

Tietosuoja-asetuksen huomioiminen Netvisor-palvelussa

Visma Solutions Oy toimii EU:n tietosuoja-asetuksen mukaisesti alihankkijana toimivana henkilötietojen käsittelijänä useille tilitoimistoille, jotka käsittelevät henkilötietojen käsittelijän roolissa asiakasyritystensä eli rekisterinpitäjien lukuun henkilötietoja.

Tietosuoja-asetuksen 28 artikla säätelee henkilötietojen käsittelijän velvollisuuksia. Asetuksen mukaan alkuperäinen henkilötietojen käsittelijä (tilitoimisto) on täysimääräisesti vastuussa alihankkijana käyttämänsä toisen henkilötietojen käsittelijän (Visma Solutions Oy) velvoitteiden suorittamisesta suhteessa rekisterinpitäjään. Oheinen selvitys pohjautuu Taloushallintoliiton valmistelemaan kyselyyn ohjelmistotaloille. Alla olevien kysymysten ja niiden vastausten kautta on kuvattuna Netvisor-palvelun EU-tietosuojalainsäädäntöön liittyvät oleelliset asiat.

Mikäli teillä on aiheeseen liittyen kysyttävää, voitte olla meihin yhteydessä tilitoimistomyyntimme kautta osoitteella tilitoimistomyynti@netvisor.fi.

Kysymys: Pääseekö henkilöstönne käsittelemään (tarkastelemaan) asiakasyritystemme henkilötietoja esimerkiksi tietokannan huoltotöiden yhteydessä tai asiakaspalvelu/helpdesk-toiminnassa?

Vastaus: Netvisorin asiakaspalvelussa on nimetyillä henkilöillä mahdollisuus ottaa pääsyoikeus asiakasympäristöön. Kaikki pääsyoikeuksien lisäämiset ja poistot lokitetaan ja niitä seurataan sisäisesti. Asiakkaalla on mahdollisuus kieltää asiakaspalvelun pääsy omaan ympäristöönsä kokonaan, mutta tämä voi hankaloittaa asiakaspalvelun tarjoamista ongelmatilanteissa.

Netvisorin tuotantoympäristön valvontatiimin nimetyillä henkilöillä on pääsy tuotantopalvelimille ja sitä kautta myös tietokantoihin, joissa asiakkaiden tiedot ovat. Pääsy tuotantoympäristöön vaatii moninkertaisen varmennuksen ja näitä yhteyksiä valvotaan sisäisesti. Näitä yhteyksiä käytetään vain ympäristön huoltotoimenpiteisiin sekä mahdollisten ongelmatilanteiden ratkaisuun.

Kysymys: Käytättekö palkanlaskentajärjestelmän tarjoamisessa alihankkijoita, joiden henkilöstöllä tai yhteistyökumppaneilla on mahdollisuus päästä käsittelemään (tarkastelemaan) asiakasyritystemme työntekijöiden henkilötietoja? Jos on, pyydämme nimeämään alihankkijat sekä heidän roolinsa palveluntuotannossa.

Vastaus: Netvisor-palvelun teknisenä yhteistyökumppanina toimii Elisa Appelsiini Oy ja Netvisor-palvelu tarjotaan heidän konesaliympäristöstään. Elisa Appelsiinin nimetyillä työntekijöillä on pääsy Netvisorin palvelimille. Elisa Appelsiini ylläpitää Netvisor-palvelun alustateknologiaa, mutta heillä ei ole suoraa pääsyä asiakasdataan. Lisäksi Netvisor-palvelun teknisenä konsulttina toimii DBPro Oy, jonka nimetyillä henkilöillä on rajattu pääsy palvelun tietokantoihin.

Kysymys: Miten on varmistettu, että ulkopuolinen taho ei pääse käsiksi tietoihin esimerkiksi tietoverkon kautta?

Vastaus: Netvisor-palveluun kirjautuminen tapahtuu aina vahvan tunnistautumisen kautta (2FA).
Palvelun kaikki tietoliikenne kulkee aina salattuna.

Tarkemmat tiedot Netvisorin tietoturvakäytännöistä löytyvät osoitteesta
https://netvisor.fi/media/netvisor-information_security_statement.pdf.

Kysymys: Miten henkilötietojen siirrot on salattu (tietokantojen ja tiedostojen siirto Internetissä)

Vastaus: Netvisor-palvelu toimitetaan pilvipalveluna, jolloin kaikki palveluun lisätyt henkilötiedot säilytetään Netvisorin suojatussa tuotantoympäristössä.

Tarkemmat tiedot Netvisorin tietoturvakäytännöistä löytyvät osoitteesta
https://netvisor.fi/media/netvisor-information_security_statement.pdf.

Kysymys: Miten on varmistettu, että vain tietyt nimetyt yrityksenne henkilöt pääsevät käsittelemään henkilötietoja?

Vastaus: Visman sisäiset käytännöt määrittelevät prosessin, jonka mukaisesti vain ne henkilöt, joiden työtehtävä edellyttää pääsyä asiakastietoihin, saavat pääsyoikeudet asiakasyritysten tietoihin.

Kysymys: Miten on varmistettu, että henkilötietojen käsittelystä (tarkastelu) jää talteen lokitiedot tarkastelijasta ja tarkastelun kohteesta?

Vastaus: Netvisor-palvelu tallentaa käyttäjien sivulataukset lokitiedostoihin, joiden kautta voidaan tarvittaessa saada selville, mitä yksittäinen henkilö on palvelussa tehnyt. Yrityksen pääkäyttäjällä ei toistaiseksi ole käytettävissä tarkastelulokia, mutta tiedot voidaan tarvittaessa toimittaa Netvisorin asiakaspalvelun kautta.

Kysymys: Onko henkilöstönne allekirjoittanut salassapitosopimuksen, joka kattaa asiakkaiden työntekijöiden henkilötiedot?

Vastaus: Kyllä, salassapitosopimus on osa työsopimusta

Kysymys: Miten henkilöstönne on koulutettu Tietosuoja-asetuksen vaatimuksiin?

Vastaus: Kaikki Visman työntekijät ovat velvoitettuja suorittamaan tietosuojakoulutuksen. Tämän lisäksi työntekijöille järjestetään tarpeen mukaan lisäkoulutusta omaan työtehtäväänsä ja rooliinsa liittyen.

Kysymys: Onko teiltä tulossa tietosuoja-asetuksen vuoksi esimerkiksi sopimusehtojen muutoksia tai ohjelmistopäivityksiä?

Vastaus: Kyllä, sopimusehdot tullaan päivittämään huhti-toukokuun aikana kattamaan tulevan tietosuojasäädöksen edellyttämät vaatimukset. Samoin Netvisor-palveluun tullaan lisäämään yksittäisiä toiminnallisuksia, jotka parantavat henkilötietojen käsittelyn läpinäkyvyyttä. Näistä julkaisemme lisätietoa Visma Solutionsin Communityssä <https://community.vismasolutions.com/>.

Kysymys: Onko järjestelmästäne mahdollisuus saada tarvittaessa henkilötiedot rakenteisessa tiedostomuodossa.

Vastaus: Netvisor-palveluun on mahdollista tallentaa henkilötietoja useilla eri tavoilla eri tarpeisiin liittyen. Palkansaajien tiedot löytyvät järjestelmästä suoraan, jonka lisäksi tiedot voidaan ladata tiedostona tai Netvisorin Web Service API-rajapinnan kautta. Muiden henkilötietojen osalta (esim. palvelun käyttäjät, CRM-yhteyshenkilöt) tiedot löytyvät järjestelmästä suoraan, josta ne ovat kopioitavissa taulukkomuodossa. Mikäli järjestelmän kautta saatavat tietojen viennit eivät ole riittäviä, suosittelemme olemaan yhteydessä asiakaspalveluumme.

Kysymys: Ovatko tietokannoissa olevat keskeiset luottamuksellisuutta edellyttävät henkilötiedot salattu tai toteutatteko tietojen salauksen ennen asetuksen voimaantuloa.

Vastaus: Netvisor-palvelussa tiedonsiirrot tehdään aina salattujen yhteyksien yli, mutta tietokannassa olevat tiedot eivät ole tällä hetkellä salattuna. Netvisor-palvelun tietokannat ovat kuitenkin Elisa Appelsiinilla turvallisessa ympäristössä ja suoraan tietokantaan pääseminen on mahdollista vain nimetyiltä henkilöiltä ja se edellyttää mm. kaksivaiheista tunnistautumista.

Kysymys: Jos asiakkaamme lopettaa asiakassuhteen, tulisi yrityksen palkanlaskennan tiedot pystyä poistamaan palvelimiltanne. Samaten yksittäisen työntekijän henkilötiedot on pystyttävä anonymisoimaan tai poistamaan, kun niitä ei enää tarvita. Onko ohjelmistossanne valmiudet tähän tai toteutatteko ne asetuksen voimaantuloajankohtaan mennessä?

Vastaus: Palvelun päättymistavasta riippumatta asiakkaan tiedot säilyvät Netvisor-palvelussa kirjanpitolain määrittämän lakisääteisen säilytysajan eli vähintään 6 vuotta. Tiedot poistetaan aikaisemmin, mikäli tilitoimisto sitä kirjallisesti pyytää. Pyyntö tietojen poistosta tapahtuu Netvisorin asiakaspalvelun kautta ja poisto toteutetaan Netvisorin tekniikan toimesta.

Yksittäisen palkansaajan poistamisessa tulee huomioida lakisääteiset vaatimukset tietojen säilytysajoista, eli palkkahallinnon aineistojen arkistointivelvoite 6 vuodeksi sekä palkkakausikohtainen henkilölistaus maksetuista palkoista, joka tulee säilyttää 10 vuotta. Toistaiseksi tietojen poistaminen tapahtuu Netvisorin tekniikan toimesta ja mikäli teillä on tarve poistaa tietoja, joiden osalta arkistointivelvoitetta ei enää ole, näiden osalta voitte kääntyä Netvisorin asiakaspalvelun puoleen.

Kysymys: Onko teillä jossakin lisätietoa Visman ja Visma Solutionsin valmistautumisesta EU:n tietosuoja-asetukseen?

Vastaus: Kyllä, lisätietoa löytyy mm. seuraavien linkkien kautta:

- Visman tietosuojasivut (englanniksi): <https://www.visma.com/privacy/>
- Visman valmistautuminen GDPR-asetukseen: <https://www.visma.com/gdpr/>
- Visman tietosuojaseloste: <https://www.visma.fi/yksityisyydensuoja/>
- Blogikirjoitus tietosuojasta Netvisorin blogissa: <https://netvisor.fi/blog/gdpr-tietosuoja-netvisorissa/>
- GDPR-aiheinen podcast Visma Solutionsin Bisnespöytä-podcastissa: <https://soundcloud.com/bisnespoyta/bisnespoyta-06-gdpr>