Versio 29.11.2024

**Vaatimukset Vastuu Groupin Partnerirajapinnoista tietoa hakeville Partnereiden laitteille ja/tai järjestelmille**

Partnereiden järjestelmien ja/tai laitteiden, jotka hakevat tietoa Vastuu Groupin seuraavista Partnerirajapinnoista, tulee täyttää alla kuvatut rajapintavaatimukset:

- Korttivarasto
- Raporttinoutaja
- Valvoja-rajapinta
- Valtti+ Tarkastaja
- Person API
- Työmaarekisteri
- Kulkuri ja Erämies

Vaatimuksia tulee lukea yhdessä rajapintadokumentaation kanssa.

**Yleiset vaatimukset henkilö- ja työntekijätietoja käsitteleville laitteille ja/tai järjestelmille**

| # | Kriteeri/kontrollitavoite | Vaatimus/kontrolli |
|---|---|---|
| 1 | Henkilötietojen luovuttamiselle Vastuu Groupin tietovarastosta Partnerin loppuasiakkaalle on laillinen peruste | Loppuasiakas on tunnistettu. Loppuasiakas on tehnyt sopimuksen palvelusta Vastuu Groupin kanssa.<br><br>Rajapintahaun yhteydessä Partnerin järjestelmä välittää loppuasiakkaan asiakastunnisteen ja partnerin palvelutunnisteen Vastuu Groupille. |
| 2 | Käsittely henkilötietojen vastaanottajan päässä suoritetaan lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (lainmukaisuus, kohtuullisuus ja läpinäkyvyys) | Järjestelmän käyttöehdoissa on käyttö rajattu sallittuihin laillisiin käyttötarkoituksiin.<br><br>Loppukäyttäjä pitää rekisteröityjen saatavilla tietosuojaselostetta tai rekisteriselostetta. |
| 3 | Partnerin järjestelmässä henkilötietoja käsitellään tavalla, joka on yhteensopiva Vastuu Groupin tietosuojaselosteen ja käyttöehtojen kanssa –(käyttötarkoitussidonnaisuus) | Vastuu Groupilta saatuja henkilö- ja yritystietoja saa käyttää vain Vastuu Groupin käyttöehdoissa ja tietosuojaselosteissa kuvattuihin sallittuihin käyttötarkoituksiin. Partnerin järjestelmässä rajapintaoikeudet saa tarjota vain sellaiselle loppuasiakkaalle, joka täyttää Vastuu Groupin asiakaskriteerit ja hyväksyy Vastuu Groupin palveluiden käyttöehdot. |
| 4 | Partnerin järjestelmässä henkilötiedot ovat asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista käyttötarkoitukseen nähden (tietojen minimointi) | Partnerin järjestelmästä tehtävillä rajapintahauilla ei haeta tietoja, joille ei ole käyttötarvetta tai käyttöperustetta. |
| 5 | Käsiteltävien henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyys) | Partnerin ja loppuasiakkaan välillä sovittuna, miten epätarkat tai virheelliset tiedot korjataan ohjeistamalla työnantajayritys korjaamaan virheelliset tiedot myös Vastuu Groupin palveluun.<br><br>Partnerin järjestelmässä on toteutettu Vastuu Groupilta haettujen tietojen päivitysmahdollisuus. |
| 6 | Henkilötietoja säilytetään vain niin kauan kuin tarpeen käyttötarkoitusta varten (säilytyksen rajoittaminen) | Henkilötietojen säilytysajoille on olemassa ohjeistus ja järjestelmässä on työkalut, joilla voidaan tunnistaa, milloin lakisääteinen vähimmäissäilytysaika on päättynyt ja poistaa sellaiset henkilötiedot, joiden käsittelylle ei ole enää muuta perustetta. |
| 7. | Henkilötietoja käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”). | Partnerilla tai sen järjestelmällä/palvelulla on ISO 27001 sertifiointi tai Partnerin järjestelmä täyttää alla olevat minimivaatimukset |

| | | |
|---|---|---|
| 7.1 | Käyttäjän tunnistaminen | Järjestelmän käyttäjä (loppuasiakasyritys ja käyttäjä) tulee tunnistaa vähintään käyttäjätunnuksella ja (vahvalla) salasanalla. Oikeutetussa käytössä tulisi olla lisäksi käytössä vahva tunnistautuminen (monen tekijän tunnistautuminen). Järjestelmässä ei saa olla jaettuja käyttäjätunnuksia ja käyttäjätilien tulee olla yksilöllisiä.<br><br>Ylläpito-oikeudet toteutettu siten, että ylläpitotehtävän suorittaja tunnistetaan. |
| 7.2 | Käyttövaltuushallinta | Järjestelmä mahdollistaa käyttöoikeuksien rajaamisen käyttäjäryhmittäin ja käyttäjän työtehtävien perusteella esimerkiksi siten, että työnjohtajaroolissa on pääsy vain oman työmaan tietoihin.<br><br>Pääkäyttäjä tai ylläpito-oikeuksia annetaan ja käytetään vain poikkeustilanteiden ratkaisemiseen ja ylläpitotehtävien suorittamiseen.<br><br>Pääkäyttäjällä/ylläpitäjällä on oikeus päästä vain oman organisaationsa tietoihin.<br><br>Koko järjestelmän palveluntuottajalla on oikeus tarkistaa virhetilanteissa sen organisaation tietoja, jolle palveluntuottaja tarjoaa palveluita. |
| 7.3 | Lokitiedot | Järjestelmä pitää riittävän yksityiskohtaista käyttölokia henkilötietojen hakemisesta, käsittelystä ja luovuttamisesta edelleen.<br><br>Pääkäyttäjän/ylläpitäjän toimenpiteet lokitetaan.<br><br>Lokitietoja säilytetään vähintään 2 vuotta. Lokit on pystyttävä hakemaan saataville säännöllistä seurantaa ja valvontaa varten (esim. tarkistus, onko sellaisten henkilöiden henkilötietoja haettu, joita ei ole raportoitu Verohallinnon työntekijäraportille). |
| 7.4 | Istunnon aikakatkaisu | Partnerin järjestelmässä on toteutettu istunnon automaattinen aikakatkaisu. |
| 7.5 | Tiedonsiirron ja tietojen salaus ns. lepotilassa | (Henkilö)tietojen siirto laitteiden ja Partnerin järjestelmän välillä ja käytetyissä rajapintahauissa on suojattu asianmukaisesti huomioiden kulloinkin käytössä olevan teknologia.<br><br>Henkilötiedot tulee olla salattuna tietokannassa tai muussa tallennussijainnissaan. |
| 7.6 | Vastuu Groupin partnerirajapintojen käyttö | Partnerijärjestelmä käyttää rajapintoja Vastuu Groupin rajapintaohjeistuksen mukaisesti ja huomioiden mm. vaatimukset henkilötietojen käsittelyn käyttötarkoitussidonnaisuudesta ja tietojen minimoinnista. |

| | | |
|---|---|---|
| 7.7 | Sovellusturvallisuus ja privacy by design | Järjestelmän sovelluskehityksessä tunnistetaan ja huomioidaan tietoturvauhat ja -riskit ja järjestelmää päivitetään säännöllisesti. Tämä käsittää myös sovelluskehittäijien tilien (digitaalisten identiteettien) ja päätelaitteiden suojaamisen tietoturvauhkia vastaan. |
| 7.8 | Poikkeavan toiminnan monitorointi | Järjestelmässä tulee olla menettely, jolla luvaton käyttö ja luvattomat käyttöyritykset voidaan havaita ja rajata tietoturvapoikkeamat ennen lisävahinkojen tapahtumista. |
| 8. | Biometrisen tunnisteen tai muun erityisiin henkilötietoryhmiin kuuluvan tiedon käsittelyn laillisuus on varmistettu | Vastuu Groupilta saatua kuvaa ei saa käyttää biometrisenä tunnisteena ilman, että käsittelyn lainmukaisuus varmistettu. |
| 9. | Rekisterinpitäjä (loppuasiakas) ja käsittelijä (Partneri) ovat toteuttaneet asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi, mikäli Partnerin järjestelmään haetaan erityisiin henkilötietoryhmiin kuuluvaa tietoa | Rekisterinpitäjän ja käsittelijän toimittava tietosuoja-asetuksen 9 artiklan ja tietosuojalain 6 §:n mukaisesti |

**Vaatimukset Korttivarasto-rajapintaa käyttäville laitteille ja/tai järjestelmille**

| # | Kriteeri/kontrollitavoite | Vaatimus/kontrolli |
|---|---|---|
| 1. | Käsiteltävien henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä (täsmällisyys) | Partnerin järjestelmässä on toteutettuna Valttikorttien sulkulistan hyödyntäminen. Partnerijärjestelmän tulee hakea päivitetty sulkulista rajapinnan välityksellä vähintään kerran viikossa. Vastuu Group suosittelee, että sulkulista haetaan kerran päivässä Valttikorttien voimassaolotietojen ajantasaisuuden varmistamiseksi. |

**Vaatimukset Raporttinoutaja-rajapintaa käyttäville laitteille ja/tai järjestelmille**

| # | Kriteeri/kontrollitavoite | Vaatimus/kontrolli |
|---|---|---|
| 1. | Partneri ei saa muodostaa omaa itsenäistä rekisteriä tilaajavastuuraporteista tai hakea tilaajavastuuraportteja rajapinnasta muihin kuin loppuasiakkaan sopimuksenmukaisiin tarkoituksiin | Partnerin järjestelmä hakee rajapinnan välityksellä kunkin loppuasiakkaan puolesta ainoastaan kyseisen loppuasiakkaan määrittelemien yritysten tilaajavastuuraportteja.<br><br>Mikäli Partnerin järjestelmä tarjoaa Luotettava Kumppani -statuksen seurantaominaisuuden, tilaajavastuuraporttien päivittymisen seuranta loppuasiakkaiden puolesta on toteutettava siten, että partnerin järjestelmä hakee rajapinnan välityksellä säännöllisesti (vähintään kerran viikossa, mutta enintään kerran päivässä) tiedon siitä, onko loppuasiakkaan seurantaan valitsemien yritysten tilaajavastuuraporttien status muuttunut. Partnerin järjestelmä noutaa loppuasiakkaan puolesta seurantaan valittujen yritysten tilaajavastuuraportit vain niiden yritysten osalta, joiden raportti on päivittynyt. Partnerin järjestelmä ei hae rajapinnan välityksellä muiden yritysten tilaajavastuuraportteja. |
| 2. | Partnerin järjestelmästä ei saa hakea takautuvasti toisen loppukäyttäjäyrityksen hakemia vanhoja tilaajavastuuraportteja (järjestelmän luotettavuus) | Kukin loppukäyttäjäyritys hakee ja tallentaa Partnerin järjestelmässä tilaajavastuuraportit vain omaa käyttöään varten ja pääsee vain itse hakemiinsa tilaajavastuuraportteihin. |

**Vaatimukset Valvoja-rajapintaa käyttäville laitteille ja/tai järjestelmille**

| # | Kriteeri/kontrollitavoite | Vaatimus/kontrolli |
|---|---|---|
| 1. | Partneri ei saa muodostaa omaa itsenäistä rekisteriä tiedoista tai hakea tietoja rajapinnasta muihin kuin loppuasiakkaan sopimuksenmukaisiin tarkoituksiin | Partnerin järjestelmä hakee rajapinnan välityksellä kunkin loppuasiakkaan puolesta ainoastaan kyseisen loppuasiakkaan määrittelemien yritysten tietoja.<br><br>Muiden kuin tilaajavastuutietojen osalta Partnerin järjestelmä ei saa tallentaa historiatietoja. Partnerijärjestelmän tulee noutaa aina kulloinkin y-tunnuksen viimeisimmät tiedot.<br><br>Mikäli Partnerin järjestelmä tarjoaa y-tunnuksen tietojen seurantaominaisuuden, seuranta tulee toteuttaa siten, että partnerin järjestelmä hakee rajapinnan välityksellä säännöllisesti (vähintään kerran viikossa, mutta enintään kerran päivässä) tiedon siitä, onko loppuasiakkaan seurantaan valitsemien yritysten tiedot muuttuneet. Partnerin järjestelmä noutaa loppuasiakkaan puolesta seurantaan valittujen yritysten tiedot vain niiden yritysten osalta, joiden tiedot ovat päivittyneet. |
| 2. | Partnerin on varmistettava, että tiedot ovat asianmukaisia, olennaisia ja rajoitettuja siihen, mikä on tarpeellista käyttötarkoitukseen nähden (tietojen minimointi) | Partnerin tulee toteuttaa järjestelmäänsä toiminnallisuudet, joilla pyritään estämään loppuasiakasta lataamasta merkittävää määrää raportteja tai tietoja erilliseen tietokantaan. |
| 3. | Partnerin järjestelmän tulee eritellä tietojen lähteet ja tietojen ajantasaisuus | Partnerin järjestelmästä tulee käydä ilmi tietojen alkuperäinen lähde (rajapinnasta saatava tietoelementti), jotta mahdolliset poisto- tai muutospyynnöt voidaan luotettavasti toteuttaa, ja loppuasiakas saa tiedon datan lähteestä. Lisäksi Partnerin järjestelmän tulee näyttää tieto datan ajantasaisuudesta. |