



Netvisor KYC -palvelun
teknologia- ja
tietoturvaseloste

Sisällysluettelo

Lukijalle	3
1. Netvisor KYC-palvelun tekninen toteutus	4
1.1. Netvisor KYC arkkitehtuuri	4
1.2. Kirjautuminen Netvisor KYC:iin	5
1.3. Integraatiot	5
1.4. Mitä pakotelistoja Netvisor KYC käyttää pakotelistavertailussa	6
2. Netvisor KYC:n tietoturva	7
2.1. Tekninen tietoturva	7
2.2. Hallinnollinen tietoturva	8
3. Palvelun ylläpito ja valvonta	9
3.1. Palvelun valvonta	9
3.2. Palvelun suorituskyky	9
3.3. Päivitykset Netvisor KYC-palveluun	10
3.4. Varmuuskopiointi ja tietojen palauttaminen	10
4. Tietosuoja	11
5. Usein kysytyt kysymykset	12
6. Lisätiedot	14

Lukijalle

Netvisor KYC on asiakkaan tuntemista automatisoiva järjestelmä, jota tuotetaan SaaS (Software as a Service) - mallilla. Visma Solutions Oy omistaa palvelun ja on vastuussa palvelun tuottamisesta. Visma Solutions Oy on osa Visma-konsernia ja näin ollen Netvisor KYC, kuten muutkin Visman palvelut noudattavat Visman yleisiä tietoturva- ja tietosuojasäännöksiä.

Tässä dokumentissa kuvataan Netvisor KYC-palvelun tekninen toteutus. Lisäksi dokumentissa esitetään miten tietoturva ja tietosuoja on Netvisor KYC palvelussa toteutettu. Dokumentin lopussa on myös osio, jossa käydään läpi yleisimmät kysymykset Netvisor KYC-palveluun liittyen ja vastaukset näihin. Dokumentissa on myös useita linkkejä lisätietoa tarjoaviin sivustoihin sekä Netvisorin omilla tukisivuilla että muilla Visman sivustoilla.

Löydät Netvisor KYC-palvelun teknologia- ja tietoturvaselosteen uusimman version osoitteesta <https://netvisorkyc.fi/teknologia-ja-tietoturva/>.

1. Netvisor KYC-palvelun tekninen toteutus

Netvisor KYC (jäljempänä "palvelu") on verkkopalvelu, jota voidaan käyttää eri verkkoselaimilla ja rajapintojen kautta.

Tavoitteemme on olla käytettävissä 24/7. Tästä poikkeuksena ovat ennalta suunnitellut käyttökatoja vaativat huoltoikkunat, joista tiedotamme etukäteen Netvisor KYC Communityn [Tiedotteissa](#), sekä niiden ulkopuoliset kiireelliset huoltotoimet, joilla takaamme nopean reagoimisen palvelun tietoturvan ja suorituskyvyn takaamiseksi.

Netvisor KYC käyttää palvelun tuottamiseen alihankkijoita. Palvelun tuotetaan Microsoft Azuren pilvessä ja konesalit sijaitsevat Irlannissa ja Norjassa. Microsoft Azure on yksi maailman suurimmista pilvipalvelualustoista, ja sen luotettavuus perustuu useisiin eri tekijöihin, kuten turvasertifikaatteihin, tietoturvastandardeihin, skaalautuvuuteen ja globaalisti hajautettuun infrastruktuuriin.

Ajantasainen lista palvelun tuottamiseen käytettävistä palveluntarjoajista ja alihankkijoista on saatavilla Visma Trust Centrestä [Netvisor KYC:n sivulta](#)

1.1. Netvisor KYC arkkitehtuuri

Netvisor KYC on teknisesti toteutettu pilvipalveluksi sen historian alusta asti. Palvelu on toteutettu pääosin Microsoftin teknologioilla ja käyttäen kulloinkin voimassa olevia alan standardeja ja suositeltavia toimintatapoja.

Netvisor KYC-palvelun arkkitehtuuri on rakennettu skaalautuvaksi, eli palvelu hyödyntää useita sovelluspalvelimia ja liikenne näille jaetaan kuormantasaimen kautta. Palvelun suunnittelussa on huomioitu vikasietoisuus, jotta toimintakyky voidaan säilyttää myös häiriöiden yhteydessä. Tuotantokäytössä olevat järjestelmät ovat fyysisesti kahdennettuja. Netvisor KYC:n tuotantoympäristö on suojattu monitasoisesti; kaikki palveluun kohdistuva liikenne suodatetaan useaan kertaan, sisältäen muttei rajautuen palomuriin, kuormantasaimen sekä volumetriseen palvelunestohyökkäyksiä estävään suojaimeen.

1.2. Kirjautuminen Netvisor KYC:iin

Netvisor KYCin käyttäjätunnus on henkilökohtainen ja käyttäjä on vastuussa omilla tunnuksillaan palvelussa tehdyistä toimenpiteistä. Netvisor-palvelun kirjautuminen tapahtuu aina vahvalla 2FA-tunnistautumisella. Saatavilla olevat kirjautumistavat ovat:

- Käyttäjätunnukseen, salasanaan ja tekstiviestitse toimitettavaan kertakäyttöiseen koodiin pohjautuva tunnistautuminen
- Microsoft Entra ID -pohjainen AD-kirjautuminen

Palvelun käyttö ei ole mahdollista pelkällä käyttäjätunnus-salasana -yhdistelmällä. Yksittäisiä palvelun osia on mahdollista päästä käyttämään suoraa linkillä, jonka kautta palveluun siirryessä käyttäjälle lähetetään kertakäyttöinen tunnistuskoodi tekstiviestillä tai sähköpostilla. Tämän kautta kuitenkin voi palvelussa tehdä vain ennalta määriteltäviä toimenpiteitä (kuten tietopyyntöön vastaaminen).

1.3. Integraatiot

Netvisor KYC-palvelu on yhdistetty useisiin kolmannen osapuolen palveluihin, jotka tarjoavat käyttäjille automaatiota ja lisäominaisuuksia.

- Integraatiot Netvisor KYC:stä esimerkiksi projektinhallintasovelluksiin
- Asiakkaiden omat integraatiot heidän ERP-järjestelmästä Netvisor KYC-sovellukseen.

Sisäänrakennettujen integraatioiden lisäksi Netvisor KYC tarjoaa integraatiokumppaneiden käyttöön ohjelmistorajapinnan, jonka avulla järjestelmään voidaan liittää kolmansien osapuolien ohjelmistoja. Kaikki rajapintaliikenne on valvottua ja suojattua. Käyttäjä voi milloin tahansa katkaista integraation omiin tietoihinsa verkkopalvelun kautta.

Ajantasainen lista integraatioista eri palveluihin löytyy [Netvisor KYC:n](#) sivuilta.

1.4. Mitä pakotelistoja Netvisor KYC käyttää pakotelistavertailussa

Netvisor KYC -palvelu hyödyntää pakotelistavertailussa aina ajantasaisinta saatavilla olevaa tietoa. Palvelu käyttää virallisia pakotelistoja varmistaakseen luotettavan ja ajankohtaisen seulonnan. Käytettävät listat sisältävät Yhdistyneiden Kansakuntien (YK) pakotelistan, Ison-Britannian (UK) listan, Euroopan unionin (EU) pakotelistan, Yhdysvaltojen OFAC-listan (Office of Foreign Assets Control), Kanadan hallituksen pakotelistan sekä Keskusrikospoliisin (KPR) ylläpitämän varainjäädytyslistan. Näin varmistetaan, että tunnistetut henkilöt ja organisaatiot tarkastetaan kattavasti kansainvälisiä vaatimuksia vasten.

Nimien vertailu pakotelistoihin tehdään hyödyntämällä yleisesti hyväksyttyjä vertailualgoritmeja ja niiden yhdistelmiä. Näihin kuuluvat muun muassa merkkijonojen samankaltaisuutta arvioivat algoritmit, kuten fuzzy matching. Näin varmistetaan, että vertailu on sekä tarkka että joustava, ja että mahdolliset osumat tunnistetaan myös tilanteissa, joissa nimi esiintyy eri muodoissa tai kirjoitusasuissa.

2. Netvisor KYC:n tietoturva

Netvisor KYCin tietoturva pohjautuu Visma-konsernin omaan tietoturvaohjelmaan ([Visma Security Program](#)), jota kaikki Visman tuotteet noudattavat. Kyseisessä ohjelmassa Visman tuotteita tarkastellaan monesta eri näkökulmasta sekä automaattisten että manuaalisten tarkastusten kautta ja jokaisen tuotteen tietoturvasta on tiedossa reaaliaikainen tilannekuva.

2.1. Tekninen tietoturva

Palvelun osista ja sen toiminnasta vastuussa ovat Netvisor KYC tuotekehitystiimi.

Netvisor KYCin tekninen tietoturva on rakennettu kerroksittain ja eri osa-alueilla tietoturva on huomioitu käyttäen yleisesti suositeltuja käytäntöjä. Turvallinen tiedonsiirto käyttäjien ja Netvisor KYCin välillä sekä palvelun sisäisesti noudattaa mm. seuraavia periaatteita:

- Tiedonsiirto tehdään salattujen yhteyksien yli (encrypted data in transit)
- Palveluun tallennetut tiedot ovat salattu (encrypted data at rest)
- Pääsynhallinta järjestelmässä perustuu monikerroksiseen autentikaatioon sekä roolipohjaisuuteen (RBAC)
- Palvelinympäristön verkkoinfrastruktuuri on rakennettu alan hyvien käytäntöjen mukaisesti ja tietoturvastandardeja noudattaen

Osana Netvisor KYCin teknistä tietoturvaa palvelusta tuotetaan logitietoja käyttäjien toimista. Lokia analysoidaan sekä automaattisten hälytysten pohjalta, että manuaalisesti tasaisin väliajoin virhetilanteiden havaitsemiseksi. Analyysia tehdään vain palvelun tietoturvan takaamiseksi.

Palvelinympäristöissä käytetyt ohjelmistot (käyttöjärjestelmä, antivirusohjelmistot, muut palvelun tuottamiseen tarvittavat ohjelmistot) päivitetään säännöllisesti ja mahdollisiin tietoturvahaavoittuvuuksiin näissä ohjelmistoissa reagoidaan viipymättä. Sovellustasolla Netvisor KYC-palvelua kehitetään tietoturvaperiaatteet edellä, huomioiden muun muassa OWASP top 10 -uhat.

Käytössämme on myös automaattisia skannaustoimintoja, joiden avulla pyrimme havaitsemaan ja korjaamaan mahdolliset uhat mahdollisimman pian. Palvelun toimintaa tarkastellaan useasta näkökulmasta hyödyntäen alan parhaita työkaluja (SAST, SCA, DAST).

2.2. Hallinnollinen tietoturva

Netvisor KYC-palvelun hallinnollinen tietoturva pohjautuu Visma-konsernin omaan tietoturvaohjelmaan, joka on kaikille Visman tuotteille pakollinen. Visman tietoturvaohjelma käsittää jatkuvia tietoturvamittareita, sisäisiä tietoturva-auditointeja sekä hallinnollisten prosessien säännöllisiä tarkastuksia. Näistä osa-alueista koostuu jokaiselle Visma-tuotteelle oma Security Maturity Index, joka antaa reaaliaikaisen kuvan siitä, mikä kunkin Visma-tuotteen tietoturvan taso on. Lisätietoa Visman tietoturvaohjelmasta löytyy [Visma Trust Centrestä](#).

Kaikki Visman työntekijät ovat velvoitettuja suorittamaan säännöllisesti konsernin tietoturva- ja tietosuojakoulutukset. Kaikkien Visman työntekijöiden sekä yhteistyökumppaneiden kanssa on solmittu salassapitosopimukset.

Vismalla on konsernitasoinen [Responsible Disclosure](#)-ohjelma, jonka kautta kuka tahansa voi luottamuksellisesti välittää Vismalle tiedon mahdollisesta haavoittuvuudesta missä tahansa Visman tuotteessa tai palvelussa.

3. Palvelun ylläpito ja valvonta

Netvisor KYCin ylläpidosta, toiminnallisuuden kehittamisestä ja päivittämisestä vastaa Netvisor KYC tuotekehitystiimi.

3.1. Palvelun valvonta

Palvelun valvonnasta huolehtii koko Netvisor KYC tuotekehitystiimi. Valvonnassa tukena on logitus, sekä automaattiset skannerit, joita Visma Solutions konsernin tasolta tuottaa taustapalveluna ja pyrkii näin löytämään mahdollisia haavoittuvuuksia Netvisor KYC palvelusta.

3.2. Palvelun suorituskyky

Netvisor KYC käyttäjälle näkyvä suorituskyky pohjautuu moneen eri tekijään, mm. käyttäjän oman internetyhteyden nopeus, asiakkaan oman laitteiston suorituskyky sekä palvelun palvelinympäristöjen suorituskyky. Kuten kaikissa verkkopalveluissa, on asiakkaan käyttötavalla merkitystä järjestelmän nopeudelle.

Pääsääntöisesti kaikki Netvisor KYC-palvelun sivulataukset tapahtuvat keskimäärin alle sekunnissa. Yksittäisten toimintojen osalta voi järjestelmä kuitenkin olla hitaampi, mikäli sivulle ladattavaa tietoa on poikkeuksellisen paljon verraten yritysten keskimääräiseen datan määrään tai yritysympäristössä on samanaikaisesti poikkeavaa käyttöä.

Mikäli jokin perustoiminto hidastuu merkittävästi ja pitkäkestoisesti, tulee asiakkaan ottaa yhteyttä asiakaspalveluun ongelman juurisyyn ratkaisemiseksi. Tämä voi olla esimerkiksi integraatioiden ajastaminen toimistoaikojen ulkopuolelle.

3.3. Päivitykset Netvisor KYC-palveluun

Netvisor KYC on Internet-selaimella käytettävä SaaS-palvelu, joten asiakkaiden ei itse tarvitse huolehtia ohjelmiston päivittämisestä uuteen versioon. Netvisor KYC-palvelun uudet ominaisuudet tulevat asiakkaiden käyttöön automaattisesti, eikä päivityksistä koidu erillisiä kustannuksia. Netvisor KYC:n päivitykset tehdään taaksepäin yhteensopivasti ja lyhyinä katkoksina normaaleiden toimistoaikojen ulkopuolella, noin kahden viikon välein.

3.4. Varmuuskopiointi ja tietojen palauttaminen

Toteutamme Netvisor KYC tietokantojen varmuuskopioinnin päivittäin.

Tietokannasta tehdään muuttuneiden tietojen osalta varmuuskopiot joka päivä, sekä viikoittain toinen varmuuskopio. Varmuuskopiot ovat fyysisesti erillään toisistaan eri datakeskuksissa, jolloin yhden datakeskuksen häiriö ei vaaranna varmuuskopioiden tilaa.

Tietokantojen viikoittaisten varmuuskopioiden talletusaika on yksi vuosi. Tietokantoihin tallennettua dataa ei voida palauttaa, mikäli muutoksesta on kulunut yli vuosi.

Tietojen palauttamisen yhteydessä esimerkiksi katoamis- tai korruptoitumistilanteessa datan menetys on minimissään viisi minuuttia, maksimissaan viikon riippuen seuraavista tekijöistä:

- milloin ja miten vikatilanne syntyi
- paljonko tapahtumasta on kulunut aikaa siihen, kun ongelma havaitaan
- kuinka laajasti vikatilanne vaikuttaa myös porrastettuihin varmistusjärjestelmiin

Normaalitilanteessa vaikutuksen kohdistuessa vain aktiiviseen dataan voimme tehdä palautuksen 5min – 1h aikavälille. Mikäli on tarve palauttaa tiedot muuhun ajankohtaan kuin edelliseen varmuuskopioituun tilanteeseen, on palautusmahdollisuus aina arvioitava tapauskohtaisesti. Huomioitahan, ettemme toteuta palautuksia asiakkaan pyynnöstä, vaan ainoastaan palvelun toiminnan takaamiseksi sekä asiakasdatan turvaamiseksi häiriötilanteissa. Palautukset suoritamme aina tapauskohtaisesti parhaan kykymme mukaisesti, emmekä voi taata yksittäisten data-alkioiden palautusta johtuen tiedon rakenteesta ja käsittelyn luonteesta.

4. Tietosuoja

Visma noudattaa kaikessa toiminnassaan voimassa olevaa tietosuojalainsäädäntöä ja paikallisia suosituksia. Visma-konsernissa tietosuojavastuut ovat jaettu Visma-konsernin sekä paikallisten Visma-yhtiöiden välillä niin, että Visma-konserni vastaa yleisesti Visman käyttämistä tietosuojaprosesseista ja konsernitason tietosuojasta. Visma Solutions Oy vastaa itse tietosuojasta oman yhtiönsä tuottamien palveluiden, kuten Netvisor KYC:n osalta.

Ajantasainen lista palvelun tuottamiseen käytettävistä palveluntarjoajista ja alihankkijoista on saatavilla Visma Trust Centrestä [Netvisor KYC:n sivulta](#)

Visma Solutionsin [tietosuojaseloste](#) kuvaa kuinka Visma Solutions Oy käsittelee henkilötietoja rekisterinpitäjänä sekä henkilötietojen käsittelijän rooleissa.

Netvisor KYCin asiakassopimuksen liitteenä on tietosuojaliite, joka toimii tietosuojasopimuksena (Data Protection Agreement, DPA). Kyseisessä sopimusliitteessä määritellään GDPR:n mukaiset vastuut sekä palvelun tuottajalle että asiakkaalle ja kuvataan kuinka mm. alihankkijoiden käyttö on toteutettu.

Viimeisimmät Netvisor KYC-palvelusopimuksen ja käyttöehdot löytyvät osoitteesta <https://netvisorkyc.fi/palveluehdot/>.

Visma tekee tietuoja-asioissa yhteistyötä paikallisten tietuoja- ja tietoturva-viranomaisten kanssa. Lisätietoa Visman tietuojatyöstä löytyy osoitteesta <https://www.visma.com/trust-centre/privacy>.

Visma Solutionsin tietosuojavastaava:

Tietoturva- ja tietuojajohtaja Riku Tarkiainen (privacy.solutions@visma.com).

5. Usein kysytyt kysymykset

Kysymys: Miten Netvisor KYC:n asiakastietojen tietoturvasta pidetään huolta?

Vastaus: Netvisor KYC -palvelun tietoturvaa kehitetään jatkuvasti monilla eri tavoilla.

Sovelluksen tietoturvaa päivitetään säännöllisesti ja sen toimintaa seurataan mm. logitusten ja muiden metriikoiden avulla. Ohjelmistoa testataan myös jatkuvasti käyttäen ulkoisia sovelluksia ja palveluita, jotka yrittävät löytää sovelluksesta heikkouksia. Käytämme myös skannauspalveluita, jotka skannaavat sovelluksen lähdekoodin mahdollisten haavoittuvuuksien ja muistivuotojen varalta ja raportoi mahdollisista havainnoista suoraan kehitystiimille.

Sovellukselle suoritetaan myös tasaisin väliajoin Visman oman tiimin toimesta penetraatiotestaus, jossa tuotekehitystiimin ulkopuolinen taho yrittää murtautua ja löytää heikkouksia sovelluksesta. Penetraatiotestauksessa löytyneet havainnot korjataan ensi tilassa.

Sovelluksen käyttämä tietokanta varmuuskopioidaan ja varmuuskopiot sijoitetaan fyysisesti eri maantieteellisiin sijainteihin. Tällöin yhden datakeskuksen mahdollinen vikatilanne ei vaaranna varmuuskopioita. Kaikki sovelluksen data (myös varmuuskopiot) sijaitsee aina EU/EEA alueella. Yhteys tietokantaan on aina salattu, sekä tietokanta itsessään käyttää salausta pitämään data turvassa mahdollisilta ulkoisilta fyysisiltä uhilta.

Pilvipalveluiden osalta noudatamme tiukkaa pääsynhallintalinjausta. Mikäli työntekijän työsuhde loppuu Netvisor KYCin osalta, hänen käyttöoikeutensa pilvipalveluihin katkeaa automaattisesti. Teemme myös säännöllisin väliajoin tarkastuksen työntekijöiden oikeuksiin eri palveluissa.

* * *

Kysymys: Miten Netvisor KYCiin kirjautuminen käytännössä tapahtuu, ovatko salasanat suojattuja?

Vastaus: Netvisor KYC-palvelun käyttämät salasanat ovat suojattu käyttäen hashing-menetelmiä ja kirjautuminen on aina kaksivaiheinen 2FA. Jos käyttäjällä on käytössä AD-kirjautuminen (käyttäen Microsoft Entra ID:tä), vastaa asiakkaan oma IT käytänteistä, joita käyttäjältä vaaditaan, jotta kirjautuminen voidaan toteuttaa.

* * *

Kysymys: Miten on määritelty vastuukysymykset ja korvausvelvollisuus tilanteessa, jossa Netvisor KYC-palvelun saatavuus tai suorituskyky on alentunut?

Vastaus: Netvisor KYC-palvelulla ei ole yleisiä SLA-lupauksia tai niihin pohjautuvia korvauksia. Korvausasiat käsitellään Netvisor KYC:n yleisten sopimusehtojen mukaisesti.

* * *

Kysymys: Kolmas osapuoli edellyttää meiltä erillisselvitystä tai sertifiointia Netvisor KYC-palvelun toiminnan osalta. Voimmeko toteuttaa palvelusta auditoinnin käyttötarkoitusta varten?

Vastaus: Visma -konsernin toteuttamat teknologia- ja tietoturvaohjelmat ovat alan standardien ja nykyajan vaatimusten mukaan suunnitellut ja kattavat vaativimpienkin asiakkaidemme tarpeet. Käymme mielellämme kanssanne läpi tietoturvaohjelmaamme tarkemmin ja suosittelemme perehtymään ohjelmien sisältöön [Visma Trust Centerissä](#) varmistaaksenne kattavuuden myös omiin tarpeisiinne. Emme lähtökohtaisesti tarjoa toistaiseksi asiakkaille teknistä ympäristöä kolmannen osapuolen auditointia (esim. penetraatiotestausta) varten, mutta voimme pyynnöstä toimittaa edellisen palveluun tehdyn penetraatiotestauksen raportin tiivistelmän.

* * *

6. Lisätiedot

Lisätietoa Visman ja Netvisor KYC tietoturvaan ja tietosuojaan liittyen löytyy seuraavista linkeistä:

Netvisor KYC:n asiakastukisivusto:

<https://support.netvisorkyc.fi/>

Visma Trust Centre:

<https://www.visma.com/trust-centre/>

Visman yleinen tietosuojaseloste:

<https://www.visma.com/privacy-statement/>

Visma Solutionsin tietosuojaseloste:

<https://www.visma.fi/yritykset/visma-solutions-oy/privacystatement-vismasolutionsoy.pdf>

Netvisor KYC sopimus- ja käyttöehdot:

<https://netvisorkyc.fi/palveluehdot/>

Visma Solutionsin tietosuojavastaavan sähköpostiosoite:

privacy.solutions@visma.com

