Ver. 2023-10-25

Underbilagor till Bilaga 1 Personuppgiftsbiträdesavtal
Bilagorna är tillämpliga för Bilaga 1

BILAGA I

FÖRTECKNING ÖVER PARTER

Personuppgiftsansvariga: [*Identitet och kontaktuppgifter för den eller de berörda personuppgiftsansvariga, samt, i tillämpliga fall, för den personuppgiftsansvariges dataskyddsombud]*

Namn: Det företag som anges som Kund på framsidan av Ramavtalet mellan PayEx och Kund gällande Fakturaservice och/eller Reskontraservice som PayEx tillhandahåller Kunden

Adress: Ref. till framsidan av Ramavtalet mellan PayEx och Kund.

Kontaktpersonens namn, befattning och kontaktuppgifter: Ref. till framsidan av Ramavtalet mellan PayEx och Kund.

Namn och kontaktuppgifter för dataskyddsombudet [*om tillämpligt*]: Information ska tillhandahållas av Kunden på begäran från PayEx.

Personuppgiftsbiträden: [*Identitet och kontaktuppgifter för den eller de berörda personuppgiftsbiträdena samt, i tillämpliga fall, för personuppgiftsbiträdets dataskyddsombud]*

Namn: PayEx Sverige AB, org. nr. 556735-5671

Adress: S:t Hansplan 1, 621 88 Visby

Kontaktpersonens namn, befattning och kontaktuppgifter: Ref. till framsidan av Ramavtalet mellan PayEx och Kund.

Kontaktuppgifter till dataskyddsombud:

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

BILAGA II

BESKRIVNING AV BEHANDLINGEN

Kategorier av registrerade vars personuppgifter behandlas

Personuppgiftsansvarigs anställda, Personuppgiftsansvarigs kunder och mottagare av fakturor, Personuppgiftsansvarigs ägare och ledamöter i styrelse/ledning.

Kategorier av personuppgifter

Autentiseringsinformation (personnummer, bankkontonummer), Kontaktuppgifter (namn, adress, telefonnummer, e-post) Historisk information (köpta varor och/eller tjänster), Transaktionsinformation (köpta varor och tjänster), spårningsinformation (IP-adress, cookies, enhet), samt de ytterligare kategorier av personuppgifter som anges i Bilaga V.

Känsliga uppgifter som behandlas (i tillämpliga fall) och tillämpade begränsningar eller skyddsåtgärder som fullt ut tar hänsyn till uppgifternas art och de risker som är förknippade med dem, t.ex. strikt ändamålsbegränsning, åtkomstbegränsningar (inbegripet åtkomst endast för personal som har gått en specialiserad utbildning), registrering av åtkomst till uppgifterna, begränsningar för vidareöverföring eller ytterligare säkerhetsåtgärder.

Såvida inte annat uttryckligen instrueras av den Personuppgiftsansvarige i detta DPA, skriftligen och godkänt av Personuppgiftsbiträdet, kommer inga speciella kategorier av personuppgifter (*känsliga personuppgifter*) att behandlas. Särskilda kategorier av personuppgifter inkluderar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, eller fackföreningsmedlemskap, och behandling av genetiska uppgifter, biometriska uppgifter i syfte att unikt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexliv eller sexuella läggning.

Behandlingens art och föremål

Föremålet för behandlingen är att tillhandahålla fakturatjänster och tillhörande reskontratjänster enligt vad som närmare anges i Avtalet mellan Personuppgiftsansvarig och Personuppgiftsbiträdet samt vad som närmare beskrivs i Bilaga V. Dessutom behöver Personuppgiftsbiträdet, i enlighet med lag, känna till sina kunder (t.ex. Personuppgiftsansvarig) för att säkerställa att Tjänsten inte oavsiktligt stödjer olaglig verksamhet och för att förhindra bedrägeri och annat missbruk av Tjänsten.

Behandlingens art är att utföra behandling som är nödvändig för det angivna ändamålet, inklusive bland annat inspelning, organisation, strukturering, lagring, anpassning och ändring, hämtning, konsultation, överföring, användning, utlämnande genom överföring, spridning eller på annat sätt tillgängliggörande, anpassning eller kombination, begränsning, radering eller förstörelse.

Ändamål för vilka personuppgifterna behandlas för den personuppgiftsansvariges räkning

Är att göra det möjligt för Personuppgiftsbiträdet att fullgöra sina skyldigheter enligt Avtalet samt vad som närmare beskrivs i Bilaga V. Personuppgiftsbiträdet kan också behandla alla kategorier av personuppgifter som anges ovan i syfte att förbättra Tjänsten. Vidare behöver Personuppgiftsbiträdet, enligt lag, känna sina kunder (t.ex. Personuppgiftsansvarig) för att säkerställa att Tjänsten inte oavsiktligt stödjer olaglig verksamhet och för att förhindra bedrägeri och annat missbruk av Tjänsten.

Behandlingens varaktighet

Behandlingens varaktighet är begränsad till den tidsperiod som krävs för att tillhandahålla Tjänsten och vad som närmare beskrivs i Bilaga V, om inte annat anges i Avtalet eller i Tillämplig Lag.

Överföringsfrekvens (t.ex. om uppgifterna överförs på engångsbasis eller kontinuerligt)

Kontinuerlig

För behandling som utförs av personuppgiftsbiträden (eller underleverantörer), ange även föremålet för behandlingen, behandlingens art och dess varaktighet

Vänligen se Bilaga IV och V.

BILAGA III

TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER, INBEGRIPET TEKNISKA OCH ORGANISATORISKA ÅTGÄRDER FÖR ATT SÄKERSTÄLLA DATASÄKERHETEN

Personuppgiftsbiträdet ska genomföra tekniska och organisatoriska åtgärder för att säkerställa en lämplig säkerhetsnivå, med hänsyn till behandlingens art, omfattning, sammanhang och syfte samt riskerna för fysiska personers rättigheter och friheter. De tekniska och organisatoriska åtgärderna beskrivs nedan i denna Bilaga III.

1. Åtgärder för pseudonymisering och kryptering av personuppgifter

a) Tekniska åtgärder för överföring inom EU/EES eller till ett land med EU-adekvansbeslut
Personuppgiftsbiträdet ska ha en implementerad policy för användning av kryptografi, inklusive användning av kryptografikontroller, skydd och hantering av kryptografiska nycklar under hela livscykeln och tillgängligheten av krypterad information (som en del av beredskapsplaneringen/ contingency planning). Personuppgiftsbiträdet ska tillämpa kryptografiska tekniker för att säkerställa informationens integritet och konfidentialitet (t.ex. för att skydda information under överföring och vila / in transit and at rest). Se även avsnitt 6, Åtgärder för skydd av uppgifter under överföring.

b) Kompletterande åtgärder för överföring till tredje land
Utöver kraven under 1 a) ovan är denna paragraf tillämplig vid överföring av personuppgifter till ett tredje land.

Alla personuppgifter måste krypteras eller pseudonymiseras före överföring för att förhindra obehörig åtkomst. Nycklar för dekryptering och/eller för att översätta pseudonymiserade personuppgifter till klartext ska förvaras av Personuppgiftsansvarig eller en anförtrodd part inom EU/EES. Krypteringen och/eller pseudonymiseringen måste implementeras på ett sådant sätt att den uppfyller "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" antagen av Europeiska dataskyddsstyrelsen när som helst. Detta för att säkerställa att krypteringsalgoritmen och dess parametrering implementeras för att ge ett robust skydd mot kryptoanalys utförd av de offentliga myndigheterna i mottagarlandet med hänsyn till:

1. De resurser och tekniska möjligheter (t.ex. datorkraft för brute-force-attacker) tillgängliga för dem
2. Styrkan på krypteringen och nyckellängden tar hänsyn till den specifika tidsperiod under vilken konfidentialiteten för de krypterade personuppgifterna måste bevaras
3. Att krypteringsalgoritmen implementeras korrekt och av korrekt underhållen programvara utan kända sårbarheter
4. Nycklarna och/eller pseudonymiseringsdata hanteras på ett tillförlitligt sätt enligt bästa praxis för att förhindra avslöjande eller obehörig åtkomst
5. Bedömning av styrkan hos krypteringsalgoritmer, deras robusthet mot kryptoanalys över tid
6. Vid användning av pseudonymisering ska personuppgifterna behandlas på ett sådant sätt att personuppgifterna inte längre kan hänföras till en specifik registrerad, eller användas för att peka ut den registrerade i en större grupp, utan användning av ytterligare information
7. Det konstateras genom en noggrann analys av de aktuella uppgifterna – med beaktande av all information som mottagarlandets offentliga myndigheter kan förväntas besitta och använda – att de pseudonymiserade personuppgifterna inte kan hänföras till en identifierad resp. identifierbar fysisk person även om den korsreferens med sådan information

Personuppgiftsbiträdet ska omedelbart göra nödvändiga uppdateringar av tjänsten som behövs för att fortsätta uppfylla ovanstående krav.

2. Åtgärder för att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna

Personuppgiftsbiträdet ska behandla personuppgifter på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inklusive skydd mot otillåten eller olaglig behandling och mot oavsiktlig förlust, förstörelse eller skada, med hjälp av lämpliga tekniska eller organisatoriska åtgärder. Personuppgiftsbiträdet ska ha ett dokumenterat och implementerat ramverk av informationssäkerhetskontroller för att säkerställa skyddet av information och IT-tjänster. Säkerhetskontrollerna ska säkerställa skyddet av informationens konfidentialitet, integritet och tillgänglighet under transport (in transit), vid användning (in use) och i vila (at rest) under hela dess livscykel och inklusive följande principer:

a) behandla informationssäkerhet som en integrerad del av den övergripande systemdesignen och integrera

säkerhetskontroller på olika IT-tjänstenivåer (t.ex. applikations-, dator- och nätverksnivå).
b) implementera principen om "defence in depth" eller motsvarande, där det finns flera skyddsskikt (t.ex. authentication, segmentation, hardening, authorization, malware protection, logging) för att undvika beroende av en typ eller metod för säkerhetskontroll.
c) när ett system eller en komponent ska interagera med andra system och komponenter ska det antas att dessa är osäkra.
d) implementera "least privilege principle" (t.ex. endast de minsta möjliga privilegierna ges till en användare eller en process vid åtkomst till systemet).
e) utforma och implementera en grundläggande funktionalitet för revisionsspår.

Personuppgiftsbiträdet ska också kontinuerligt övervaka effektiviteten av säkerhetskontrollerna och åtgärda eventuella upptäckta brister omedelbart.

3. Åtgärder för att säkerställa förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident

Personuppgiftsbiträdet ska ha;

- Dokumenterade och implementerade rutiner för att hantera informationssäkerhetsincidenter för att säkerställa ett snabbt, effektivt och strukturerat svar på informationssäkerhetsincidenter.
- En beredskapsprocess för att hantera allvarliga säkerhetsincidenter.
- Business Continuity Plans and Disaster Recovery Plans eller motsvarande för att upprätthålla acceptabla servicenivåer i händelse av problem som kan störa tillgängligheten för informationen eller IT-tjänsterna. Processorn ska regelbundet testa planerna och utvärdera testresultaten för ständig förbättring.
- Dokumenterade och implementerade backupprocedurer för att säkerställa att information och IT-tjänster säkerhetskopieras och återställs inom bestämda tidsramar. Proceduren ska ta hänsyn till olika risker (t.ex. maskinvarufel, ransomware). Säkerhetskopior ska skyddas.
- Backupbilder ska tas och testas regelbundet i enlighet med beslutat mål för återställningspunkt (recovery point objective) och mål för återhämtningstid (recovery time objective).

4. Förfaranden för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärderna för att säkerställa behandlingens säkerhet

Personuppgiftsbiträdet ska ha en dokumenterad och implementerad riskhanteringsprocess och ett försäkransprogram (assurance program) för att övervaka kontrolleffektiviteten, identifiera och hantera utestående informationssäkerhetsrelaterade risker, för att säkerställa konfidentialitet, integritet och tillgänglighet för Personuppgiftsbiträdets information.

Personuppgiftsbiträdet ska utföra informationssäkerhetsuppföljningsaktiviteter (t.ex. mätningar, granskningar, bedömningar och tester) för att säkerställa att informationssäkerhetskontroller är effektiva och inte kringgås och att avvikelser och risker identifieras (t.ex. gap-analys mot informationssäkerhetspolicy och rutiner, granskning av efterlevnad, granskning av risker för IT-tjänstens informationssäkerhet, penetrationstester, interna och externa revisioner av IT-tjänsterna). Personuppgiftsbiträdet ska utvärdera resultaten av informationssäkerhetsuppföljningen och uppdatera sina säkerhetsrutiner och säkerhetskontroller utan onödiga dröjsmål.

Det är som standard inte tillåtet att använda Personuppgiftsansvarigs personuppgifter för testaktiviteter såvida det inte uttryckligen godkänts av den Personuppgiftsansvarig.

5. Åtgärder för identifiering och godkännande av användare

Personuppgiftsbiträdet ska ha dokumenterade och implementerade rutiner för åtkomsthantering (access management). Sådana förfaranden bör övervakas och granskas regelbundet.

Förfarandena ska omfatta följande:

a) Användaransvar: användare ska ha och använda unika användar-id för att säkerställa att användare kan identifieras för de åtgärder som utförs i IT-tjänsterna. Personuppgiftsbiträdet bör därför inte använda delade konton för IT-tjänster.
b) Åtkomsträttigheter: ska beviljas på basis av ”need-to-know” och ”least privilege basis” och ska beviljas, ändras eller dras in i tid.
c) Auktorisation: åtkomsträttigheter ska vara föremål för dokumenterade auktorisationer
e) Uppdelning av arbetsuppgifter: motstridiga uppgifter och ansvarsområden är åtskilda för att minska möjligheter till obehörig eller oavsiktlig modifiering eller missbruk.
f) Autentisering: autentiseringsmetoderna ska överensstämma med personuppgifternas och IT-tjänsternas

känslighet.
g) Återcertifiering av åtkomst: åtkomsträttigheter ska ses över med jämna mellanrum (minst var sjätte månad för privilegierad åtkomst) för att säkerställa att användare inte har överdrivna behörigheter och att åtkomsträttigheter dras tillbaka när de inte längre behövs.
h) Loggning av användaraktiviteter i IT-tjänster: användares aktiviteter ska loggas och övervakas. Privilegerad åtkomst ska vara föremål för striktare utökad loggning och övervakning.
i) Privilegierad åtkomsträtt: starkare kontroller över privilegierad åtkomst ska tillämpas, t.ex. genom en strikt auktoriseringsprocess, minimera behörigheter, tillämpa multifaktorautentisering, granulär loggning, noggrann övervakning av konton och säkerställa åtskillnad av arbetsuppgifter.

6. Åtgärder för skydd av uppgifter under överföring

Alla personuppgifter måste krypteras under överföring. Personuppgiftsbiträdet ska ha säkerhetskontroller som kan skydda mot obehörig trafikavlyssning eller störning. Trådlös nätverksanslutning ska vara krypterad enligt bästa praxis.

Personuppgiftsbiträdet ska ha dokumenterade och implementerade procedurer för att bevilja företagsnätverksåtkomst till endast auktoriserade enheter. Personuppgiftsbiträdet bör utvärdera om slutpunkter (endpoints) (t.ex. servrar, arbetsstationer, mobila enheter) uppfyller säkerhetsstandarderna som definierats av dem innan de beviljas åtkomst till företagets nätverk.

Parterna som är inblandade i kommunikationen kommer överens om en pålitlig certifieringsmyndighet eller infrastruktur med offentlig nyckel för att säkerställa autentisering av både avsändare och mottagare som är involverade i all kommunikation. Om transportkryptering inte ger lämplig säkerhet i sig på grund av erfarenhet av sårbarheter i infrastrukturen eller mjukvaran som används, krypteras även personuppgifter end-to-end på applikationslagret (application layer).

Krypteringen av personuppgifter under överföring (in transit) måste implementeras på ett sådant sätt att den uppfyller " Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" antagen av Europeiska dataskyddsstyrelsen.

7. Åtgärder för skydd av uppgifter under lagring

Utöver alla andra kontroller som beskrivs i detta dokument som gäller information i vila (information at rest), inklusive men inte begränsat till, kryptering, autentisering/auktorisering och revisionsspår, ska Personuppgiftsbiträdet ha dokumenterade och implementerade säkerhetskopieringsprocedurer för att säkerställa att informationen och IT-tjänsterna säkerhetskopieras och återställs inom bestämda tidsramar. Proceduren ska ta hänsyn till olika risker (t.ex. maskinvarufel, ransomware). Säkerhetskopior ska skyddas. Backupbilder ska tas och testas regelbundet i enlighet med beslutat mål för återställningspunkt (recovery point objective) och mål för återhämtningstid (recovery time objective).

Om personuppgifter överförs till ett 3:e land för lagring måste de krypteras innan de överförs enligt avsnitt. Se avsnitt 1, Åtgärder för pseudonymisering och kryptering av personuppgifter.

8. Åtgärder för att säkerställa fysisk säkerhet på platser där personuppgifter behandlas

Personuppgiftsbiträdet ska kontinuerligt identifiera fysiska och miljömässiga hot (t.ex. naturkatastrofer, illvilliga attacker, olyckor) och implementera adekvata kontroller för att mildra dessa hot. Fysisk tillgång till lokaler och IT-utrustning där Personuppgiftsansvarigs personuppgifter behandlas ska begränsas till behöriga anställda. För molnbaserad hosting är Personuppgiftsbiträdet skyldig att använda etablerade och välkända leverantörer med datacenter inom EU.

Personuppgiftsbiträdet ska ha ett dokumenterat och implementerat ramverk av informationssäkerhetskontroller för att säkerställa skyddet av information och IT-tjänster (t.ex. 2-faktors autentisering, intrångssystem, stängsel). Alla tillträden till lokalerna ska registreras och loggas. Datacenter kräver strikt fysisk åtkomstkontroll och ytterligare säkerhetsarrangemang (t.ex. bevakning, fuktkontroll, brandlarm, temperaturkontroll och stödjande elförsörjning).

9. Åtgärder för att säkerställa loggning av händelser
Personuppgiftsbiträdet ska ha åtminstone ett grundläggande system som möjliggör loggning av händelser.

10. Åtgärder för att säkerställa systemkonfiguration, inklusive standardkonfiguration

Personuppgiftsbiträdet ska ha dokumenterade och implementerade säkerhetskonfigurationsbaslinjer (security configuration baselines) för alla komponenter (t.ex. operativsystem, databaser, nätverksenheter). Personuppgiftsbiträdet ska kontinuerligt kontrollera IT-tjänsternas tekniska överensstämmelse mot en definierad säkerhetsbaslinje (t.ex. hardening configuration). Identifierade avvikelser ska bedömas och åtgärdas genom lämpliga

åtgärder för att hantera den förknippade risken.

11. Åtgärder för intern it och styrning och hantering av IT-säkerhet

Personuppgiftsbiträdet ska ha dokumenterade och implementerade roller och ansvar för informationssäkerhet, inklusive ansvar och ansvar för informationssäkerhet i hela organisationen. Personuppgiftsbiträdet ska ha en individuell roll utsedd med ett övergripande ansvar för informationssäkerhetshanteringen inom organisationen (t.ex. CISO).

12. Åtgärder för certifiering/säkring av processer och produkter

Personuppgiftsbiträdet ska ha implementerat ett Information Security Management System (ISMS) för att säkerställa att informationssäkerhetsarbetet som utförs av Personuppgiftsbiträdet är strukturerat, adekvat och föremål för ledningens granskning. ISMS ska följa gemensamma informationssäkerhetsstandarder (t.ex. ISO/IEC 27001 eller annat rimligt alternativ och inkludera ett ramverk för informationssäkerhet (t.ex. policy och förfaranden), som implementeras i hela Personuppgiftsbiträdets organisation, inklusive tjänster som tillhandahålls den Personuppgiftsansvariga. Om det finns eventuella specifika krav på certifiering/försäkran som anges i tillämplig lag eller förordning eller som specificerats av personuppgiftsansvarig på annat håll i.f.h.t. Personuppgiftsbiträdet, bör dessa krav uppfyllas.

13. Åtgärder för att säkerställa uppgiftsminimering

Personuppgiftsbiträdet ska även se till att behandla och lagra personuppgifterna i enlighet med eventuella skriftliga instruktioner från Personuppgiftsansvarig, skriftligt dokumenterade i personuppgiftsbiträdesavtalet mellan Personuppgiftsbiträdet och Personuppgiftsansvarig.

14. Åtgärder för att säkerställa datakvalitet

Den Personuppgiftsansvarige ska säkerställa att det finns dokumenterade processer och rutiner för att säkerställa att personuppgifter är korrekta och aktuella.

15. Åtgärder för att säkerställa begränsad lagring av uppgifter

Personuppgiftsbiträdet ska ha rutiner för att hantera datalagring och radering i enlighet med anvisningar från den Personuppgiftsansvarige.

16. Åtgärder för att möjliggöra dataportabilitet och säkerställa radering

Personuppgiftsbiträdet måste kunna stödja den Personuppgiftsansvarige i att fullgöra sina skyldigheter om dataportabilitet enligt beskrivningen i GDPR.

Personuppgiftsbiträdet ska ha dokumenterade och implementerade procedurer för att säkerställa att alla processorlagringsmedieenheter på ett säkert sätt raderas eller förstörs fysiskt genom att använda allmänt accepterade metoder (t.ex. NIST SP 800-88 guidelines for Media Sanitization) för säker informationsborttagning.

……

Ver. 2023-10-25

BILAGA IV

FÖRTECKNING ÖVER UNDERLEVERANTÖRER

Personuppgiftsbiträdet har fått tillåtelse, av den Personuppgiftsansvarige, att använda följande Underbiträden. Tillägg och/eller ändringar av denna lista regleras i DPA inklusive Bilaga 1 klausul 7.7 (a):

1. Namn: [Alla underleverantörer som används av Personuppgiftsbiträdet listas i nedan matris]

Adress: [Vänligen se matrisen nedan]

Kontaktpersonens namn, befattning och kontaktuppgifter: [Delges av Personuppgiftsbiträdet på skriftlig begäran från Personuppgiftsansvarig]

Beskrivning av behandlingen (inklusive en tydlig ansvarsfördelning om flera underleverantörer har godkänts): [Vänligen se matrisen nedan]

2. ……

Namn och adress Underbiträde	**Beskrivning av Behandlingen**	**Kategorier av registrerade**	**Kategorier av Personuppgifter**	**Retentionstid för Personuppgifter**	**Plats för Behandling (Geografisk)**	**Överföringsfrekvens**
Postnord Strålfors AB, Terminalvägen 24, 171 73 Solna	Utskrift av fakturor*, krav och brev ***Gäller endast för tjänsten "Fakturaservice"**	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	90 dagar	Sverige	Dagligen, när fakturor, krav och brev skapas/printas.
Edi solutions AB, Box 9169, 400 94 Göteborg (*Gäller ej Reskontraservice med belåning PxR*)	Integration och omstrukturering av datafiler skickade av Personuppgiftsansvarig	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Inkommande/utgående filer/API, databas, backuper: 6 månader E-post med installationsinstruktioner /instruktioner om uppsätt (inklusive PayEx-kontaktinformation): raderas omedelbart efter att installationen/uppsät	Sverige, Moln lagring på servers lokaliserade inom EU (Azure)	Dagligen, när integration används av Personuppgiftsansvarig för fakturering eller återrapportering till kunds ERP/affärssystem.

				t är klar. E-post från PayEx-kunder: Microsoft 365 GDPR-standard		
21 Grams, Lumaparksvägen 9, 12125 Stockholm	Distribution av e-fakturor B2C* (nätbank) och B2B (EDI), digital distribution av fakturor, krav och brev ***Gäller endast för tjänsten "Fakturaservice"**	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	90 dagar	Sverige, Norge, Finland, Danmark, beroende på distributionsland.	Dagligen, när fakturor, krav och brev distribueras.
I de fall då Personuppgiftsansvarig integrerar med Personuppgiftsbiträdet genom användning av Partner, kommer sådan Partner att betraktas som ett underbiträde till Personuppgiftsbiträdet.	Vänligen se Bilaga V p. 5. Partner kommer motta faktura, reskontra och/eller informationsrapporter från Personuppgiftsbiträdet.	Information som listas i Bilaga II i detta DPA.	Information som listas i Bilaga II i detta DPA.	Enligt instruktion från Personuppgiftsansvarig till Partner och/eller Personuppgiftsbiträdet.	Enligt överenskommelse mellan Partner och Personuppgiftsansvarig.	Dagligen
Asteria AB Sveavägen 45, 1 tr 111 34 Stockholm	Integration och omstrukturering av datafiler skickade av Personuppgiftsansvarig	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Inkommande/utgående filer/API, databas, backuper: 6 månader E-post med installationsinstruktioner /instruktioner om uppsätt (inklusive PayEx-kontaktinformation): raderas omedelbart efter att installationen/uppsätt är klar. E-post från PayEx-kunder:	Sverige, Moln lagring på servers lokaliserade inom EU (Azure)	Dagligen, när integration används av Personuppgiftsansvarig för fakturering eller återrapportering till kunds ERP/affärssystem.

				Microsoft 365 GDPR-standard		
LinkMobility	Lagring och distribution av SMS/meddelanden	Personuppgiftsansvarigs kunder	Mobilnummer och meddelanden	3 månader	EU/EEA områden	Löpande, realtid
SpeedLedger AB Fabrikstorget 1 412 50 Göteborg (*Gäller ej Fakturaservice PxR eller Reskontraservice med belåning PxR)*	Integration och omstrukturering av datafiler skickade av Personuppgiftsansvarig	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Inkommande/utgående filer/API, databas, backuper: 6 månader E-post med installationsinstruktioner /instruktioner om uppsätt (inklusive PayEx-kontaktinformation): raderas omedelbart efter att installationen/uppsätt är klar. E-post från PayEx-kunder: Microsoft 365 GDPR-standard	Sverige, Moln lagring på servers lokaliserade inom EU (Azure)	Dagligen, när integration används av Personuppgiftsansvarig för fakturering eller återrapportering till kunds ERP/affärssystem.
Microsoft Azure Microsoft Ireland Operations Limited One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521 Irland (*Observera att*	Microsoft Azure är en plattform för molntjänster. Den tillhandahåller ett brett utbud av molntjänster, inklusive beräkning, analys, lagring och nätverk. Azure fungerar som lagringsplats och	Information som listas i Bilaga II i detta DPA.	Information som listas i Bilaga II i detta DPA.	Personuppgiftsbiträdet har möjlighet att komma åt, extrahera och radera lagrade uppgifter. Principer för lagring och radering av uppgifter följer de skriftliga instruktioner som dokumenterats i personuppgiftsbiträ	Microsoft ska lagra och bearbeta Kunddata inom Europeiska unionen med primär lagringsplats i Microsoft Clod Data Centers i Gävle & Sandviken, Sverige och	Löpande, realtid

Personuppgiftsbiträdets användning av Underbiträdet Microsoft Azure initieras stegvis och att förväntas vara i full användning i slutet av Q4 2024, samt att startdatum för migrering till Microsoft Azure är satt till att initieras under Q1-Q3 2024.)	personuppgifter nås, extraheras och behandlas av Personuppgiftsbiträdet för att tillhandahålla den Tjänst som beskrivs i Avtalet mellan Personuppgiftsansvarig och Personuppgiftsbiträdet.			desavtalet mellan Personuppgiftsbiträdet och den Personuppgiftsansvarige och Underbiträdet har därför inget inflytande över åtkomst, utdrag och radering av lagrade uppgifter.	sekundär (backup) lagringsplats i Microsoft Clod Data Centers i Staffanstorp, Sverige	
Efecte AB Drottninggatan 33, 111 51 Stockholm Sverige	Ärendehantering	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Ärenden/tickets sparas I 13 månader	Finland	Löpande, då slutkunder kontaktar Personuppgiftsbiträdets kundservice med fakturafrågor
Telia Company Stjärntorget 1, 169 79 Solna Sverige	Kundtjänst via telefon och chatt med programvaran Telia ACE	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Telefonsamtal och chatt-loggar sparas i 90 dagar.	Sverige	Löpande, då slutkunder kontaktar Personuppgiftsbiträdets kundservice med fakturafrågor
Apix Messaging Oy* (*Gäller endast; Fakturaservice PxR Finland samt Reskontraservice med belåning PxR Finland*)	Konvertering av fakturadataformat	Personuppgiftsansvarigs kunder	Autentiseringsinformation, kontaktinformation, transaktionsinformation	Inkommande fakturor, säkerhetskopiering av databaser: 7 år	Finland, molnlagringsservrar finns inom EU	Dagligen, när integration används av Personuppgiftsansvarig för fakturering
Mastercard Payment Services (*Gäller endast Fakturaservice i Norway*)	Lagring och Fakturahotell	Personuppgiftsansvarigs kunder	Information som listas i Bilaga II i detta DPA.	Mastercard Payment Services GDPR standard.	EU/EEA	Löpande, realtid

Utöver listan över underbiträden som beskrivs i denna BILAGA IV har Personuppgiftsbiträdet rätt att behandla personuppgifter inom PayEx-koncernen när sådan behandling är nödvändig för att kunna tillhandahålla Tjänsten på det sätt som definieras i Avtalet. När ett företag i PayEx-koncernen behandlar personuppgifter på uppdrag av Personuppgiftsbiträdet, åtar sig varje företag i PayEx-koncernen att behandla personuppgifter i enlighet med Tillämplig Lag, Avtalet och Personuppgiftsansvarigs instruktioner som anges i Bilaga 1 och dess underbilagor i DPA:t mellan Personuppgiftsansvarig och Personuppgiftsbiträdet.

Ver. 2023-10-25

BILAGA V

PERSONUPPGIFTSANSVARIGS INSTRUKTION TILL PERSONUPPGIFTSBITRÄDET

1. *Rättslig grund för behandling*

Den Personuppgiftsansvarige ansvarar för att behandlingen av uppgifter i enlighet med Avtalet och detta DPA är laglig i enlighet med Tillämplig Lag, oavsett om de registrerade har samtyckt till behandlingen eller om det finns annan rättslig grund för behandlingen, samt att personuppgifterna som omfattas av detta DPA, som Personuppgiftsbiträdet behandlar på uppdrag av Personuppgiftsansvarig har samlats in för specifika, explicita och motiverade ändamål och i övrigt i enlighet med Tillämplig Lag och att dessa ändamål har angetts i sin helhet och korrekt i Bilaga II. Den Personuppgiftsansvarige kommer omedelbart att meddela Personuppgiftsbiträdet om arten, föremålet eller ändamålet för personuppgifter som behandlas enligt Avtalet ändras.

2. *Lagringstid och lagring av Personuppgifter*

Personuppgiftsbiträdet kommer att lagra personuppgifter endast så länge som det är nödvändigt, i slutändan reglerat av Avtalet och så som vidare specificerat i detta DPA punkt 3.2. Den Personuppgiftsansvarige har instruerat Personuppgiftsbiträdet att tillhandahålla tjänsten på det sätt som definierats i Avtalet. När den Personuppgiftsansvarige och Personuppgiftsbiträdet inte längre har ett giltigt avtal på plats kommer Personuppgiftsbiträdet endast att lagra personuppgifter om det krävs enligt lag eller, i andra fall, under den definierade perioden för Avtalet, Avtalsperioden, men inte längre än till den tidpunktpunkt där Personuppgiftsbiträdet har upphört med administrationen och avslutat alla ärenden som finns i reskontran, inklusive fordringar som är under Långtidsbevakning.

Specifikation i förhållande till filer som kommuniceras till Personuppgiftsbiträdet via fil, CUSIN eller API: Den Personuppgiftsansvarige har samtyckt till att följa Personuppgiftsbiträdet regler och instruktioner som är tillämpliga vid tidpunkten för sändning och mottagning av filer. Om en teknisk beskrivning har upprättats och fogats till Avtalet ska denna följas. Personuppgiftsbiträdet kommer att lagra data som mottas från den Personuppgiftsansvarige via fil eller genom annan elektronisk kommunikation under en period av 13 månader.

Specifikation i relation till filer som kommuniceras av Personuppgiftsbiträdet till Personuppgiftsansvarige; Lagring av rapporter och skapade dokument har en generell lagringstid på 13 månader från skapande, exemplifierat nedan, såsom:

Rapport	**Lagringstid**
Reskontrarapport	13 månader från skapande
Skapade fakturor	13 månader från skapande
Fakturafordringar	13 månader från skapande
Slutkund tillgodo, detaljerad	13 månader från skapande
Oplacerade inkassobetalningar, detaljerad	13 månader från skapande
Oplacerade betalningar, detaljerad	13 månader från skapande
Nedskrivningsrapport, detaljerad	13 månader från skapande
Nedskrivningsrapport	13 månader från skapande
Åldersanalys	13 månader från skapande

3. *Distribution*

Personuppgiftsbiträdet kommer att distribuera fakturor, krav och annan kommunikation som beskrivs i Avtalet i enlighet med instruktioner som erhålls från Personuppgiftsansvarige via API, fil eller annan elektronisk kommunikation, och distribuera faktura, krav och annan kommunikation enligt Tjänstebeskrivningen tillhörigt Avtalet. Den Personuppgiftsansvarige

garanterar, såsom beskrivs i avsnitt 1, Bilaga V till detta DPA, den rättsliga grunden för behandling och att Personuppgiftsbiträdet kan distribuera fakturor, krav och annan kommunikation till de registrerade som kommunicerats till Personuppgiftsbiträdet från Personuppgiftsansvarig.

4. Fakturaportalen

Personuppgiftsbiträdet kommer att göra fakturainformation tillgänglig gällande Personuppgiftsansvariges slutkunder i en fakturaportal. Fakturaportalen är tillgänglig för slutkunder som mottar faktura via e-post eller när en länk eller integration till Fakturaportalen upprättas/används av Personuppgiftsansvarig. I Fakturaportalen kan slutkunden få tillgång till information om sina fakturor och följa status på en faktura (betald/obetald etc.). Slutkunden kommer även att ha möjlighet att betala sin mottagna faktura genom att använda tillgängliga betalningsmedel i Fakturaportalen. Den Personuppgiftsansvarige instruerar Personuppgiftsbiträdet att göra fakturainformation tillgänglig avseende den Personuppgiftsansvariges slutkunder i en Fakturaportal. Fakturainformation ska avse producerade slutkundsfakturor, påminnelser och i tillämpliga fall inkassomeddelanden (obs: distribution av inkassokrav kommer att följa den hierarki som beskrivs i Tjänstebeskrivningen av Avtalet, som beskrivs här i avsnitt 3 i denna Bilaga V. Fakturainformation och betalningsalternativ för sådana distribuerade anspråk kommer dock att vara tillgängliga via Fakturaportalen). Informationen i Fakturaportalen kommer att göras tillgänglig för slutkunden i enlighet med Personuppgiftsansvariges instruktioner till Personuppgiftsbiträdet, det vill säga när Personuppgiftsbiträdet skickar information genom användning av e-postadresser (insamlad och överförd till Personuppgiftsbiträdet av Personuppgiftsansvarig via fil, CUSIN eller API eller som på annat sätt överenskommits mellan Parterna) för att kommunicera fakturor och annan kommunikation/dokument/utlåtanden/sammanställningar etc. Informationen i Fakturaportalen kommer i allmänhet att göras tillgänglig genom länkinkludering (i t.ex. e-post) eller omdirigering för att därigenom överföras till slutkund utan behov av identitetsverifiering/stark autentisering, förutom i de fall slutkunden är skyldig att verifiera identiteten vid användning av tillgängliga betalningsmedel i Fakturaportalen, eller vid tillgång till information om ett inkassokrav. Vidare instruerar den Personuppgiftsansvarige Personuppgiftsbiträdet att tillgängliggöra information, till den Personuppgiftsansvariges i form av rapporter eller på annat sätt enligt beskrivningen i Avtalet, rörande den Personuppgiftsansvariges slutkunder som väljer att betala med hjälp av tillgängliga betalmedel i Fakturaportalen.

5. Partner

I ett scenario där Personuppgiftsansvarig har en integrerad lösning till Personuppgiftsbiträdet, vilket innebär att Personuppgiftsansvarig har integrerat till Personuppgiftsbiträdet genom användning av en Partner (d.v.s. en separat juridisk person som tillhandahåller bland annat integrationstjänster där Controllers ERP/e-handelssystem eller liknande integreras mot Personuppgiftsbiträdet på uppdrag av den Personuppgiftsansvarige), instruerar den Personuppgiftsansvarige härmed Personuppgiftsbiträdet att ta emot sådana personuppgifter, som tillhandahålls genom Partner till Personuppgiftsbiträdet på uppdragsgivarens vägnar, som om de mottagits direkt från den Personuppgiftsansvarige. Personuppgiftsansvarige instruerar vidare Personuppgiftsbiträdet att skicka faktura-, reskontra- och betalningsrapporter/information till Partner. Personuppgifter som överförs till Partner kommer att innehålla information som anges i Bilaga II till detta DPA. För tydlighetens skull betraktas Partner endast som underbiträde i förhållande till överföring av personuppgifter, enligt anvisningar från Personuppgiftsansvarige till Personuppgiftsbiträde, i form av faktura-, reskontra- och betalningsrapporter/information.

I ett scenario där Personuppgiftsansvarig har en partnerlösning där Personuppgiftsansvarig har ett separat avtal med en Finansieringspartner (till exempel en bank som tillhandahåller en finansieringslösning till Personuppgiftsansvarig) och ett separat avtal med Personuppgiftsbiträdet (avseende faktura-, administrations- och reskontratjänster d.v.s. Reskontratjänst med Finansiering PxR), och där Personuppgiftsansvarigs överenskommelse med Finansieringspartnern kräver att Personuppgiftsbiträdet delar viss faktura/reskontradata till sådan Finansieringspartner, instruerar den Personuppgiftsansvarige härmed Personuppgiftsbiträdet att ta emot personuppgifter, som tillhandahålls genom Finansieringspartner till Personuppgiftsbiträdet på uppdragsgivarens vägnar, som om det togs emot direkt från den Personuppgiftsansvarige. Personuppgiftsansvarig instruerar vidare Personuppgiftsbiträdet att skicka faktura-, reskontra- och betalningsrapporter/information samt kreditrelaterad information till Finansieringspartner. Personuppgifter som överförs till Finansieringspartner kommer att innehålla information som listas i Bilaga II till detta DPA. Personuppgiftsansvariges instruktioner finns närmare detaljerade i Tjänsteavtalet (avsnitt gällande personuppgifter) mellan Personuppgiftsansvarig och Personuppgiftsbiträdet.

6. Personuppgiftsansvarigs användning av tredje part

I ett scenario där Personuppgiftsansvarig använder en tredje part för att sända/kommunicera information kopplat till Tjänsten svarar Personuppgiftsansvarig för sådan tredje part så som för sig själv. Om tredje part utsetts av Personuppgiftsansvarig för att kommunicera fakturainformation, inklusive personuppgifter, via fil, CUSIN eller API eller som på annat sätt

överenskommits ansvarar Personuppgiftsansvarig för sådan fakturainformation, inklusive personuppgifter, och att uppgifterna samlats in i enlighet med Tillämplig Lag. Om Personuppgiftsansvarigs överenskommelse med tredje part kräver att Personuppgiftsbiträdet delar viss faktura/reskontradata med sådan tredje part, instruerar den Personuppgiftsansvarige härmed Personuppgiftsbiträdet att ta emot personuppgifter, som tillhandahålls genom tredje part till Personuppgiftsbiträdet på Personuppgiftsansvarigs vägnar, som om det togs emot direkt från den Personuppgiftsansvarige. Personuppgiftsansvarig instruerar vidare Personuppgiftsbiträdet att skicka faktura-, reskontra- och betalningsrapporter/information samt kreditrelaterad information till tredje part. Personuppgifter som överförs till tredje part kommer att innehålla information som listas i Bilaga II till detta DPA. Personuppgiftsansvariges instruktioner finns närmare detaljerade i Tjänsteavtalet (avsnitt gällande personuppgifter) mellan Personuppgiftsansvarig och Personuppgiftsbiträdet.