databehandlerens behandling på vegne af den Dataansvarlige er blevet indsamlet til specifikke, eksplicitte og begrundede formål og i øvrigt er i overensstemmelse med Gældende Lov, og at disse formål er angivet fuldt ud og korrekt i Bilag II. Den dataansvarlige vil straks give besked til Databehandleren, hvis behandlingens formål af de personoplysninger, der behandles i henhold til Aftalen, ændres.

Den Dataansvarlige er endvidere ansvarlig for at sikre, at Databehandleren ikke behandler andre kategorier af personoplysninger end dem, der er anført i Bilag II på vegne af den Dataansvarlige.

2. *Opbevaringstid og lagring af personoplysninger*

Databehandleren opbevarer kun personoplysninger, så længe det er nødvendigt, i sidste ende reguleret af Aftalen som defineret i DPA p. 3.2. Den Dataansvarlige har instrueret Databehandleren om at levere Tjenesten på den måde, der er defineret i Aftalen. Når den Dataansvarlige og Databehandleren ikke længere har en gyldig Aftale, vil Databehandleren kun opbevare personoplysninger, hvis det er påkrævet ved lov eller i andre tilfælde under den definerede periode for Aftalen, kontraktperioden, men ikke længere end til det punkt, hvor databehandleren har ophørt med administrationen og afsluttet alle sager, der er i hovedbogen, herunder Krav, der er under Overvågning.

Specifikation i forhold til filer, der er kommunikeret til Databehandler via fil, CUSIN eller API: Den Dataansvarlige har indvilliget i at overholde Databehandlers regler og instruktioner gældende på tidspunktet for afsendelse og modtagelse af filer. Hvis der er udarbejdet en teknisk beskrivelse og vedlagt Aftalen, skal denne følges. Databehandleren vil opbevare data modtaget fra den Dataansvarlige via fil eller ved anden elektronisk kommunikation i en periode på 13 måneder, eksemplificeret nedenfor, såsom:

Rapport	**Opbevaringstid**
Reskontrorapport	13 måneder fra oprettelse
Oprettede fakturaer	13 måneder fra oprettelse
Faktura	13 måneder fra oprettelse
Overskud, detaljeret	13 måneder fra oprettelse
Inkassobetalinger, detaljeret	13 måneder fra oprettelse
Betalinger, detaljeret	13 måneder fra oprettelse
Nedskrivningsrapport, detaljeret	13 måneder fra oprettelse
Nedskrivningsrapport	13 måneder fra oprettelse
Aldersanalyse	13 måneder fra oprettelse

3. *Distribution*

Databehandleren vil distribuere fakturaer, krav og anden kommunikation beskrevet i Aftalen i henhold til instruktioner modtaget fra Dataansvarlig via API, fil eller anden elektronisk kommunikation, og distribuere faktura som specificeret i Tjenestebeskrivelse i Aftalen, når det er relevant. Den Dataansvarlige garanterer, som beskrevet i afsnit 1, Bilag V til denne DPA, den retlige grundlag for behandlingen, og at Databehandleren kan distribuere fakturaer, krav og anden kommunikation til registrerede modtaget fra Dataansvarlig.

4. *Fakturaportal (Gælder kun for "Fakturaservice" baseret på reskontrosystemet PxR)*

Databehandler vil stille fakturaoplysninger vedrørende den Dataansvarliges kunder til rådighed i en Fakturaportal. Fakturaportalen er tilgængelig for slutkunder ved modtagelse af faktura pr. e-mail, eller når et link eller integration til Fakturaportalen etableres/anvendes af Dataansvarlig. I Fakturaportalen kan slutkunden få adgang til information om deres fakturaer og følge status på en faktura (betalt/ubetalt osv.). Slutkunden vil også have mulighed for at betale modtagne fakturaer ved brug af tilgængelige betalingsmetoder i Fakturaportalen. Dataansvarlig instruerer Databehandler i at stille fakturaoplysninger vedrørende Dataansvarliges kunder til rådighed i en Fakturaportal. Fakturainformation betyder producerede slutkundefakturaer, rykkere og hvor det er relevant inkassoskrivelser (bemærk: udsendelsen af inkassokrav vil følge hierarkiet beskrevet i Tjenestebeskrivelse af Aftalen, som beskrevet i afsnit 3 i Bilag V. Fakturainformation og betalingsmuligheder for sådanne udsendte krav vil dog være tilgængelige via Fakturaportalen). Oplysningerne i Fakturaportalen vil blive gjort tilgængelige for slutkunden i henhold til Databehandlerens instruktion til Databehandleren, dvs. når Databehandleren sender oplysninger ved brug af e-mailadresser (indsamlet og overført til Databehandleren af Dataansvarlig via fil, CUSIN eller API eller som ellers aftalt mellem Parterne) at kommunikere fakturaer og andre meddelelser/dokumenter/opgørelser/sammenstillinger mv. Oplysningerne i Fakturaportalen vil generelt blive gjort tilgængelige via link (f.eks. i e-mails) eller omdirigere og derved overføre slutkunden uden der er behov for identitetsbekræftelse/stærk autentificering, undtagen i tilfælde hvor slutkunden skal bekræfte sin identitet ved brug af tilgængelige betalingsmetoder i fakturaportalen, eller ved adgang til oplysninger om et inkassokrav. Den Dataansvarlige pålægger endvidere Databehandleren at stille oplysninger til rådighed for den Dataansvarlige i form af rapporter eller på anden måde som beskrevet i Aftalen vedrørende den Dataansvarliges kunder, der vælger at betale ved brug af tilgængelige betalingsmetoder i Fakturaportalen.

5. *Partner*

I scenarier, hvor Dataansvarlig har en integreret løsning til Databehandler, hvilket betyder, at Dataansvarlig har integreret til Databehandler gennem brug af en Partner (dvs. en separat juridisk enhed, der bl.a. leverer integrationstjenester, hvorved Dataansvarliges ERP/e-handelssystem eller lignende integreres til Databehandler på vegne af den Dataansvarlige), instruerer den Dataansvarlige hermed Databehandleren i at modtage sådanne personoplysninger, som leveres gennem Partner til Databehandleren på vegne af den Dataansvarlige, som om de var direkte modtaget fra Dataansvarlig. Dataansvarlig pålægger endvidere Databehandler at sende faktura-, reskontro- og betalingsrapporter/oplysninger til Partner. Personoplysninger, der overføres til Partner, vil indeholde oplysninger, der er anført i Bilag II til denne DPA. For overskuelighedens skyld betragtes Partner kun som underdatabehandler i forhold til overførsel af personoplysninger, som instrueret af Dataansvarlig til Databehandler, i form af faktura-, reskontro- og betalingsrapporter/oplysninger.

I scenarier, hvor Dataansvarlig har en partnerløsning, hvor Dataansvarlig har en separat aftale med en Finansieringspartner (for eksempel en bank, der leverer en finansieringsløsning til Dataansvarlig) og en separat aftale med Databehandler (vedrørende *Reskontroservice for kunder med fakturafinansiering med administration*), og hvor den Dataansvarliges aftale med Finansieringspartneren kræver, at visse faktura-/reskontrodata deles af Databehandleren med en sådan Finansieringspartner, instruerer Dataansvarlig herved Databehandleren om at modtage personoplysninger, som er givet gennem Finansieringspartner til Databehandleren på vegne af den Dataansvarlige, som hvis den er modtaget direkte fra Dataansvarlig. Dataansvarlig instruerer endvidere Databehandler i at sende faktura-, reskontro- og betalingsrapporter/oplysninger og kreditrelaterede oplysninger til Partner. Personoplysninger, der overføres til Partner, vil indeholde oplysninger, der er anført i Bilag II til denne DPA. Dataansvarliges instruktioner er yderligere detaljeret i Tjenesteaftalen (afsnittet Behandling af personoplysninger) mellem Dataansvarlig og Databehandler.

6. *Tredjeparts tjenesteudbydere*

I et scenarie, hvor den Dataansvarlig bruger en tredjepart til at sende/kommunikere oplysninger forbundet med Tjenesten, er den Dataansvarlige ansvarlig for en sådan tredjepart som for sig selv. Hvis en tredjepart udpeges af den Dataansvarlige til at kommunikere fakturaoplysninger, herunder persondata, via fil, CUSIN eller API eller som på anden måde er aftalt, er den Dataansvarlige ansvarlig for sådanne fakturaoplysninger, herunder persondata, samt at data er indsamlet iht. Gældende Lov. Hvis den Dataansvarliges aftale med en tredjepart kræver, at Databehandleren deler visse faktura-/reskontrodata med en sådan tredjepart, instruerer den Dataansvarlige herved Databehandleren i at modtage personoplysninger, som er leveret gennem tredjeparten til den Dataansvarlige på vegne af den Dataansvarlige, som var de var modtaget direkte fra Dataansvarlig. Dataansvarlig instruerer endvidere Databehandler i at sende faktura-, finans- og betalingsrapporter/oplysninger samt kreditrelaterede oplysninger til en sådan tredjepart. Personoplysninger, der overføres til tredjepart, vil omfatte oplysninger anført i Bilag II til denne DPA. Den Dataansvarliges instruktioner er i relevante tilfælde yderligere specificeret i Serviceaftalen (afsnit vedrørende persondata) mellem den Dataansvarlige og Databehandleren.