

Hallittu AI-alusta

Tietoturva, tietojen käsittely ja
vaatimustenmukaisuuskuvaus

Hallittu AI-alusta

Tietoturva, tietojen käsittely ja vaatimustenmukaisuuskuvaus

Sisällys

1.	Hallittu palvelu ja vastuunjako	3
2.	Alustan tietoturva	4
3.	Datan hallinta ja tietosuoja	5
4.	Vaatimustenmukaisuus: ISO 27001 ja NIS2	6
5.	Jatkuvuus ja häiriötilanteet	6
6.	Vastuullisuus.....	7



1. Hallittu palvelu ja vastuunjako

Magic Cloudin hallittu AI-alusta tarjoaa Suomessa tuotetun ympäristön AI-ratkaisuille. Palvelu yhdistää kielimallit, laskentakapasiteetin, oman aineiston hyödyntämiseen tarvittavat työkalut sekä käyttäjien ja resurssien hallinnan. Organisaatio voi hyödyntää AI:ta esimerkiksi tiedonhaussa, dokumenttien käsittelyssä ja omissa sovelluksissaan ilman oman alustainfrastruktuurin ylläpitoa ja huolta tietojen siirtymisestä organisaation tai Suomen ulkopuolelle.

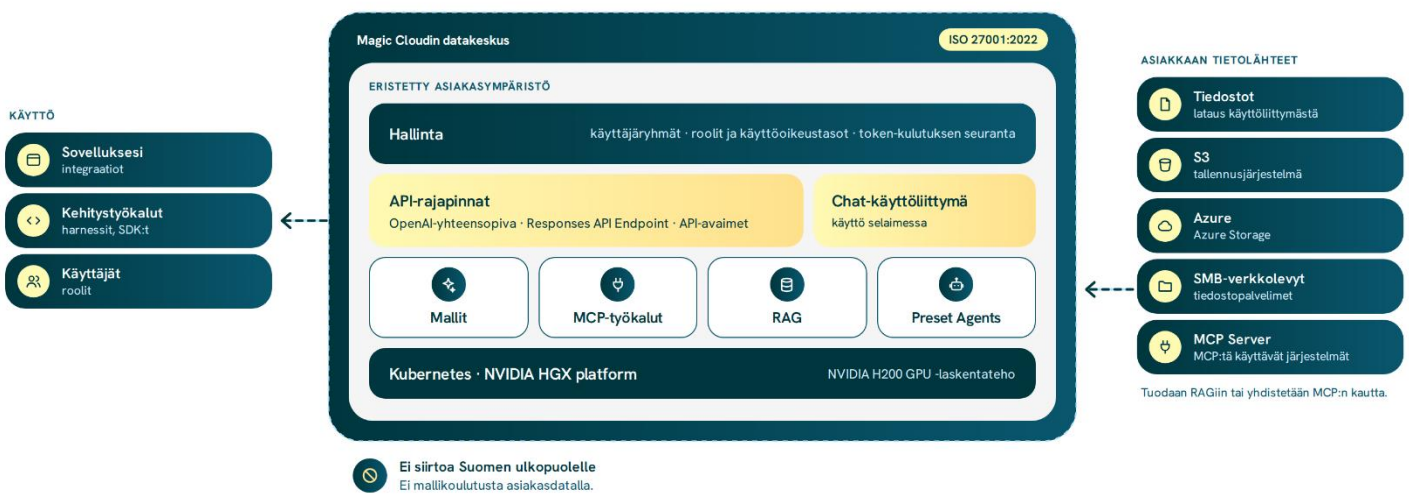
Palvelu tuotetaan Magic Cloudin omista datakeskuksista Suomesta. Magic Cloud on 100% suomalaisomistuksessa oleva yritys.

Magic Cloud vastaa alustan infrastruktuurista, teknisestä ylläpidosta, päivityksistä, haavoittuvuuksien hallinnasta, mallien elinkaaren hallinnasta sekä palvelun suorituskyvyn valvonnasta. **Asiakas** päättää käyttötarkoituksista, käsiteltävistä aineistoista ja käyttöoikeuksista sekä vastaa AI:n hyödyntämisestä omassa toiminnassaan. Tarkempi kuvaus ja palvelukohtaiset sitoumukset määritellään sopimuksessa.

Palvelukomponentti	Palvelun kuvaus
Mallit	Palvelussa käytetään eri julkaisijoiden valmiiksi kouluttamia tekoälymalleja, joista asiakas voi valita käyttötarkoitukseensa soveltuvan vaihtoehdon. Valinnassa ja käytössä huomioidaan mallin alkuperä, versio ja lisenssiehdot. Ajantasainen mallivalikoima on julkaistu Magic Cloudin verkkosivuilla. Asiakas vastaa mallin toiminnasta ja soveltuvuudesta omaan käyttöön.
Mallien elinkaaren hallinta	Magic Cloud valitsee, validoi ja ylläpitää alustan mallikirjastoa asiakkaiden käyttötapauksien sekä markkinakehityksen pohjalta. Jokainen malli validoidaan laadun, suorituskyvyn ja tietoturvan osalta ennen julkaisua. Mallien vaihtumisesta ilmoitetaan sähköpostitse asiakkaille etukäteen.
RAG	Alustan RAG-toiminnallisuus hakee asiakkaan aineistosta tietoa kielimallin vastauksen tueksi. Oman aineiston hyödyntäminen ei edellytä mallin kouluttamista asiakkaan tiedoilla. Asiakkaan aineistosta luodaan vektoritietokanta palveluun, jossa tieto päivittyy synkronointi-intervallin mukaan asiakkaan oman alkuperäisen aineiston sijainnin mukaan.
MCP	Alustan MCP-tuen (Model Context Protocol) avulla AI-ratkaisuun voidaan liittää ulkoisia järjestelmiä tietojen hakemista ja sovittujen toimintojen suorittamista varten. Pääsynhallinta toteutetaan joko OAuth-tunnisteilla tai API-avaimella.

Palvelukomponentti	Palvelun kuvaus
Sisäänrakennettu Chat	Alustan sisäänrakennettua Chatin avulla voi tehdä kyselyitä ja tallentaa keskusteluja alustalle linkitettyihin työkaluihin sekä aineistoihin. Jokaisella käyttäjällä on Chat-käyttöliittymä, jonne voi tallentaa kyselyitä.

Arkkitehtuuri



2. Alustan tietoturva

Alustan tekninen suojaus perustuu asiakasympäristöjen loogiseen eristykseen. Magic Cloud huolehtii alustan päivityksistä, haavoittuvuuksien hallinnasta ja palvelun valvonnasta osana teknistä ylläpitoa.

Tietoturvakontrolli	Toiminto
Eristys	Asiakasympäristöt ovat loogisesti eristetty toisistaan.
Alustan pääsynhallinta	Asiakas määrittelee käyttäjä-, ryhmä- ja resurssikohtaiset käyttöoikeudet malleihin, aineistoihin ja työkaluihin. API-avainten oikeuksia voidaan rajata käyttötarkoituksen mukaan.
API-avaimet	Palvelussa on rajatut API-avaimet mallien, RAGin, MCP:n ja agenttien käyttöön joko käyttäjä-,ryhmä- tai ympäristökohtaisesti.

Tietoturvakontrolli	Toiminto
Haavoittuvuuksien hallinta	Haavoittuvuuksien hallinta toteutetaan osana palvelun ylläpitoa. Magic Cloud seuraa julkisia tietoturvatiedotteita ja tunnistettuja haavoittuvuuksia sekä toteuttaa tarvittavat toimenpiteet haavoittuvuuksien korjaamiseksi.
Päivitykset	Magic Cloud suorittaa tarvittavat päivitykset (infrastruktuuritasolta sovellustasolle) alustan laadun, suorituskyvyn ja tietoturvan varmistamiseksi.

3. Datan hallinta ja tietosuoja

Asiakasdataa käsitellään vain asiakkaan eristetyssä ympäristössä Suomessa, eikä sitä käytetä AI-mallien koulutukseen.

Palvelukomponentti	Datan hallinta
Mallit	AI-alusta ja siihen liitetty kielimallit toimivat Magic Cloudin omassa, Suomessa sijaitsevassa ympäristössä. Asiakasaineistoa, käyttäjien syötteitä ja mallien vastauksia ei käytetä mallien kouluttamiseen tai hienosäätöön. Tietoja ei myöskään välitetä ulkopuolisille mallipalveluille.
Chat	Sisäänrakennetun Chatin kyselyt ja keskustelut tallentuvat käyttäjän henkilökohtaiseen chat-työkaluun. Asiakas ja käyttäjä voivat poistaa ja lisätä keskusteluita.
API-avaimet	Kolmannen osapuolen työkaluissa käytettävät promptit ja kyselyt eivät tallennu alustalle, kun alustaa käytetään API-rajapintojen kautta.
RAG	Asiakas hallinnoi tiedonhakua varten alustalle tallentamaansa aineistoa (RAG-aineisto). RAG-resurssin tai asiakasympäristön poistaminen kattaa sekä siihen tallennetun aineiston että tiedonhakua varten muodostetut tiedot. Poisto ei vaikuta lähdejärjestelmässä oleviin alkuperäisiin tietoihin.
Varmuuskopiointi	Asiakasympäristöön liittyvä työkalujen käyttö, käyttäjät, käytön seuranta sekä chatin keskustelut varmuuskopioidaan.

Kun asiakas toimii rekisterinpitäjänä, Magic Cloud käsittelee henkilötietoja asiakkaan lukuun henkilötietojen käsittelysopimuksen ja asiakkaan kirjallisten ohjeiden mukaisesti.

Sopimuksessa määritellään käsittelyn sisältö ja ehdot sekä yksilöidään palveluun osallistuvat alikäsittelijät. Asiakas vastaa käsittelyn oikeusperusteesta ja siitä, että henkilötiedot ovat käyttötarkoituksen kannalta tarpeellisia. Magic Cloud avustaa asiakasta rekisteröityjen oikeuksien toteuttamisessa ja tarvittaessa tietosuojaa koskevassa vaikutustenarvioinnissa käsittelysopimuksen ja yleisen tietosuojaa-asetuksen (GDPR) mukaisesti.

4. Vaatimustenmukaisuus: ISO 27001 ja NIS2

ISO/IEC 27001:2022 ja tietoturvan hallinta

Magic Cloudin ISO/IEC 27001:2022-sertifioitu tietoturvallisuuden hallintajärjestelmä kattaa datakeskus- ja pilvipalvelut tukitoimintoihin ja -prosesseihin. Tietoturvan ylläpitoa ja kehittämistä ohjaavat riskien arviointi ja käsittely. Hallintajärjestelmän toimintaa arvioidaan säännöllisillä sisäisillä auditoinneilla, johdon katselmuksilla sekä riippumattoman sertifiointielimen auditoinneilla.



NIS2

Magic Cloudin tietoturvan hallinta, jatkuvuusmenettelyt ja poikkeamien käsittely tukevat asiakkaan riskienhallintaa ja palveluntarjoajan arviointia. Ne tukevat myös NIS2-sääntelyn vaatimusten täyttämistä silloin, kun asiakas kuuluu sen soveltamisalaan. Magic Cloud ja asiakas vastaavat kumpikin omaan toimintaansa soveltuvista lakisääteisistä velvoitteista.

AI Act ja käyttötapauksen arviointi

EU:n AI-asetuksen (AI Act) vaatimukset määräytyvät käyttötarkoituksen, riskiluokan ja osapuolten roolien perusteella. Magic Cloud vastaa alustapalvelun tarjoamiseen soveltuvista velvoitteistaan. Asiakas arvioi omaan käyttötapaukseensa liittyvät vaatimukset ja huolehtii henkilöstönsä perehdyttämisestä, AI-osaamisen kehittämisestä sekä käyttötapauksen edellyttämästä ihmisen valvonnasta ja AI:n käytön läpinäkyvyydestä.

5. Jatkuvuus ja häiriötilanteet

Datakeskusten kriittinen infrastruktuuri on kahdennettu. Tarkempi kuvaus datakeskuksestamme löytyy [täältä](#). Häiriötilanteissa Magic Cloud rajoittaa häiriön vaikutuksia, huolehtii palvelun palauttamisesta ja tiedottaa asiakkaalle sovitun toimintamallin sekä soveltuvan lainsäädännön mukaisesti. Poikkeamat ja korjaustoimet dokumentoidaan.

Magic Cloud ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta. NIS2-direktiivin mukaisesti ensi-ilmoitus tapahtuu 24 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.

Merkittävistä poikkeamista ja kyberuhkista ilmoittamisessa noudatetaan myös soveltuvia kyberturvallisuuslain velvoitteita.

Magic Cloudin tekninen tukipalvelu palvelee asiakkaita arkisin klo 8-16 välillä.

6. Vastuullisuus



Magic Cloud käyttää 100-prosenttisesti uusiutuvaa sähköä ja kehittää palvelutuotantonsa energiatehokkuutta sekä laitteiden vastuullista elinkaarenhallintaa. Ympäristötyötä ohjaa Ekokompassi-sertifioitu ympäristöjärjestelmä, jonka tavoitteiden toteutumista seurataan säännöllisesti. Toimintaa arvioidaan riippumattomissa ulkoisissa auditoinneissa. Kehittämistoimien kohdentamista tukee vuosittainen hiilijalanjälkilaskenta, jonka ulkopuolinen taho toteuttaa GHG Protocol -standardin mukaisesti.

Asiakas voi vaikuttaa AI:n käytön resurssitarpeeseen valitsemalla tehtävän vaativuutta vastaavan mallin ja mitoittamalla käytön tarpeen mukaan. Asiakas voi myös hyödyntää Magic Cloudin julkaisemia vastuullisuustietoja omassa raportoinnissaan ja hankintapäätöksensä tukena. Tarkempia tietoja ympäristötyöstä ja hiilijalanjälkilaskennan tuloksista toimitetaan pyydettäessä.

