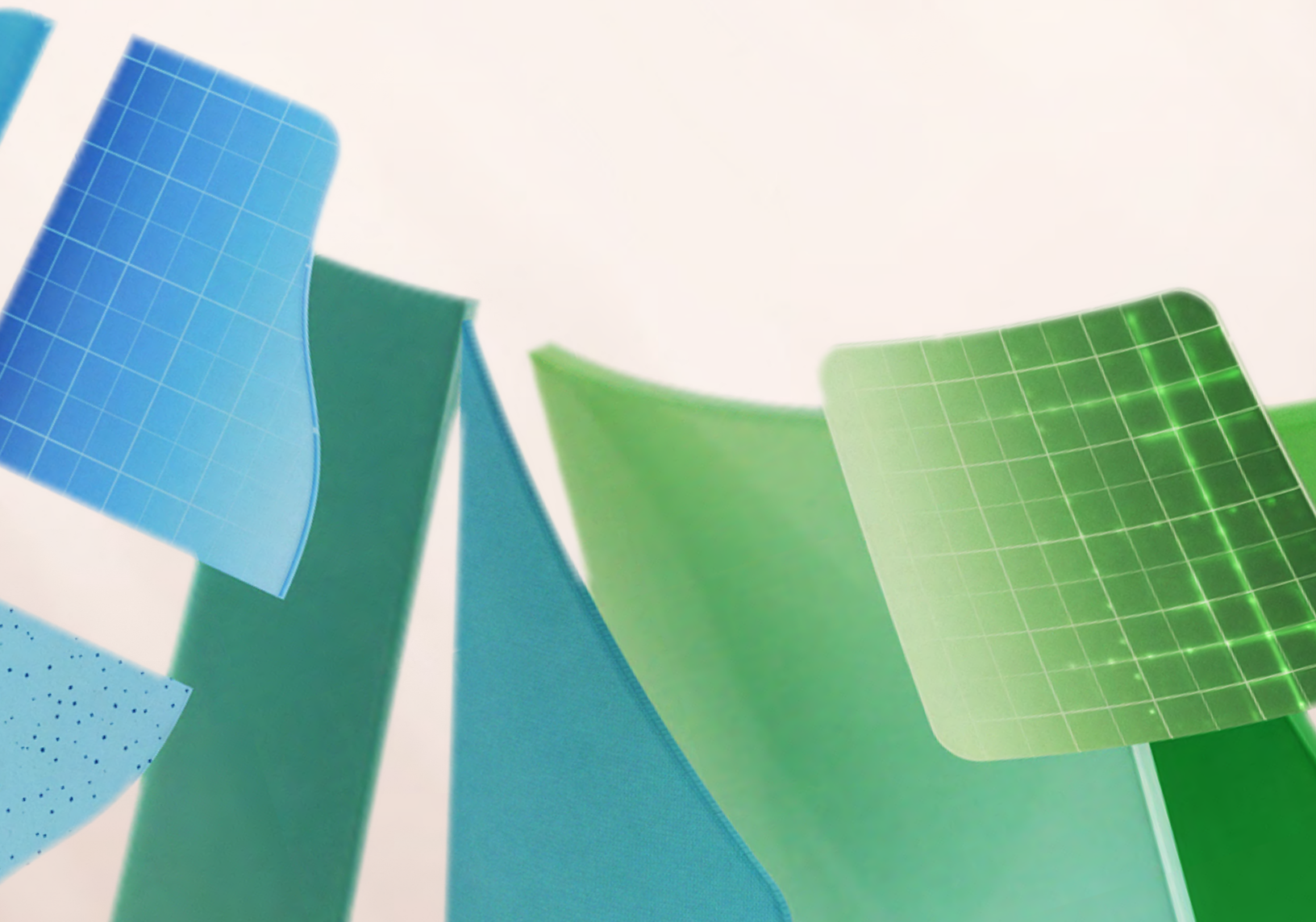


Data mallillaan

Tehokas datahallinnointi tekoälymenestystä varten



Sisältö

Johdanto

Datan hallinnointi on tekoälyn turvallisen omaksumisen perusta

Generatiivinen tekoäly voi uudistaa liiketoimintasi – mutta sen hyödyntäminen riippuu yrityksesi datan laadusta ja käytettävyydestä.

Organisaatiot, jotka pitävät vahvaa datanhallintaa etusijalla, saavat kilpailuetua tekoälyn avulla. Datan hallinnointi auttaa varmistamaan, että tekoälyn kyselyissä käyttämä ja tuottama data on oikeanlaista, suojattua, kontrolloitua ja vaatimustenmukaista.

Datan laatu ja käytettävyys:

Tekoälyjärjestelmät tukeutuvat suuriin korkealaatuisiin datajoukkoihin voidakseen tarjota parhaan mahdollisen vastauksen organisaatiosi ainutlaatuisten työkulkujen kontekstissa. Datan parempi laatu johtaa tehokkaampiin tekoälypohjaisiin oivalluksiin ja ennusteisiin.

Vaatimustenmukaisuus: Vankka datanhallinta varmistaa sääntöjen noudattamisen, mikä pienentää oikeudellisten ongelmien ja sakkojen riskiä.

Tietoturva: Oikeaoppiset datatunnisteet ja hallinta suojaavat arkaluontoista tietoa luvattomalta käytäntöä, sopimattomalta jakamiselta ja tietomurroilta.

Luottamus: Luotettava datahallinnointi vahvistaa sidosryhmien luottamusta tekoälyn tuotoksiin, mikä puolestaan edistää tekoälyhankkeiden laajempaa omaksumista ja tukea.

Tämä e-kirja esittelee kriittisiä datanhallintakäytäntöjä, jotka tekevät organisaatiosta tekoälyvalmiin. Se esittelee, kuinka luodaan tiukat datan laatuvaatimukset, varmistetaan vaatimustenmukaisuus säännösten kanssa sekä toteutetaan datan suojaukseen ja tietoturvaan liittyvät toimenpiteet. Olipa kyse arkaluontoisen kokousmateriaalin asiaankuulumattoman jakamisen estämisestä tai tietovuodoilta suojautumisesta, opit strategioita, joilla voit edistää luottamusta tekoälyjärjestelmiin ja tehdä datasta helposti käytettävää käytännönläheisen analytiikan tuottamiseksi. Näitä käytäntöjä omaksumalla organisaatiosi voi hyödyntää tekoälyn koko potentiaalia jatkuvassa innovoinnissa ja kilpailuetujen saavuttamisessa.

Generatiivisen tekoälyn käyttötapaukset

Viestinnän nopeuttaminen: Laadi personoitua sisältöä nopeammin ja vapauta aikaa suhteiden luomiseen ja yhteistyöhön.

Tehokkuuden parantaminen: Vähennä rutiinitehtäviin käytettyä aikaa, lisää tuottavuutta ja pienennä kustannuksia.

Innovaatioiden mahdollistaminen: Auta generoimaan ideoita ja ehdotuksia uusista tuotteista ja palveluista.

Asiakaskokemusten personointi: Mukauta sisältöä ja suosituksia lisätäkseen asiakasuskollisuutta ja -vuorovaikutusta.

1 Datahallinnon vahvistaminen tekoälytransformaatiota varten

Jokaisella yrityksellä on datan käyttöä koskevia käytäntöjä ja prosesseja. Datan hallinnointikehykset vaihtelevat maturiteetiltaan ja kattavuudeltaan, mutta vain harvat on täysin optimoitu tekoälyä varten. Vaikka monet datahallinnon parhaat käytännöt pysyvät samoina – esimerkiksi datan tarkkuuden ja yhdenmukaisuuden varmistaminen – tekoälyinvestointien maksimoimiseksi muita osa-alueita tulee päivittää. Tarkastellaanpa muutamia keskeisiä alueita.

Datan näkyvyys

Tekoälyjärjestelmien datavirtojen yksityiskohtainen tietämys mahdollistaa luvattoman tai sopimattoman käytön havaitsemisen ja vähentämisen. Tämä näkyvyys tukee tietoturvaa ja vaatimustenmukaisuutta, suojaten arkaluontoista dataa tekoälyn lisäarvon maksimoimiseksi.

Perinteinen datahallinnointi on keskittynyt datan sijaintien selvittämiseen ja käyttöoikeuksien hallintaan. Kuitenkin, kun tekoäly integroituu yhä enemmän liiketoimintaan, datahallinnon on

pysyttävä kehittyvien tietoturvatarpeiden tasalla. Esimerkiksi erittäin arkaluontoisen tuotteen lanseerauksen yhteydessä hallinnon on nyt ulotuttava tekoälyn generoiman sisällön hallintaan. Tämä varmistaa, että tekoälyn tuottamat projektiasiakirjat, viestintä ja analytiikka ovat suojattuja. Tämä tarkoittaa suojatoimien käyttöönottoa, jotta ainoastaan valtuutetut tiimiläiset pääsevät hyödyntämään tekoälyä projektitietojen analysointiin ja yhteenvetoihin.

Lisäksi organisaatiot voivat paremmin hallita tekoälyn liittyviä toimintakustannuksia hallinnoimalla datan käsittely- ja tallennusmääriä.

Datan laatu

Tekoäly korostaa korkealaatuisen datan merkitystä, sillä huono datan laatu heikentää suoraan tekoälyn tuloksia. Kun sovellat tekoälytyökaluja yrityksesi datakyselyissä, on syytä varmistaa, että data on ajantasaista ja luotettavaa. Yhtä tärkeää on ymmärtää sellaisen datan alkuperä ja laatu, jota tiimisi käyttää omien tekoälymallien ja sovellustensa laatimiseen. Säännölliset datan auditoinnit, tiukat validointiprosessit ja ennakoiva hallinta auttavat varmistamaan datan eheyden. Keskittymällä näihin osa-alueisiin organisaatiot voivat saavuttaa luotettavia tekoälytuloksia, jotka tukevat parempaa päätöksentekoa ja innovointia.

Käyttäjien hallinta

Tekoälyn avulla käyttäjät voivat hyödyntää dataa monipuolisesti. He kommunikoivat Microsoft 365 Copilotin kaltaisten tekoälyjärjestelmien kanssa luonnollista kieltä käyttäen. Kun käyttöoikeudet ja suojaukset ovat kunnossa, tekoäly voi hyödyntää datasta (kuten tiedostoista, keskusteluista ja sähköposteista) ja ulkoisista lähteistä lisäosien avulla saatua tietoa vastauksen generointiin.

On erittäin tärkeää valvoa näissä prosesseissa käytettyä dataa, jotta tekoäly antaa oikeita ja pohjustettuja vastauksia. Alaviitteiden tai alkuperäisiin lähteisiin johtavien linkkien avulla käyttäjät voivat tarkistaa tiedot. Tämä vähentää datan väärinkäytön riskiä ja takaa säädösvaatimusten noudattamisen.

Vaatimustenmukaisuus ja eDiscovery

Tekoälyn yleistyminen tuo mukanaan uusia haasteita vaatimustenmukaisuudessa sekä eDiscoveryssä (eli oikeustapausten datankäsittelyssä). Erityisen haastavaa on tekoälyn tuottaman datan hallinta ja sopeutuminen jatkuvasti muuttuviin lakisääteisiin vaatimuksiin. Datan hallinnointimallien päivittäminen näiden haasteiden ratkaisemiseksi edellyttää kattavia käytäntöjä tekoälyn generoiman sisällön käsittelyyn. Tähän lukeutuu esimerkiksi sen varmistaminen, että tekoälyn tuottamia asiakirjoja ja viestintää seurataan, luokitellaan ja tallennetaan tietoturvallisesti. Saattaa olla tarpeen esimerkiksi päivittää käytäntöjä, jotta tekoälyn luomat sähköpostit tai raportit merkitään ja arkistoidaan asianmukaisesti myöhempiä hakuja varten.

eDiscovery-valmiuksien parantaminen tarkoittaa sellaisten tekoälytyökalujen integroimista, jotka pystyvät etsimään ja tunnistamaan tekoälyn luomaa sisältöä eri alustoilta. Muun muassa oikeudellisessa selvityksessä eDiscovery-työkalujen on pystyttävä löytämään ja noutamaan tiettyjä tekoälyn tuottamia asiakirjoja, tiivistämään merkityksellistä viestintää sekä tarjoamaan selkeät kirjausketjut vaatimustenmukaisuuden osoittamiseksi. Näiden ominaisuuksien päivittämisen myötä organisaatiot voivat hallita dataa entistä paremmin oikeudellisissa auditoinneissa ja tutkimuksissa. Näin voidaan varmistaa, että kaikki merkittävä tekoälyn tuottama tieto on saatavilla ja puolustettavissa oikeudenkäynneissä.

Datasuojaus

Tekoälyohjattujen toimintojen suojaamisen tulisi perustua Zero Trust -periaatteisiin identiteettitasolla, jolloin luvattoman pääsyn riski minimoidaan. Säännölliset päivitykset päätepisteisiin – kuten laitteisiin ja sovelluksiin – vähentävät haavoittuvuuksia, joita voidaan käyttää hyväksi. Organisaation sisällä käytössä olevien generatiivisen tekoälyn työkalujen tunteminen mahdollistaa luvattomien tai turvattomien sovellusten estämisen, mikä puolestaan ehkäisee potentiaalisia tietomurtoja. Kun vain luotetuille henkilöille annetaan pääsy tekoälytyökaluihin ja dataan, organisaatiot voivat parantaa datan eheyttä ja suojata tekoälyoperaatioitaan mahdollisilta uhilta.



Mikä on Zero Trust?

Zero Trust on tietoturvamalli, jossa jokainen pyyntö tarkistetaan ikään kuin se tulisi ei-luotetusta verkosta. Sen sijaan, että kaikki yrityksen palomuurin sisäpuolella oleva oletettaisiin turvalliseksi, tämä lähestymistapa noudattaa periaatetta "älä koskaan luota, vahvista aina".

Zero Trust -periaatteet

Nimenomainen vahvistaminen:

Todenna ja valtuuta aina kaikkien saatavilla olevien datapisteiden perusteella.

Vähäisimpien käyttöoikeuksien soveltaminen: Rajoita käyttäjien oikeuksia riskipohjaisten mukautuvien käytäntöjen ja tietosuojan avulla sekä antamalla vain tarpeelliset käyttöoikeudet vain tarvittaessa.

Tietomurron oletaminen: Rajoita vahinkoja, hallitse käyttöoikeuksia, varmista tiedon salaaminen sekä hyödynnä dataa uhkien tunnistamisessa ja puolustuksen tehostamisessa.

Datan hoitajuuden rooli tekoälytransformaatioissa: Alkuperät, laatu ja luotettavuus

Kun organisaatiot ottavat käyttöönsä tekoälyä tukemaan liiketoimintapäätöksiään, on tärkeää varmistaa, että nämä järjestelmät pystyvät tuottamaan oikeellisia ja luotettavia tuloksia. Tekoälyn vastauksia pohjustavan datan on oltava käytettävää, yhdenmukaista ja hyvin dokumentoitua.

Datan hoitajuus tukee luotettavaa tekoälyä: hallinnointikäytännöillä seurataan datan alkuperää, tarkistetaan sen laatua sekä varmistetaan luotettavuus ja tarkkuus. Nämä käytännöt luovat perustan tekoälyjärjestelmille, jotka tuottavat luotettavaa analytiikkaa ja mahdollistavat tietoon perustuvan ja luotettavan päätöksenteon.

Datan historiatiedot: Tietojen alkuperän ja muutosten ymmärtäminen

Datan historiatiedot seuraavat datan kulkua organisaatiossa. Niissä on dokumentoitu datan alkuperät, muunnokset ja määränpäätt. Tekoälyä hyödyntävien yritysten on kriittisen tärkeää ymmärtää datan historiatiedot useista syistä:

- **Läpinäkyvyys:** Datan alkuperän ja muutosten ymmärtäminen auttaa varmistamaan tekoälyn generoimien tuotosten tarkkuuden sekä takaa sääntelyn vaatimustenmukaisuuden tarjoamalla selkeän kuvan datahistoriasta.
- **Jäljitettävyys:** Datan historiatiedot mahdollistavat organisaatioille virheiden tai epäyhdenmukaisuuksien jäljittämisen niiden lähteeseen, mikä helpottaa vianmäärittystä ja datan korjaamista.
- **Vaikutusanalyysi:** Sen ymmärtäminen, kuinka dataa käytetään generatiivisen tekoälyn työkaluissa, auttaa arvioimaan, miten datalähteiden tai käsittelymenetelmien muutokset saattavat vaikuttaa tuotosten tarkkuuteen ja liiketoimintatuloksiin.

Datan laatu: Laatu määrittää tekoälyvastausten arvon

Datan laatu vaikuttaa suoraan tekoälyn tuotosten luotettavuuteen. Laadukas data luo kontekstin, jonka avulla tekoälymallit voivat tuottaa oikeita ja arvokkaita vastauksia käyttäjien syötteisiin. Datan laadun keskeisiä osa-alueita ovat:

- **Tarkkuus:** Datan tulee kuvastaa oikein todellisia olosuhteita.
- **Täydellisyys:** Kaiken tarvittavan datan on oltava saatavilla ja selvitettyä.
- **Yhdenmukaisuus:** Datan on oltava yhdenmukaista eri järjestelmissä ja ajan kuluessa.
- **Oikea-aikaisuus:** Datan on oltava ajantasaista ja käytettävissä tarpeen mukaan.

Datan luotettavuus: Luotettavan datan varmistaminen

Datan luotettavuus tarkoittaa, että data täyttää yhdenmukaisesti laatuvaatimukset ja on käytettävissä silloin kun sitä tarvitaan. Tekoälyä hyödyntäville yrityksille luotettava data on ratkaisevan tärkeää tekoälytyökalujen ja niiden ohjaamien päätösten luotettavuuden edistämiseksi. Datan luotettavuuden varmistaminen sisältää seuraavat:

- **Datan vikasietoisuus:** Sellaisten varmuuskopiointijärjestelmien käyttöönotto, jotka estävät datahävikin ja parantavat käytettävyyttä.
- **Säännölliset varmuuskopiot:** Säännölliset varmuuskopiot datan vioittumisen tai katoamisen varalta.
- **Valvonta ja hälytykset:** Valvontajärjestelmien käyttöönotto datan ongelmien havaitsemiseksi ja sidosryhmien hälyttämiseksi reaaliajassa.
- **Katastrofien jälkeiset palautumissuunnitelmat:** Datan palauttamiseen ja operatiivisen toiminnan jatkamiseen liittyvien suunnitelmien kehittäminen ja testaus disruptioiden jälkeen.

Hallinnoinnin, tietoturvan ja vastuullisen tekoälyn suhde

Yhdessä datan hallinnointi ja tietoturva muodostavat perustan vastuulliselle tekoälyn käytölle. Korkealaatuinen, tietoturvallinen data varmistaa, että tekoäly toimii eettisesti ja tehokkaasti. Keskeisiä arvioitavia osa-alueita ovat datan luokittelu, käyttöoikeuksien valvonta, salaus, tapausvaste ja sääntelyyn liittyvä vaatimustenmukaisuus.

Datan luokittelu

Datan luokittelu on olennainen osa sitä, miten tekoälytyökalut käsittelevät arkaluontoista tietoa. Tyypillisesti data ja kokoukset luokitellaan yleisiksi, luottamuksellisiksi tai erittäin luottamuksellisiksi. Asianmukainen luokittelu takaa, että tekoäly käyttää vain asianmukaisia tietoja, mikä pienentää riskiä siitä, että arkaluontoista dataa joutuisi luvottomien käyttäjien nähtäville.

Väärä luokittelu voi puolestaan johtaa siihen, että tekoäly käsittelee dataa, jota pitäisi rajoittaa. Tämä voi aiheuttaa tietoturvaloukkauksia tai vaatimustenmukaisuusongelmia. Tehokas datanhallinta – joko automatisoitujen työkalujen tai loppukäyttäjäkäytäntöjen avulla – takaa datan oikean luokittelun, suojaa arkaluontoista tietoa sekä tukee tekoälyä luotettavien ja vaatimustenmukaisten tuotosten toimituksessa.

Käyttöoikeuksien valvonta

Nämä hallintamekanismit määrittelevät, kenellä on pääsy tekoälyyn liittyvään dataan ja mitkä sovellukset tai identiteetit saavat olla vuorovaikutuksessa kyseisen datan kanssa. Heikot käyttöoikeuksien valvontamekanismit voivat johtaa arkaluontoisen tiedon luvattomaan paljastumiseen, mikä kasvattaa tietomurtojen ja väärinkäytösten riskiä.

Datahallinnointi on keskeisessä roolissa näiden hallintamekanismien toteuttamisessa. Se rajoittaa dataan pääsyn ainoastaan valtuutetuille henkilöille ja tietyille sovelluksille sekä varmistaa arkaluontoisen datan asianmukaisen käsittelyn. Tämä suojaa datan eheyttä ja varmistaa tekoälyjärjestelmien toimivan tietoturvallisilla, luotettavilla datajoukoilla, mikä parantaa niiden luotettavuutta ja vaatimustenmukaisuutta.

Salaus

Datan suojaaminen sieppaukselta ja manipuloinnilta salauksen avulla auttaa varmistamaan, että generatiivisen tekoälyn työkalut voivat pohjustaa vastauksensa oikeaan kontekstiin – esimerkiksi työhön liittyvään dataan, tiedostoihin, keskusteluihin ja sähköposteihin – ilman datavuotojen riskiä.

Datahallinnoinnin käytännöt voivat määrätä vankkoja salauskäytäntöjä, jotka suojaavat dataa sen koko elinkaaren ajan. Tämä lähestymistapa takaa, että tekoälytyökalut pystyvät antamaan luotettavia vastauksia ja ylläpitämään samalla datasi suojausta ja luottamusta.

Tapausvaste

Organisaation arkaluontoinen data voi paljastua tapauksissa, joissa generatiivisen tekoälyn työkaluilla päästään luvottomasti käsiksi tiedostoihin, sähköposteihin tai muihin yritystietoihin, joiden pohjalta vastauksia generoidaan.

Ennakoiva tapausvastesuunnitelma on ratkaisevan tärkeä näissä skenaarioissa. Ilman tällaista suunnitelmaa organisaatio ei ainoastaan aseta arkaluontoista dataa paljastumisvaaraan vaan myös tukeutuu mahdollisesti vaarallisiin tekoälytuotoksiin. Datahallinnointi sisältää yksityiskohtaisten vastausmenettelyjen käytön. Niiden avulla voidaan nopeasti puuttua tietoturvaloukkauksiin, minimoida niiden vaikutukset sekä ylläpitää tekoälyjärjestelmien luotettavuutta.

Säädösten noudattaminen

Tekoälysovellusten on noudatettava tietosuoja- ja yksityisyyttä koskevia säädöksiä, kuten EU:n yleistä tietosuoja-asetusta ja CCPA:ta. Vaatimustenmukaisuuden laiminlyönti voi johtaa merkittäviin rangaistuksiin ja luottamuksen murentumiseen. On myös olennaista ymmärtää, missä tekoälytyökalut käsittelevät dataa, sillä monet maksuttomat työkalut saattavat käsitellä dataa globaalisti tai yrityksesi tavanomaisten tallennussijaintien ulkopuolella. Datahallinnointi varmistaa, että tekoälysovellukset toimivat paitsi laillisten raamien sisällä, myös pitävät datan oikeiden palvelurajojen sisällä organisaatiosi vaatimustenmukaisuusstandardien mukaisesti. Tämä lähestymistapa tukee eettistä tekoälyn käyttöä ja edistää luottamusta tekoälyteknologiaan.



Datan hallinnointikehityksen päivittäminen tekoälyn omaksumisen tueksi

Kehittyvässä tekoäly-ympäristössä on tärkeää tunnistaa nykyisessä datanhallinnoinnin kehityksessä erityiset osa-alueet, jotka saattavat vaatia ylimääräistä huomiota. Sen sijaan, että uudistaisit koko järjestelmän, voit keskittyä osa-alueisiin, jotka todennäköisimmin kehittyvät. Näin kohdennat työpanoksesi sinne, missä se parhaiten kasvattaa tekoälyn lisäarvoa, ja samalla varmistat datasi tietoturvan. Seuraavassa on näkökohtia, joihin kannattaa miettiä vastauksia:

Käytäntöjen ja toimintatapojen mukauttaminen

Tekoälyyn liittyy uudenlaista datankeruuta, -käsittelyä ja -käyttöä. Datakäytäntöjen päivittäminen voi auttaa vastaamaan tietosuojaa, sääntelyn vaatimusten-mukaisuutta ja eettistä käyttöä koskeviin tarpeisiin. Esimerkiksi datan anonymisointi tietyissä tapauksissa voi suojata henkilötietoja ja tehdä niiden käytöstä turvallisempaa tekoälyn koko elinkaaren ajan.

Tehtävät ja vastuut

On välttämätöntä sisällyttää tekoälyvalmius kaikkiin datahallintaan liittyviin rooleihin. Tekoälyn datavaatimuksiin perehtyneet työntekijät voivat toimia hoitajina, jotka tukevat datan laatua ja vaatimustenmukaisuutta. Toimintojen välinen yhteistyö lakiosasto-, IT- ja datatiedetiimien kesken voi auttaa ratkaisemaan tekoälyyn liittyviä haasteita tehokkaammin.

Datastandardien ja -määritelmien mukauttaminen

Dataformaattien, määritelmien ja laatumittareiden standardointi helpottaa tekoälytyökalujen käyttöä ohjaavien organisaatiotason käytäntöjen toteuttamista. Selkeät datastandardit tekevät helpommaksi päätellä, mistä datajoukoista tekoälytyökalut voivat tehdä päätelmiä liiketoimintakontekstin tarjoamiseksi ja minkälaista dataa käyttäjät voivat ladata analysointia varten. Tämä takaa, että tekoälysovellukset hyödyntävät merkityksellisintä ja luotettavinta dataa, mikä lisää niiden tehokkuutta ja tukee organisaation käytäntöjen noudattamista.

Jatkuva kehittyminen

Datahallinnointi on jatkuva prosessi erityisesti tekoälyn yhteydessä. Säännöllinen hallintorakenteesi auditointi ja päivittäminen voi auttaa mukautumaan tekoälyn uusiin kehityskulkuihin ja sääntelyn muutoksiin. Tekoälyä voidaan käyttää hallinnointikäytäntöjen tarkistamiseen ja tehostamiseen sekä mahdollisten puutteiden löytämiseen ja parannusten ehdottamiseen. Tämä proaktiivinen lähestymistapa parantaa vaatimustenmukaisuutta ja tehokkuutta tekoälytekniikoiden kehittyessä.

Tehokkaan datahallinnoinnin työkalut ja tekniikat

Mukauttaminen liiketoimintatavoitteisiin:

Varmista, että datahallinnoinnin strategiasi tukee organisaation pyrkimyksiä parantaa päätöksentekoa ja tehokkuutta.

Rutiinitehtävien automatisointi:

Hyödynnä automaatiota toistuvissa tehtävissä, kuten datan luokittelussa ja käyttöoikeuksien hallinnassa, jotta vähennät manuaalisia virheitä ja parannat tietoturvaa.

Korkeiden tarkkuusstandardien

varmistaminen: Käytä validointi- ja puhdistustyökaluja datan eheyden ylläpitämiseksi ajan mittaan.

Käyttäjien koulutus:

Tarjoa datanhallinnointityökalujen ja -menetelmien koulutusta estääksesi hallinnan ongelmia ja varmistaaksesi käytäntöjen noudattamisen.

Säännölliset auditoinnit:

Tarkista säännöllisesti datan käsittelytavat, jotta voit varmistaa niiden pysyvän ajan tasalla sääntely- ja organisaatiomuutoksissa.

Loppusanat

Tehokas datanhallinta tekoälyvalmiuksien parantamiseksi Microsoft 365:llä

Tekoälyn vastuullinen käyttö edellyttää vankkaa datahallinnointia. Tehokas datahallinnointi takaa datan käytettävyyden, tarkkuuden ja tietoturvan, minkä ansiosta tekoäly voi tarjota luotettavaa analytiikkaa ja edistää innovointia. Datat laadun, vaatimustenmukaisuuden ja tietoturvan asettaminen etusijalle parantaa tekoälyn valmiuksia, tukee parempaa päätöksentekoa sekä pitää yllä kilpailuetua.

Microsoft 365: Tehosta tekoälyvalmiuttasi

Microsoft 365 tarjoaa alan parhaita tuottavuussovelluksia, joissa on sisäiset työkalut datan luokitteluun, hallintaan ja suojaamiseen. Nämä ominaisuudet tukevat datan hallinnointikehystäsi ja edesauttavat tekoälyn itsevarmaa käyttöönottoa, kun olet siihen valmis. Microsoft 365 auttaa sinua varmistamaan seuraavat:

- **Datan laatu:** Tekoälyn tuotosten tarkkuus ja luotettavuus.
- **Vaatimustenmukaisuus:** Sääntelyvaatimusten noudattaminen ja oikeudellisten riskien vähentäminen.
- **Zero Trust -tietoturva:** Arkaluontoisten tietojen suojaaminen luvattomalta käytöltä, tietomurroilta ja kyberuhilta.

Tutustu vankkaan suojaukseen sekä tekoälyllä parannettuihin ja kattaviin tuottavuustyökaluihin, jotka auttavat organisaatiotasi toimimaan tehokkaasti ja tietoturvallisesti.



Tutustu Microsoft 365:een