3. Palvelun ylläpito ja valvonta

Netvisor KYCin ylläpidosta, toiminnallisuuksien kehittämisestä 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, elkä 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. Huomioittehan, 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 konsernitasoisesta 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 tietosuoja-asioissa yhteistyötä paikallisten tietosuoja- ja tietoturva-viranomaisten kanssa. Lisätietoa Visman tietosuojatyöstä löytyy osoitteesta https://www.visma.com/trust-centre/privacy.

Visma Solutionsin tietosuojavastaava:
Tietoturva- ja tietosuojajohtaja 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.

* * *