

LIITE I:

LUETTELO OSAPUOLISTA

Rekisterinpitäjä(t): *[Rekisterinpitäjän (rekisterinpitäjien) ja tarvittaessa rekisterinpitäjän tietosuojavastaavan tunnistetiedot ja yhteystiedot]*

Nimi: Yritys, joka on listattu asiakkaaksi PayExin asiakkaalle tarjoamaa laskutuspalvelua ja/tai reskontrapalvelua koskevan PayExin ja asiakkaan välisen puitesopimuksen etusivulla

Osoite: Viittaus PayExin ja asiakkaan välisen puitesopimuksen etusivulle

Yhteys henkilön nimi, asema ja yhteystiedot: Viittaus PayExin ja asiakkaan välisen puitesopimuksen etusivulle

Tietosuojavastaavan nimi ja yhteystiedot (*tarvittaessa*): Asiakas toimittaa tiedot PayExin pyynnöstä

Henkilötietojen käsittelijä(t): *[Henkilötietojen käsittelijän/käsittelijöiden ja tarvittaessa henkilötietojen käsittelijän tietosuojavastaavan tunnistetiedot ja yhteystiedot]*

Nimi: PayEx Suomi Oy, FO 2156811-3

Osoite: PL 178 15101 Lahti

Yhteys henkilön nimi, asema ja yhteystiedot: Viittaus PayExin ja asiakkaan välisen puitesopimuksen etusivulle

Tietosuojavastaavan nimi ja yhteystiedot (*tarvittaessa*):

Sähköpostiosoite:

dpo@payex.com

Osoite: PayEx Sverige AB,

Att: Dataskyddsbudet

621 88 Visby, Sverige

Puhelin: +46 (0) 8 - 20 24 00

LIITE II:

HENKILÖTIETOJEN KÄSITTELYN KUVAUS

Niiden rekisteröityjen ryhmät, joiden henkilötietoja käsitellään

Rekisterinpitäjän työntekijät, rekisterinpitäjän asiakkaat ja laskujen vastaanottajat, rekisterinpitäjän omistajat ja rekisterinpitäjän hallituksen/johtoryhmän jäsenet.

Käsiteltävät henkilötietoryhmät

Todentamistiedot (henkilötunnus, pankkitilin numero), yhteystiedot (nimi, osoite, puhelinnumero, sähköpostiosoite), historiatiedot (ostetut tavarat ja/tai palvelut), tapahtumatiedot (ostetut tavarat ja palvelut), seurantatiedot (IP-osoite, evästeet, laite) ja liitteessä V esitetyt muut henkilötietoryhmät.

Käsiteltävät arkaluonteiset tiedot (jos sellaisia on) ja sovelletut rajoitukset tai suojatoimet, joissa otetaan täysimääräisesti huomioon tietojen luonne ja niihin liittyvät riskit, kuten tiukat käyttötarkoituksen rajoitukset, pääsyrajoitukset (mukaan lukien pääsy vain erikoiskoulutusta saaneelle henkilöstölle), tietojen saantia koskevan rekisterin pitäminen, tietojen edelleen siirtämisen rajoitukset tai lisäturvatoimenpiteet.

Ellei rekisterinpitäjä ole tässä tietojenkäsittelysopimuksessa nimenomaisesti kirjallisesti ja henkilötietojen käsittelijän hyväksymänä toisin ohjeistanut, mitään erityisiä henkilötietoryhmiä (arkaluonteisia tietoja) ei käsitellä. Erityisiä henkilötietoryhmiä ovat tiedot, joista käy ilmi henkilön rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja ja biometrisiä tietoja luonnollisen henkilön yksiselitteistä tunnistamista varten, terveyttä tai henkilön seksuaalista käyttäytymistä tai seksuaalista suuntautumista koskevia tietoja.

Henkilötietojen käsittelyn luonne

Käsittelyn tavoitteena on laskutuspalvelujen ja niihin liittyvien reskontrapalvelujen tarjoaminen rekisterinpitäjän ja henkilötietojen käsittelijän välisen puitesopimuksen ja liitteessä V tarkemmin kuvatun mukaisesti. Lisäksi henkilötietojen käsittelijällä on lakisääteinen velvollisuus tuntea asiakkaansa (esim. rekisterinpitäjä) varmistaakseen, ettei palvelu tahattomasti tue laitonta toimintaa, ja estääkseen petokset ja muut palvelun väärinkäytökset.

Tietojen käsittely on luonteeltaan sellaista, mikä on välttämätöntä todettua tarkoitusta varten, sisältäen esimerkiksi tietojen tallentamisen, järjestämisen, jäsentämisen, säilyttämisen, mukauttamisen ja muokkaamisen, hakemisen, konsultoinnin, siirron, käytön, luovuttamisen siirtämällä, välittämällä tai asettamalla muutoin saataville, mukauttamisen tai yhdistämisen, rajoittamisen, poistamisen tai tuhoamisen.

Tarkoitus/tarkoitukset, jota/joita varten henkilötietoja käsitellään rekisterinpitäjän puolesta

Varmistaa, että henkilötietojen käsittelijä pystyy täyttämään puitesopimuksen ja liitteessä V kuvatun mukaiset velvoitteensa. Henkilötietojen käsittelijä voi lisäksi käsitellä kaikkia edellä mainittuja henkilötietoryhmiä palvelun parantamiseksi. Lisäksi henkilötietojen käsittelijän on lain mukaan tunnettava asiakkaansa (esim. rekisterinpitäjä) varmistaakseen, ettei palvelu tahattomasti tue laitonta toimintaa, ja estääkseen petokset ja muut palvelun väärinkäytökset.

Henkilötietojen käsittelyn kesto

Käsittelyn kesto rajoittuu palvelun tarjoamisen edellyttämään aikaan ja siihen, mitä liitteessä V on tarkemmin kuvattu, ellei puitesopimuksessa tai sovellettavassa laissa toisin mainita.

Siirron tiheys (esim. siiretäänkö tietoja kertaluonteisesti vai jatkuvasti)

Jatkuvasti

Henkilötietojen käsittelijöiden tai alikäsittelijöiden suorittamasta käsittelystä on ilmoitettava myös käsittelyn kohde, luonne ja kesto

Katso liitteet IV ja V

LIITE III:

TEKNISET JA ORGANISATORISET TOIMENPITEET, MUKAAN LUKIEN **TEKNISET JA ORGANISATORISET TOIMENPITEET TIETOTURVAN** **VARMISTAMISEKSI**

Kuvaus henkilötietojen käsittelijän/käsittelijöiden toteuttamista teknisistä ja organisatorisista turvatoimenpiteistä (mukaan lukien asiaankuuluvat sertifiointit) asianmukaisen turvallisuustason varmistamiseksi ja ottaen huomioon käsittelyn luonne, soveltamisala, asiayhteys ja tarkoitus sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit. Tekniset ja organisatoriset toimenpiteet kuvataan jäljempänä tässä liitteessä.

1. HENKILÖTIETOJEN PSEUDONYMISOINTI JA SALAUS

a. Tekniset toimenpiteet siirtoa varten EU/ETAN: sisällä tai maahan, jolla on EU:n myöntämä vastaavuuspäätös

Henkilötietojen käsittelijällä on oltava täytäntöönpantu salaustekniikan käytön käytäntö, joka kattaa salauksen hallintakeinojen käytön, salausavainten koko elinkaaren aikaisen suojaamisen ja hallinnan sekä salattujen tietojen saatavuuden (osana jatkuvuussuunnittelua). Henkilötietojen käsittelijän on käytettävä salaustekniikoita tietojen eheyden ja luottamuksellisuuden varmistamiseksi (esim. liikkuvien ja lepäävien tietojen suojaamiseksi). Katso myös kohta 6. Tietojen suojaaminen siirron aikana.

b. Tiedonsiirtovälineitä täydettävät suojatoimet kolmansiin maihin

Siirrettäessä henkilötietoja kolmanteen maahan sovelletaan edellä kohdassa 1 a) esitettyjen vaatimusten lisäksi tätä kohtaa.

Kaikki henkilötiedot on luvattoman pääsyn estämiseksi salattava tai pseudonymisoitava ennen siirtoa.

Rekisterinpitäjän tai toimeksi saaneen osapuolen on säilytettävä salauksen purkamiseen ja/tai pseudonymisoitujen henkilötietojen selkeään muotoon palauttamiseen tarkoitetut avaimet EU:n/ETA:n alueella. Salaus ja/tai pseudonymisointi on toteutettava tavalla, joka täyttää "Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi", jotka Euroopan tietosuojaneuvosto on kulloinkin hyväksynyt. Näin varmistetaan, että salausalgoritmi ja sen parametrisointi toteutetaan siten, että ne tarjoavat vankan suojan vastaanottajamaan viranomaisten suorittamaa salauksen ratkointia vastaan, seuraavat asiat huomioiden:

1. Vastaanottajamaan viranomaisten käytettävissä olevat resurssit ja tekniset valmiudet (esim. laskentateho väsytyshyökkäyksiä varten).
2. Salauksen vahvuudessa ja avaimen pituudessa otetaan huomioon se määrätty ajanjakso, jonka ajan salattujen henkilötietojen salassapito on varmistettava.
3. Salausalgoritmi toteutetaan oikein ja asianmukaisesti ylläpidetyllä ohjelmistolla, jossa ei ole tunnettuja haavoittuvuuksia.
4. Avaimia ja/tai pseudonymisointitietoja hallinnoidaan luotettavalla tavalla parhaita käytäntöjä noudattaen tietojen paljastumisen tai luvattoman käytön estämiseksi.
5. Salausalgoritmien vahvuuden arviointi, niiden kestävyys salauksen ratkointia vastaan ajan kuluessa.

6. Pseudonymisoinnin yhteydessä henkilötietoja on käsiteltävä siten, ettei niitä voida enää yhdistää tiettyyn rekisteröityyn tai käyttää rekisteröidyn erottamiseen suuremmasta ryhmästä ilman lisätietoja.
7. Käsiteltävien tietojen perusteellisen analyysin pohjalta varmistetaan – huomioiden kaikki tiedot, joita vastaanottajamaan viranomaisten voidaan olettaa pitävän hallussaan ja käyttävän – että pseudonymisoituja henkilötietoja ei voida yhdistää tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön vaikka niitä verrattaisiin tällaisiin tietoihin.

Henkilötietojen käsittelijän on viipymättä tehtävä tarvittavat päivitykset, jotta palvelu täyttää aina edellä mainitut vaatimukset.

2. HENKILÖTIETOJEN KÄSITTELYJÄRJESTELMIEN JA PALVELUIDEN JATKUVAN LUOTTAMUKSELLISUUDEN, EHEYDEN, KÄYTETTÄVYYDEN JA VIKASIIETOISUUDEN VARMISTAMINEN

Henkilötietojen käsittelijän on henkilötietoja käsitellessään asianmukaisilla teknisillä tai organisatorisilla toimenpiteillä varmistettava henkilötietojen riittävä tietoturva, mukaan lukien suojaus luvattomalta tai laittomalta käsittelyltä sekä epähuomiossa tapahtuvalta menettämiseltä, tuhoutumiselta tai vahingoittumiselta. Henkilötietojen käsittelijällä on oltava dokumentoitu ja täytäntöönpantava tietoturvallisuuden hallintakeinojen viitekehys tietojen ja IT-palveluiden suojauksen varmistamiseksi. Tietoturvallisuuden hallintakeinoilla varmistetaan tietojen luottamuksellisuus, eheys ja saatavuus liikkeessä, käytössä ja levossa koko niiden elinkaaren ajan, noudattaen muun muassa seuraavia periaatteita:

- a. Tietoturvaa kohdellaan erottamattomana osana yleistä järjestelmäsuunnittelua, ja tietoturvallisuuden hallintakeinot integroidaan IT-palvelujen eri tasoille (esim. sovellus-, tietokone- ja verkkotasolle).
- b. Noudatetaan syvyysuuntaisen turvallisuuden periaatetta tai vastaavaa periaatetta, jossa on käytössä useita suojaustasoja (esim. todennus, segmentointi, koventaminen, valtuutus, haittaohjelasuojaus, lokitus), jotta vältetään turvautuminen vain yhteen tietoturvallisuuden hallintakeinojen tyyppiin tai menetelmään.
- c. Jos järjestelmä tai komponentti on vuorovaikutuksessa toisten järjestelmien tai komponenttien kanssa, näiden oletetaan olevan suojaamattomia.
- d. Noudatetaan pienimmän valtuuden periaatetta (esim. käyttäjälle tai prosessille myönnetään pienimmät mahdolliset valtuudet järjestelmään pääsyyn).
- e. Suunnitellaan ja toteutetaan perustasoinen kirjausketjutoiminnallisuus.

Henkilötietojen käsittelijän on myös jatkuvasti seurattava tietoturvallisuuden hallintakeinonsa tehokkuutta ja korjattava havaitut puutteet viipymättä.

3. HENKILÖTIETOJEN SAATAVUUDEN JA HENKILÖTIETOIHIN PÄÄSYN NOPEAN PALAUTTAMISEN VARMISTAMINEN FYYSISEN TAI TEKNISEN VIAN SATTUESSA

Henkilötietojen käsittelijällä on oltava:

- Dokumentoidut ja täytäntöönpannut tietoturvapoikkeamien hallinnan menettelytavat, joilla varmistetaan nopea, tehokas ja järjestelmällinen reagointi tietoturvapoikkeamiin.
- Häätätilaneprosessi vakavien tietoturvapoikkeamien käsittelemiseksi.
- Liiketoiminnan jatkuvuussuunnitelmat, palautumissuunnitelmat tai vastaavat suunnitelmat hyväksyttävän palvelutason ylläpitämiseksi ongelmatilanteissa, jotka saattavat häiritä tietojen tai IT-palvelujen saatavuutta. Henkilötietojen käsittelijän on säännöllisesti testattava suunnitelmiansa toimivuutta ja arvioitava testien tuloksia jatkuvaa parantamista varten.
- Dokumentoidut ja täytäntöönpannut varmuuskopiointimenettelyt, joilla varmistetaan, että tiedot ja IT-palvelut varmuuskopioidaan ja palautetaan määritetyssä ajassa. Menettelyssä on huomioitava erilaiset riskit (esim. laitteistoviat, kiristyshaittaohjelmat). Varmuuskopiot on suojattava.
- Levykuvat varmuuskopioidaan ja testataan säännöllisesti määritetyn palautuspistetaavoitteen ja palautusaikatavoitteen mukaisesti.

4. TEKNISTEN JA ORGANISATORISTEN TOIMENPITEIDEN TEHOKKUUDEN SÄÄNNÖLLISEN TESTAUKSEN, TUTKINNAN JA ARVIOINNIN PROSESSIT, JOILLA VARMISTETAAN TIETOJEN KÄSITTELYN TURVALLISUUS

Henkilötietojen käsittelijällä on oltava dokumentoitu ja täytäntöönpantu riskienhallintaprosessi ja varmistusohjelma, joilla seurataan hallintakeinojen tehokkuutta, tunnistetaan ja hallitaan jäljellä olevia tietoturvariskejä ja varmistetaan henkilötietojen käsittelijän tietojen luottamuksellisuus, eheys ja saatavuus.

Henkilötietojen käsittelijän on suoritettava tietoturvaan liittyviä valvontatoimia (esim. mittauksia, tarkistuksia, arviointeja ja testauksia) varmistaakseen, että sen tietoturvallisuuden hallintakeinot ovat tehokkaita eikä niitä ohiteta ja että poikkeamat ja riskit tunnistetaan (esim. tietoturvakäytäntöjen ja -menettelyjen puuteanalyysi, vaatimustenmukaisuuden arvioinnit, IT-palvelun tietoturvariskien arviointi, koehyökkäykset, IT-palvelujen sisäiset ja ulkoiset tarkastukset). Henkilötietojen käsittelijän on arvioitava tietoturvaan liittyvän valvontansa tulokset ja päivitettävä tietoturvamenettelynsä ja täytäntöönpannut tietoturvallisuuden hallintakeinonsa ilman aiheetonta viivytystä.

Rekisterinpitäjän henkilötietoja ei oletusarvoisesti saa käyttää testaustoimintaan ellei rekisterinpitäjä ole antanut siihen nimenomaista suostumusta.

5. KÄYTTÄJÄN TUNNISTAMINEN JA LUVAN MYÖNTÄMINEN

Henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut pääsynhallintamenettelyt. Menettelyitä on valvottava ja tarkastettava säännöllisesti.

Menettelyihin on sisällyttävä seuraavat:

a) Käyttäjän vastuuvollisuus: Käyttäjillä on oltava yksilölliset käyttäjätunnukset, joita heidän on käytettävä, jotta varmistetaan, että käyttäjät voidaan tunnistaa IT-palveluissa suoritettujen toimien osalta. Henkilötietojen käsittelijän ei sen vuoksi tule käyttää IT-palveluissa jaettuja tilejä.

b) Käyttövaltuudet: Käyttövaltuudet on myönnettävä tarpeellisuus- ja pienimmän valtuuden periaatteita noudattaen, ja niitä on myönnettävä, muutettava tai poistettava oikea-aikaisesti.

- c) Valtuutus: Käyttövaltuuksien myöntämisen tulee edellyttää dokumentoitua valtuutusta.
- e) Tehtävien erillään pitäminen: Keskenään ristiriitaiset tehtävät ja vastualueet erotetaan toisistaan luvattoman tai tahattoman muuttamisen ja väärinkäytön mahdollisuuksien vähentämiseksi.
- f) Todentaminen: Todentamismenetelmien on vastattava henkilötietojen ja IT-palveluiden arkaluonteisuuden tasoa.
- g) Käyttövaltuuksien uudelleenvahvistus: Käyttövaltuudet on tarkistettava määräajoin (korotettujen käyttövaltuuksien osalta vähintään 6 kuukauden välein) sen varmistamiseksi, ettei käyttäjillä ole tarpeettoman laajoja oikeuksia ja että käyttövaltuudet poistetaan, kun niitä ei enää tarvita.
- h) Käyttäjien IT-palveluissa tekemien toimien lokitus: Käyttäjien toimet kirjataan lokiin ja niitä seurataan. Korotettuihin käyttövaltuuksiin sovelletaan tiukempaa tehostettua lokitusta ja valvontaa.
- i) Korotetut käyttövaltuudet: Korotettuihin käyttövaltuuksiin on sovellettava tiukempia tietoturvallisuuden hallintakeinoja, esimerkiksi tiukkaa valtuutusmenettelyä, mahdollisimman suppeita valtuuksia, monivaiheista todentamista, yksityiskohtaista lokitusta, tilien tiivistä valvontaa, tehtävien erillään pitämistä.

6. TIETOJEN SUOJAAMINEN SIIRRON AIKANA

Kaikki henkilötiedot on salattava siirron aikana. Henkilötietojen käsittelijällä on oltava käytössään tietoturvallisuuden hallintakeinoja, joilla suojaudutaan luvattomalta liikenteen pysäyttämiseltä tai häirinnältä. Langaton verkkoyhteys on salattava parhaiden käytäntöjen mukaisella tavalla.

Henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut menettelyt, joilla pääsy yrityksen verkkoon myönnetään vain valtuutetuille laitteille. Henkilötietojen käsittelijän on arvioitava, täyttävätkö pääte pisteet (esim. palvelimet, työasemat, mobiililaitteet) käsittelijän määrittämät tietoturvastandardit ennen kuin niille myönnetään pääsy yrityksen verkkoon.

Tiedonsiirron osapuolet sopivat luotettavasta julkisen avaimen varmenteen myöntäjästä tai infrastruktuurista, jolla varmistetaan kaikkeen tiedonsiirtoon osallistuvien lähettäjien ja vastaanottajien todentaminen. Jos siirronaikainen salaus ei käytetyn infrastruktuurin tai ohjelmiston koettujen haavoittuvuuksien vuoksi yksinään mahdollista asianmukaista suojausta, henkilötiedot salataan päästä päähän myös sovelluskerroksessa.

Liikkuvien henkilötietojen salaus on toteutettava tavalla, joka täyttää "Suositukset 1/2020 toimenpiteistä, joilla täydennetään tiedonsiirtovälineitä EU:ssa henkilötiedoille taatun suojan tason noudattamiseksi", jotka Euroopan tietosuojaneuvosto on kulloinkin hyväksynyt.

7. TIETOJEN SUOJAAMINEN TALLENTAMISEN AIKANA

Kaikkien muiden tässä asiakirjassa kuvattujen, lepäviä tietoja koskevien hallintakeinojen lisäksi, mukaan lukien esimerkiksi salaus, todentaminen/valtuutus ja kirjausketju, henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut varmuuskopiointimenettelyt sen varmistamiseksi, että tiedot ja IT-palvelut

varmuuskopioidaan ja palautetaan määritetyn ajan kuluessa. Menettelyssä on huomioitava erilaiset riskit (esim. laitteistoviat, kiristyshaittaohjelmat). Varmuuskopiot on suojattava. Levykuvat varmuuskopioidaan ja testataan säännöllisesti määritetyn palautuspistetavoitteen ja palautusaikatavoitteen mukaisesti.

Jos henkilötietoja siirretään säilytettäväksi kolmanteen maahan, ne on salattava ennen siirtoa kohdan mukaisesti. Katso kohta 1, Henkilötietojen pseudonymisointi ja salaus.

8. HENKILÖTIETOJEN KÄSITTELYPAIKKOJEN FYYSISEN TURVALLISUUDEN VARMISTAMINEN

Henkilötietojen käsittelijän on jatkuvasti havainnoitava fyysisiä ja ympäristöuhkia (esim. luonnonkatastrofit, vihamieliset hyökkäykset, onnettomuudet) ja pantava täytäntöön riittäviä hallintakeinoja näiden uhkien lieventämiseksi. Fyysinen pääsy tiloihin ja IT-laitteisiin, joissa rekisterinpitäjän henkilötietoja käsitellään, on rajattava valtuutettuihin työntekijöihin. Pilvipohjaisessa isännöinnissä henkilötietojen käsittelijä on velvollinen hyödyntämään vakiintuneita ja tunnettuja palveluntarjoajia, joiden datakeskukset sijaitsevat EU:n alueella.

Henkilötietojen käsittelijällä on oltava dokumentoitu ja täytäntöönpanu tietoturvallisuuden hallintakeinojen viitekehys tietojen ja IT-palveluiden suojauksen varmistamiseksi (esim. kaksivaiheinen tunnistus, tietomurtohälytin, aidat). Kaikki kulku tiloihin rekisteröidään ja kirjataan lokiin. Datakeskukset edellyttävät tarkkaa fyysistä kulunvalvontaa ja lisäturvallisuusjärjestelyjä (esim. vartiointi, kosteuden ja lämpötilan valvonta, palohälyttimet ja redundanttinen sähkönsyöttö).

9. TAPAHTUMIEN KIRJAAMISEN VARMISTAMINEN

Henkilötietojen käsittelijällä on oltava vähintään perustasoinen tapahtumien lokituksen mahdollistava järjestelmä.

10. JÄRJESTELMÄN KONFIGURAATION VARMISTAMINEN (ML. OLETUSKOKOONPANO)

Henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut tietoturvallisuuden konfiguraation perustasot kaikille komponenteille (esim. käyttöjärjestelmä, tietokannat, verkkolaitteet). Henkilötietojen käsittelijän on jatkuvasti tarkistettava IT-palveluiden tekninen vaatimustenmukaisuus suhteessa määriteltyyn tietoturvallisuuden perustasoon (esim. konfiguraation koventaminen). Havaitut poikkeamat on arvioitava ja niihin on puututtava asianmukaisin toimenpitein niihin liittyvän riskin käsittelemiseksi.

11. SISÄISTÄ TIETOTEKNIikka- JA TIETOTURVAHALLINTOA JA KOSKEVAT TOIMENPITEET

Henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut tietoturvallisuuteen liittyvät roolit ja vastuut, joissa tulee olla määritelty vastuuvollisuus sekä vastuu tietoturvallisuudesta koko organisaatiossa. Henkilötietojen käsittelijän on nimettävä henkilökohtainen rooli, jolla on kokonaisvastuu tietoturvallisuuden hallinnasta organisaatiossa (esim. keskustietojärjestelmien tietoturvavastaava).

12. PROSESSIEN JA TUOTTEIDEN SERTIFIOINTI/VARMISTUS

Henkilötietojen käsittelijällä on oltava täytäntöönpanu tietoturvallisuuden hallintajärjestelmä sen varmistamiseksi, että henkilötietojen käsittelijän suorittama tietoturvallisuustyö on jäsenneltyä, riittävää ja johdon katselmusten alaista.

Tietoturvallisuuden hallintajärjestelmän on täytettävä yleisimpien tietoturvastandardien (e.g. ISO/IEC 27001 tai riittävän vastaava vaihtoehto) vaatimukset ja siihen on sisällyttävä tietoturvallisuuden viitekehys (esim. politiikka ja menettelytavat), jotka pannaan täytäntöön koko henkilötietojen käsittelijän organisaatiossa rekisterinpitäjälle tarjottavat palvelut mukaan luettuina. Jos sertifiointeille/varmistukselle määrätään sovellettavassa laissa tai asetuksessa tai muualla rekisterinpitäjän toimesta erityisvaatimuksia, nämä vaatimukset on täytettävä.

13. TIETOJEN MINIMOINNIN VARMISTAMINEN

Henkilötietojen käsittelijän on myös varmistettava, että henkilötietoja käsitellään ja säilytetään rekisterinpitäjän antamien kirjallisten ohjeiden mukaisesti, jotka on dokumentoitu kirjallisesti henkilötietojen käsittelijän ja rekisterinpitäjän välisessä tietojenkäsittelysopimuksessa.

14. TIETOJEN LAADUN VARMISTAMINEN

Rekisterinpitäjän on huolehdittava dokumentoiduista prosesseista ja toimintatavoista, joilla varmistetaan, että henkilötiedot ovat oikeita ja ajantasaisia.

15. TIETOJEN RAJOITETUN SÄILYTTÄMISEN VARMISTAMINEN

Henkilötietojen käsittelijällä on oltava menettelytavat tietojen säilyttämiseksi ja poistamiseksi rekisterinpitäjän ohjeiden mukaisella tavalla.

16. TIETOJEN SIIRRETTÄVYYDEN MAHDOLLISTAMINEN JA NIIDEN POISTAMISEN VARMISTAMINEN

Henkilötietojen käsittelijän on pystyttävä tukemaan rekisterinpitäjää tämän tietosuojasetuksessa kuvattujen tietojen siirrettävyyttä koskevien velvoitteiden täyttämässä.

Henkilötietojen käsittelijällä on oltava dokumentoidut ja täytäntöönpannut menettelyt sen varmistamiseksi, että kaikki henkilötietojen käsittelijän tallennusvälineet tyhjennetään turvallisesti tai tuhoetaan fyysisesti käyttämällä yleisesti hyväksytyjä menetelmiä (esim. NIST SP 800-88 -ohjeet tallennusmedian tyhjentämiseen) tietojen turvallisen poistamisen varmistamiseksi.

LIITE IV:
HENKILÖTIETOJEN ALIKÄSITTELIJÖIDEN LUETTELO

Rekisterinpitäjä on valtuuttanut henkilö tietojen käsittelijän käyttämään seuraavia alikäsittelijöitä. Lisäykset ja/tai muutokset tähän luetteloon on säänneltä DPA:ssa liitteessä 1 lauseke 7.7. (a):

1. Nimi: [Kaikki henkilö tietojen käsittelijän käyttämät alikäsittelijät on lueteltu alla olevassa taulukossa]

Osoite: [Katso alla oleva taulukko]

Yhteys henkilön nimi, asema ja yhteystiedot: [Voidaan toimittaa pyynnöstä]

Kuvaus henkilö tietojen käsittelystä (mukaan lukien selkeä vastuunjako, jos lupa on myönnetty useammalle henkilö tietojen alikäsittelijälle): [Katso alla oleva taulukko]

2. ...

Henkilö tietojen alikäsittelijän nimi ja osoite	Käsittelyn kuvaus	Rekisteröityjen ryhmät	Henkilö tietoryhmät	Henkilö tietojen säilytysaika	Käsittelypaikka	Henkilö tietojen siirron tiheys
Postnord Strålfors AB, Terminalvägen 24, 171 73 Solna	Laskujen*, vaatimusten ja kirjeiden tulostaminen *Koskee vain Laskutuspalvelua	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	90 päivää	Ruotsi	Päivittäin, kun laskuja, vaatimuksia ja kirjeitä laaditaan/tulostetaan.
Edi solutions AB, Box 9169, 400 94 Göteborg (Ei koske Reskontrapalvelua,	Rekisterinpitäjän lähettämien tiedostojen integrointi ja uudelleenjärjestely	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	Saapuvat/lähtevät tiedostot/API, tietokanta, varmuuskopiot: 6 kuukautta	Ruotsi, pilvitalennus EU:n alueella sijaitsevilla palvelimilla (Azure)	Päivittäin, kun rekisterinpitäjä käyttää integraatiota laskutukseen tai asiakkaan toiminnanohjaus- tai liiketoimintajärjestelmään raportointiin.

<i>johon sisältyy laskujen diskonttaus PxR)</i>				Asennusohjeet (mukaan lukien PayExin yhteystiedot) sisältävä sähköposti: poistetaan heti, kun asennus on valmis. Sähköpostit PayExin asiakkailta: Microsoft 365:n GDPR-standardi		
21 Grams, Lumaparksvägen 9, 12125 Stockholm	B2C* (verkkopankki)- ja B2B (EDI) - verkkolaskujen jakelu, laskujen, vaatimusten ja kirjeiden digitaalinen jakelu * Koskee vain Laskutuspalvelua	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	90 päivää	Ruotsi, Norja, Suomi, Tanska, jakelumaasta riippuen.	Päivittäin, kun laskuja, vaatimuksia ja kirjeitä jaellaan.
Jos rekisterinpitäjä integroituu henkilötietojen käsittelijään kumppanin välityksellä, kumppania pidetään henkilötietojen käsittelijän alikäsittelijänä.	Ks. liite V, s. 5. Kumppani saa laskut, reskontrat ja/tai tietoraportit henkilötietojen alikäsittelijältä.	Tämän tietojenkäsittelysopimuksen liitteessä II luetellut tiedot.	Tämän tietojenkäsittelysopimuksen liitteessä II luetellut tiedot.	Rekisterinpitäjän kumppanille ja/tai henkilötietojen käsittelijälle antamien ohjeiden mukaisesti.	Kumppanin ja rekisterinpitäjän välisen sopimuksen mukaisesti.	Päivittäin

<p>Asteria AB Sveavägen 45, 1 tr 111 34 Stockholm</p>	<p>Rekisterinpitäjän lähettämien tiedostojen integrointi ja uudelleenjärjestely</p>	<p>Rekisterinpitäjän asiakkaat</p>	<p>Todentamistiedot, yhteystiedot, tapahtumatiedot</p>	<p>Saapuvat/lähtevät tiedostot/API, tietokanta, varmuuskopiot: 6 kuukautta</p> <p>Asennusohjeet (mukaan lukien PayExin yhteystiedot) sisältävä sähköposti: poistetaan heti, kun asennus on valmis.</p> <p>Sähköpostit PayExin asiakkailta:</p> <p>Microsoft 365:n GDPR-standardi</p>	<p>Ruotsi, pilvitalennus EU:n alueella sijaitsevilla palvelimilla (Azure)</p>	<p>Päivittäin, kun rekisterinpitäjä käyttää integraatiota laskutukseen tai asiakkaan toiminnanohjaus- tai liiketoimintajärjestelmään raportointiin.</p>
<p>LinkMobility</p>	<p>Tekstiviestipalvelujen tallennus ja jakelu.</p>	<p>Rekisterinpitäjän asiakkaat</p>	<p>Matkapuhelinnumero ja tekstiviestit.</p>	<p>3 kuukautta</p>	<p>EU/ETA</p>	<p>Jatkuvasti, reaaliaikaisesti</p>
<p><i>SpeedLedger AB Fabrikstorget 1 412 50 Göteborg</i></p> <p><i>(Ei koske Laskutuspalvelua PxR ja/tai Reskontrapalvelua, johon sisältyy laskujen diskonttaus PxR)</i></p>	<p>Rekisterinpitäjän lähettämien tiedostojen integrointi ja uudelleenjärjestely</p>	<p>Rekisterinpitäjän asiakkaat</p>	<p>Todentamistiedot, yhteystiedot, tapahtumatiedot</p>	<p>Saapuvat/lähtevät tiedostot/API, tietokanta, varmuuskopiot: 6 kuukautta</p> <p>Asennusohjeet (mukaan lukien PayExin yhteystiedot) sisältävä sähköposti: poistetaan heti, kun asennus on valmis.</p>	<p>Ruotsi, pilvitalennus EU:n alueella sijaitsevilla palvelimilla (Azure)</p>	<p>Päivittäin, kun rekisterinpitäjä käyttää integraatiota laskutukseen tai asiakkaan toiminnanohjaus- tai liiketoimintajärjestelmään raportointiin.</p>

				Sähköpostit PayExin asiakkailta: Microsoft 365:n GDPR-standardi		
<p>Microsoft Azure</p> <p>Microsoft Ireland Operations Limited</p> <p>One Microsoft Place</p> <p>South County Business Park</p> <p>Leopardstown</p> <p>Dublin 18</p> <p>D18 P521</p> <p>Ireland</p> <p><i>(Huomaa, että henkilötietojen käsittelijän Microsoft Azuren käyttö alikäsittelijänä on alkamassa vaiheittain, ja sen odotetaan olevan täydessä käynnissä vuoden 2024 neljännen vuosineljänneksen loppuun mennessä. Microsoft Azureen siirtymisen on tarkoitus alkaa vuoden 2024 kolmen</i></p>	<p>Microsoft Azure on pilvipalvelualusta. Se tarjoaa laajan valikoiman pilvipalveluita, mukaan lukien laskenta-, analytiikka-, tallennus- ja verkkotoimintoja. Azure toimii tallennussijaintina, ja henkilötietojen käsittelijä käyttää, poimii ja käsittelee henkilötietoja tarjotakseen rekisterinpitäjän ja henkilötietojen käsittelijän välisessä puitesopimuksessa kuvatun palvelun.</p>	<p>Tämän tietojenkäsittelysopimuksen liitteessä II luetellut tiedot.</p>	<p>Tämän tietojenkäsittelysopimuksen liitteessä II luetellut tiedot.</p>	<p>Henkilötietojen käsittelijällä on mahdollisuus käyttää, poimia ja poistaa tallennettuja tietoja. Tietojen säilyttämisessä ja poistamisessa noudatetaan henkilötietojen käsittelijän ja rekisterinpitäjän välisessä tietojenkäsittelysopimuksessa dokumentoituja kirjallisia ohjeita, eikä alikäsittelijällä siten ole vaikutusvaltaa tallennettujen tietojen käyttöön, poimintaan tai poistamiseen.</p>	<p>Microsoft tallentaa ja käsittelee asiakastietoja Euroopan unionin alueella siten, että ensisijainen tallennussijainti on Microsoft Cloud Data Centereissä Ruotsin Gävlessä ja Sandvikenissä ja toissijainen (vara)tallennussijainti Microsoft Cloud Data Centerissä Ruotsin Staffanstorpissa.</p>	<p>Jatkuvasti, reaaliaikaisesti</p>

<i>ensimmäisen neljänneksen aikana.)</i>						
Efecte AB Drottninggatan 33, 111 51 Stockholm Sverige	Tapausten hallinta	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	Tapaukset/palvelupyynnöt säilytetään 13 kuukauden ajan	Suomi	Jatkuvasti, kun loppuasiakkaat ottavat yhteyttä henkilötietojen käsittelijän asiakaspalveluun laskuihin liittyvissä kysymyksissä.
Telia Company Stjärntorget 1, 169 79 Solna Sverige	Asiakaspalvelu puhelimitse ja chatissa Telia ACE -ohjelmiston avulla	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	Puhelut ja chat-lokit tallennetaan 90 päivän ajaksi.	Ruotsi	Jatkuvasti, kun loppuasiakkaat ottavat yhteyttä henkilötietojen käsittelijän asiakaspalveluun laskuihin liittyvissä kysymyksissä.
Apix Messaging Oy* <i>(Koskee ainoastaan Laskutuspalvelua PxR Suomessa ja/tai Reskontrapalvelua, johon sisältyy laskujen diskonttaus PxR Suomessa)</i>	Laskun tiedon tallennusmuotojen muuntaminen	Rekisterinpitäjän asiakkaat	Todentamistiedot, yhteystiedot, tapahtumatiedot	Saapuvat laskut, tietokannan varmuuskopio: 7 vuotta	Suomi, pilvitalennuspalvelimet sijaitsevat EU:n alueella	Päivittäin, kun rekisterinpitäjä käyttää integraatiota laskutukseen
Mastercard Payment Services <i>(Koskee ainoastaan Laskutuspalvelua PxR Norjassa)</i>	Tallennustila ja laskuhotelli	Rekisterinpitäjän asiakkaat	Tämän tietojenkäsittelysopimuksen liitteessä II luetellut tiedot.	Mastercard Payment Servicesin GDPR-standardi.	EU/ETA	Jatkuvasti, reaaliaikaisesti

LIITE V:

REKISTERINPITÄJÄN OHJEET HENKILÖTIETOJEN KÄSITTELIJÄLLE

1. *Käsittelyn oikeusperuste*

Rekisterinpitäjä vastaa siitä, että puitesopimuksen ja tämän tietojenkäsittelysopimuksen mukainen henkilötietojen käsittely on laillista ja sovellettavan lainsäädännön mukaista riippumatta siitä, ovatko rekisteröidyt antaneet suostumuksensa käsittelyyn vai onko käsittelylle jokin muu oikeusperuste. Rekisterinpitäjä vastaa lisäksi sen varmistamisesta, että tämän tietojenkäsittelysopimuksen soveltamisalaan kuuluvat henkilötiedot, joita henkilötietojen käsittelijä käsittelee rekisterinpitäjän puolesta, on kerätty tiettyjä, nimenomaisia ja oikeutettuja tarkoituksia varten ja muutoin sovellettavan lain mukaisella tavalla ja että nämä tarkoitukset on ilmoitettu kokonaisuudessaan ja oikein liitteessä II. Rekisterinpitäjä ilmoittaa henkilötietojen käsittelijälle välittömästi, jos puitesopimuksen nojalla käsiteltävien henkilötietojen luonne, kohde tai tarkoitus muuttuu.

2. *Henkilötietojen säilytysaika ja säilytys*

Henkilötietojen käsittelijä säilyttää henkilötietoja vain niin kauan kuin se on tarpeen, mistä säännellään viime kädessä puitesopimuksella ja kuten tässä tietojenkäsittelysopimuksen kohdassa 3.2 on tarkemmin määritelty. Rekisterinpitäjä on ohjeistanut henkilötietojen käsittelijää tarjoamaan palvelun puitesopimuksessa määritellyllä tavalla. Kun rekisterinpitäjän ja henkilötietojen käsittelijän välillä ei enää ole voimassa olevaa kaupallista sopimusta, henkilötietojen käsittelijä säilyttää henkilötietoja vain, jos laki sitä edellyttää, tai muissa tapauksissa puitesopimuksen voimassaolon eli sopimuskauden ajan, kuitenkin enintään siihen asti, kunnes henkilötietojen käsittelijä on lopettanut hallinnon ja sulkenut kaikki reskontrassa olevat kohdat, mukaan lukien seurannassa olevat saatavat.

Tarkennus koskien henkilötietojen käsittelijälle tiedoston, CUSIN:n tai API:n kautta välitettyjä tiedostoja: Rekisterinpitäjä on sitoutunut noudattamaan henkilötietojen käsittelijän sääntöjä ja ohjeita, joita sovelletaan tiedostojen lähettämisen ja vastaanottamisen ajankohtana. Jos puitesopimukseen on laadittu ja liitetty tekninen kuvaus, sitä on noudatettava. Henkilötietojen käsittelijä säilyttää rekisterinpitäjältä tiedoston tai muun sähköisen tiedonsiirron välityksellä saamansa tiedot 13 kuukauden ajan.

Tarkennus koskien henkilötietojen käsittelijän rekisterinpitäjälle välittämiä tiedostoja; Raporttien ja laadittujen asiakirjojen säilytyksessä yleinen säilytysaika on 13 kuukautta laatimishetkestä alkaen alla olevien esimerkkien mukaisesti:

Raportti	Säilytysaika
Reskontraraportti (Reskontrarapport)	13 kuukautta
Laaditut laskut (Skapade fakturor)	13 kuukautta
Laskusaamiset (Fakturafordringar)	13 kuukautta
Liikasuoritus, yksityiskohtainen (Slutkund tillgodo, detaljerad)	13 kuukautta
Perintämaksut, yksityiskohtaiset (Oplacerade inkassobetalningar, detaljerad)	13 kuukautta
Yrityksen tilit, yksityiskohtaiset (Oplacerade inkassobetalningar, detaljerad)	13 kuukautta
Arvonlennusraportti, yksityiskohtainen (Nedskrivningsrapport, detaljerad)	13 kuukautta
Arvonlennusraportti (Nedskrivningsrapport)	13 kuukautta
Ikäanalyysi (Åldersanalys)	13 kuukautta

3. *Jakelu*

Jos sopimuksessa niin sovitaan; henkilötietojen käsittelijä jakaa laskut, vaatimukset ja muut sopimuksessa kuvatut viestit rekisterinpitäjältä CUSIN:ssä tai API:ssa saatujen ohjeiden mukaisesti ja käyttää sopimuksen palvelukuvauksessa kuvailun hierarkian ylintä käytettävissä olevaa jakelumenetelmää. Rekisterinpitäjä takaa tämän tietojenkäsittelysopimuksen liitteen V kohdassa 1 kuvatulla tavalla henkilötietojen käsittelyn oikeusperusteen ja sen, että henkilötietojen käsittelijä voi jakaa laskuja, vaatimuksia ja muita viestejä rekisterinpitäjältä CUSIN:n tai API:n kautta tai muilla keinoilla saatuihin henkilötietojen ryhmiin.

4. *Laskuportaali*

Jos sopimuksessa niin sovitaan; henkilötietojen käsittelijä asettaa rekisterinpitäjän asiakkaita koskevat laskutiedot saataville Laskuportaaliin. Laskuportaali on loppuasiakkaiden käytettävissä, kun nämä saavat laskun sähköpostitse tai kun rekisterinpitäjä on luonut/käyttänyt linkkiä tai integraatiota Laskuportaaliin. Laskuportaalissa loppuasiakas voi tarkastella laskujensa tietoja ja seurata laskun tilaa (maksettu/maksamaton jne.). Loppuasiakkaalla on myös mahdollisuus maksaa saamansa lasku Laskuportaalissa käytettävissä olevilla maksutavoilla. Rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää asettamaan rekisterinpitäjän asiakkaita koskevat laskutiedot saataville Laskuportaaliin. Laskutiedoilla tarkoitetaan laadittuja loppuasiakkaiden laskuja,

muistutuksia ja tarvittaessa perintäilmoituksia (huom. perintävaatimusten jakelussa noudatetaan sopimuksen palvelukuvauksessa kuvattua hierarkiaa tämän liitteen V kohdassa 3 kuvatulla tavalla. Tällaisten jaeltujen vaatimusten laskutiedot ja maksuvaihtoehdot ovat kuitenkin saatavilla Laskuportaalin kautta). Laskuportaalissa olevat tiedot asetetaan loppuasiakkaan saataville rekisterinpitäjän henkilötietojen käsittelijälle antamien ohjeiden mukaisella tavalla, eli kun henkilötietojen käsittelijä lähettää tietoja käyttämällä sähköpostiosoitteita (jotka rekisterinpitäjä kerää ja siirtää henkilötietojen käsittelijälle CUSIN:n tai API:n kautta tai osapuolten välillä muutoin sovitulla tavalla) laskujen ja muiden viestien/asiakirjojen/otteiden/koontien jne. välittämiseksi. Laskuportaalin tiedot asetetaan yleensä saataville linkin (esimerkiksi sähköpostiin sisällytetyn) tai uudelleenohjauksen välityksellä, jolloin loppukäyttäjä siirretään siten, ettei henkilöllisyyden todentamista/vahvaa tunnistusta tarvita, paitsi tapauksissa, joissa loppuasiakkaan on vahvistettava henkilöllisyytensä käyttäessään laskuportaalissa käytettävissä olevia maksukeinoja tai kun tilanteeseen liittyy pääsy perintävaatimusta koskeviin tietoihin. Lisäksi rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää asettamaan rekisterinpitäjän saataville raporttien muodossa tai muulla sopimuksessa määritellyllä tavalla tiedot rekisterinpitäjän asiakkaista, jotka päättävät maksaa laskuportaalissa käytettävissä olevilla maksutavoilla.

5. *Kumppani*

Tilanteessa, jossa rekisterinpitäjällä on henkilötietojen käsittelijään integroitu ratkaisu, tarkoittaen, että rekisterinpitäjä on integroinut henkilötietojen käsittelijään kumppanin välityksellä (eli erillisen oikeushenkilön, joka tarjoaa esimerkiksi integraatiopalveluja, joissa rekisterinpitäjän toiminnanohjausjärjestelmä/verkkokaupparjestelmä tai vastaava on integroitu henkilötietojen käsittelijään rekisterinpitäjän puolesta), rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää vastaanottamaan tällaiset henkilötiedot, jotka toimitetaan kumppanin kautta henkilötietojen käsittelijälle rekisterinpitäjän puolesta, ikään kuin ne olisi vastaanotettu suoraan rekisterinpitäjältä. Lisäksi rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää lähettämään lasku-, reskontra- ja maksuraportit/-tiedot kumppanille. Kumppanille siirretyt henkilötiedot sisältävät tämän tietojenkäsittelysopimuksen liitteessä II esitettyjä tietoja. Selvyyden vuoksi todetaan, että kumppania pidetään henkilötietojen alikäsittelijänä ainoastaan, kun henkilötietoja siirretään rekisterinpitäjältä henkilötietojen käsittelijälle antamien ohjeiden mukaisesti lasku-, reskontra- ja maksuraporttien/-tietojen muodossa.

Tilanteessa, jossa rekisterinpitäjällä on kumppaniratkaisu, jossa rekisterinpitäjällä on erillinen sopimus rahoituskumppanin kanssa (esimerkiksi pankin, joka tarjoaa rekisterinpitäjälle rahoitusratkaisun) ja erillinen sopimus rekisterinpitäjän kanssa (koskien laskutus-, hallinto- ja reskontrapalveluita eli Reskontrapalvelua, jossa on laskujen diskonttaus PxR) ja jossa rekisterinpitäjän sopimus rahoituskumppanin kanssa edellyttää, että henkilötietojen käsittelijä jakaa tietyt lasku-/reskontratiedot tällaisen rahoituskumppanin kanssa, rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää vastaanottamaan henkilötiedot, jotka toimitetaan henkilötietojen käsittelijälle rahoituskumppanin välityksellä rekisterinpitäjän puolesta, ikään kuin ne olisi saatu suoraan rekisterinpitäjältä. Lisäksi rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää lähettämään lasku-, reskontra- ja maksuraportit/-tiedot sekä luottoon liittyvät tiedot rahoituskumppanille. Rahoituskumppanille siirrettävät henkilötiedot sisältävät tämän tietojenkäsittelysopimuksen liitteessä II lueteltuja tietoja. Rekisterinpitäjän ohjeet on kuvattu tarkemmin rekisterinpitäjän ja käsittelijän välisessä palvelusopimuksessa (henkilötietoja koskeva osio).

6. *Rekisterinpitäjän kolmannen osapuolen käyttö*

Tilanteessa, jossa rekisterinpitäjä käyttää kolmatta osapuolta palveluun liittyvien tietojen lähettämiseen/välittämiseen, rekisterinpitäjä on vastuussa tällaisesta kolmannelta osapuolelta samoin kuin itsestään. Jos rekisterinpitäjä nimittää kolmannen osapuolen välittämään laskutietoja henkilötiedot mukaan lukien tiedoston, CUSIN:n tai API:n kautta tai muutoin sovitulla tavalla, rekisterinpitäjä on vastuussa tällaisista laskutiedoista henkilötiedot mukaan lukien sekä siitä, että tiedot on kerätty sovellettavan lain mukaisella tavalla. Jos rekisterinpitäjän ja kolmannen osapuolen välinen sopimus edellyttää, että henkilötietojen käsittelijä jakaa tiettyjä lasku-/reskontratietoja tällaisen kolmannen osapuolen kanssa, rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää vastaanottamaan kolmannen osapuolen kautta henkilötietojen käsittelijälle rekisterinpitäjän puolesta toimitetut henkilötiedot ikään kuin ne olisi saatu suoraan rekisterinpitäjältä. Lisäksi rekisterinpitäjä ohjeistaa henkilötietojen käsittelijää lähettämään lasku-, reskontra- ja maksuraportit/-tiedot sekä luottoon liittyvät tiedot tällaisille kolmansille osapuolille. Kolmansille osapuolille siirrettävät henkilötiedot sisältävät tämän tietojenkäsittelysopimuksen liitteessä II lueteltuja tietoja. Rekisterinpitäjän ohjeet on kuvattu tarkemmin rekisterinpitäjän ja käsittelijän välisessä palvelusopimuksessa (henkilötietoja koskeva osio).