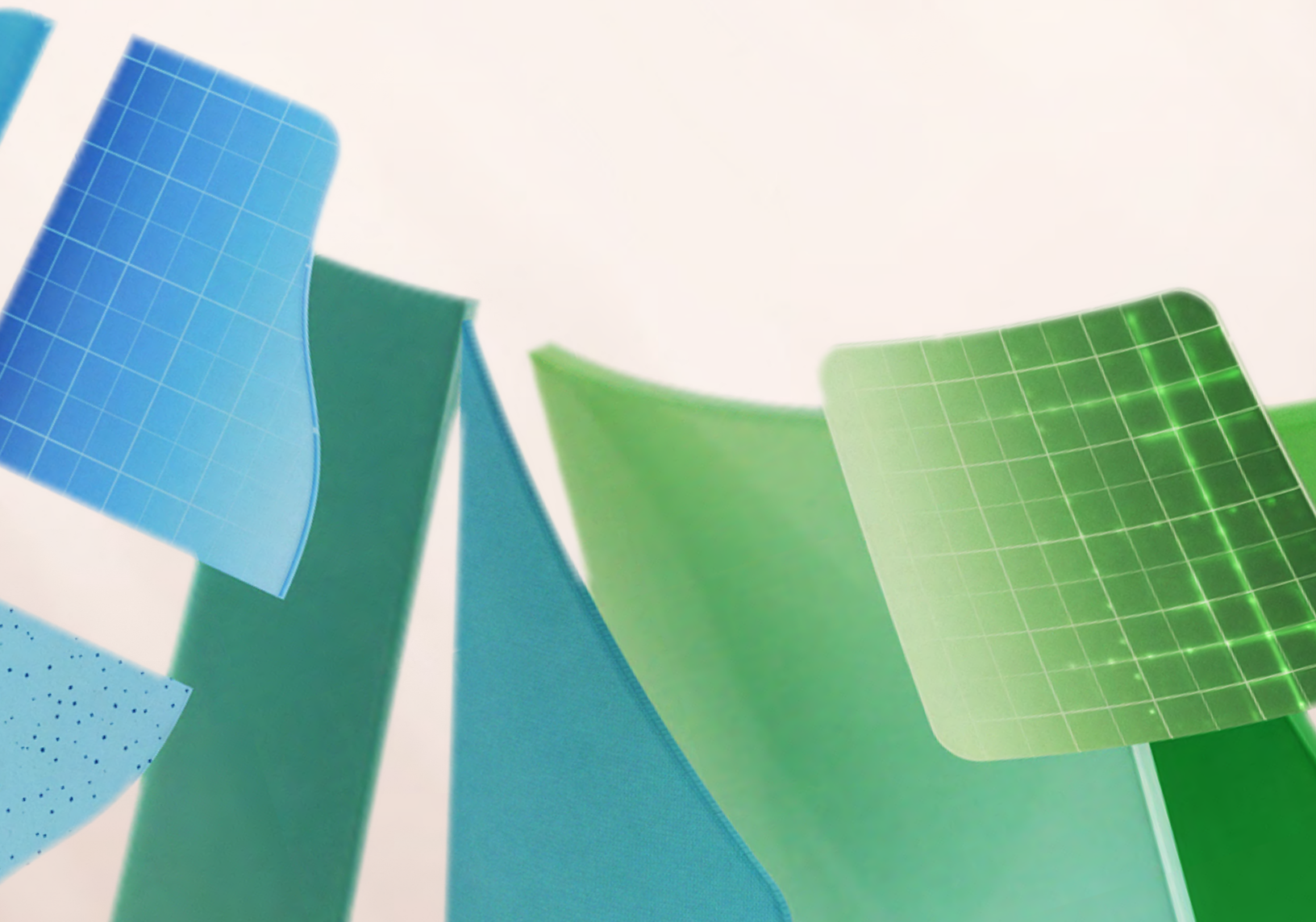


Håll koll på data

Datastyrning för en lyckad AI-strategi



Innehåll

Inledning

Datastyrning är den säkra AI-användningens ryggrad

Generativ AI erbjuder förutsättningarna för företagsomvandling – men för att utnyttja dess potential behöver data vara tillgängliga och högkvalitativa.

Organisationer som prioriterar en god datastyrningsstrategi kan skaffa sig konkurrensfördelar med hjälp av AI. Datastyrning säkerställer att data som frågas och genereras av AI är korrekta, säkra, kontrollerade och uppfyller efterlevnadskrav.

Datakvalitet och tillgänglighet:

För att kunna generera bra svar behöver AI-systemen tillgång till stora, högkvalitativa datauppsättningar med sammanhangsinformation från organisationens unika arbetsflöden. Ju högre datakvalitet, desto effektivare AI-insikter och förutsägelser.

Efterlevnad: En god datastyrningsstrategi säkerställer att lagar och andra föreskrifter efterlevs, vilket minskar risken för juridiska problem och företagsböter.

Säkerhet: Rätt etikettering och hantering av data bidrar till att skydda känslig information från obehörig åtkomst, olämplig delning och läckor.

Tillit: Tillförlitlig datastyrning ökar intressenternas tillit till AI-systemens utdata, vilket främjar en mer utbredd användning och ett ökat stöd för AI-initiativ.

I den här e-boken presenteras viktiga datastyrningsmetoder som gör din organisation AI-redo. Vi tar upp hur man implementerar robusta datakvalitetsstandarder, säkerställer efterlevnad av lagar och andra föreskrifter och inför åtgärder för dataskydd och säkerhet. Från att förhindra hemligt mötesinnehåll från att spridas externt till att skydda organisationen mot dataläckor – du får lära dig om strategier för att öka tilliten till AI-system och tillgängliggöra data för att skapa användbara insikter. Med hjälp av de här metoderna kan din organisation utnyttja AI-teknikens fulla potential för att främja kontinuerlig innovation och konkurrenskraft.

Användningsfall för generativ AI

Accelerera kommunikationen:

Skriv personligt innehåll snabbare och frigör tid för nätverkande och samarbete.

Öka effektiviteten: Lägg mindre tid på rutinarbete, öka produktiviteten och minska kostnaderna.

Främja innovation: Skapa nya idéer och förslag till produkter och tjänster.

Personanpassa

kundupplevelserna: Skräddarsy innehåll och rekommendationer för att öka kundlojaliteten och engagemanget.

Stark datastyrning för AI-omvandling

Alla företag har policyer och processer som styr dataanvändning. Datastyrningsramverken varierar i mognad och omfattning, men få är optimerade för AI-tekniken. Många datastyrningsmetoder – som att se till att data är korrekta och konsekventa – förändras inte, men andra behöver uppdateras om man vill kunna maximera värdet av sina AI-investeringar. Vi ska titta närmare på ett par viktiga områden.

Datasynlighet

För att hitta och åtgärda obehörig eller olämplig dataanvändning behöver man ha detaljerad kunskap om dataflödet i AI-systemen. Insyn är grunden till säkerhet och efterlevnad, så att känsliga data är skyddade och värdet av AI-investeringen kan maximeras.

Traditionellt sett har fokus för datastyrning legat på att veta var data finns lagrade och hur åtkomsten kontrolleras. Men när AI i allt större omfattning integreras i verksamheten måste strategin för datastyrning anpassas till nya säkerhetskrav. Exempel: Under en känslig

produktlansering måste styrningsstrategin nu också omfatta hanteringen av AI-genererat innehåll, så att AI-genererade dokument, meddelanden och insikter om projektet skyddas. Det innebär att man måste införa skyddsåtgärder som säkerställer att endast behöriga medarbetare kan komma åt och använda AI-systemen för att analysera eller sammanfatta projektinformation.

Genom att hantera databehandlings- och lagringsvolymerna på ett korrekt sätt får organisationer dessutom bättre koll på kostnaderna som är förknippade med AI-tekniken.

Datakvalitet

AI gör det ännu viktigare med högkvalitativa data, då låg datakvalitet direkt påverkar AI-utdata. När man använder AI-verktyg för att fråga företagsdata vill man ha data som är aktuella och tillförlitliga. Lika viktigt är det att veta vad de data som teamen använder för att bygga egna AI-modeller och program har för ursprung och kvalitet. Regelbunden datagranskning, strikta valideringsprocesser och proaktiv hantering bidrar till att upprätthålla dataintegriteten. Genom att lägga fokus på de här områdena kan organisationer uppnå tillförlitliga AI-resultat som främjar innovation och ett bättre beslutsfattande.

Användarhantering

Med AI-teknik interagerar användarna med data på ett sofistikerat sätt. De kommunicerar med AI-system som Microsoft 365 Copilot med frågor på naturligt språk. När lämpliga behörigheter och skyddsåtgärder införts kan AI-tekniken komma åt relevant sammanhang från data för att generera svar, såsom filer, chattar och e-postmeddelanden. Även externa källor kan nås via plugin-program.

Det är viktigt att övervaka de data som används i de här processerna för att se till att AI producerar korrekta, väl underbyggda svar. Tack vare fotnoter och länkar till källor kan användarna verifiera informationen – vilket ökar transparensen, minskar risken för datamissbruk och säkerställer att lagar och andra föreskrifter efterlevs.

Efterlevnad och eDiscovery

AI skapar nya utmaningar i fråga om efterlevnad och datahantering i juridiska ärenden (eDiscovery), särskilt vad gäller hanteringen av AI-genererade data och anpassningen till nya juridiska krav. För att uppdatera datastyrningsramverket så att det kan hantera sådana utmaningar måste man utveckla policyer som omfattar AI-genererat innehåll, till exempel genom att se till att AI-producerade dokument eller meddelanden spåras, kategoriseras och lagras på ett säkert sätt. Företagspolicyer kan till exempel behöva uppdateras så att AI-genererade e-postmeddelanden och rapporter taggas och arkiveras för framtida bruk på korrekt sätt.

För att förbättra eDiscovery-funktionerna behöver man integrera AI-verktyg som kan söka efter och identifiera AI-genererat innehåll på olika plattformar. Under en rättsutredning måste eDiscovery-verktyg exempelvis kunna hitta och hämta specifika dokument, sammanfatta relevant kommunikation och skapa tydliga granskningskedjor för att påvisa efterlevnad. Genom att uppgradera de här funktionerna underlättar organisationer för juridiska undersökningar och utredningar, så att all relevant AI-genererad information finns tillgänglig och kan användas i juridiskt syfte.

Datasäkerhet

Att skydda en AI-driven verksamhet bör innefatta tillämpningen av Zero Trust-principer på identitetsnivå för att minimera risken för obehörig åtkomst. Regelbundna uppdateringar av slutpunkter, inklusive enheter och program, minskar förekomsten av sårbarheter som kan komma att utnyttjas. Kunskap om vilka verktyg för generativ AI som används inom organisationen gör att osanktionerade och osäkra program kan blockeras, vilket i sin tur motverkar risken för säkerhetsöverträdelser. Genom att begränsa åtkomsten till AI-verktyg och data till betrodd personal kan organisationer uppnå högre dataintegritet och skydda AI-verksamheten från potentiella hot.



Vad är Zero Trust?

Zero Trust är en säkerhetsmodell som bygger på att varje åtkomstbegäran verifieras som om den kom från ett icke betrott nätverk. I stället för att anta att allt inom företagets brandväggar är säkert, tillämpar metoden principen "lita aldrig på någon eller något, verifiera alltid".

Zero Trust-principer

Verifiera explicit: Autentisera och auktorisera alltid utifrån alla tillgängliga datapunkter.

Använd åtkomst med minsta möjliga behörighet: Begränsa användaråtkomsten med JIT/ETA-riskbaserade (Just-In-Time and Just-Enough Access) adaptiva policyer och dataskydd.

Förutsätt att en överträdelse har skett: Begränsa omfattningen av skador, kontrollera åtkomsten, använd kryptering och utnyttja data till att upptäcka hot och stärka försvaret.

Dataförvaltningens roll i AI-omvandlingen: ursprung, kvalitet och tillförlitlighet

När organisationer inför AI som stöd i beslutsfattandet måste systemen kunna generera korrekta och tillförlitliga resultat. De data som AI-svaren baseras på måste vara lättillgängliga, konsekventa och väldokumenterade.

God dataförvaltning främjar AI-utdatas trovärdighet eftersom styrningspolicyer spårar datas ursprung, kontrollerar dess kvalitet och säkerställer dess tillförlitlighet och korrekthet. De här metoderna skapar ett AI-system som genererar tillförlitliga insikter och möjliggör väl underbyggda och tydliga affärsbeslut.

Dataursprung: Förstå ursprunget och ändringar av information

Dataursprung är processen att spåra informationens resa genom organisationen. Det innebär att man dokumenterar dataursprung, omvandlingar och datadestinationer. Det är viktigt för AI-drivna företag att förstå datas ursprung av flera skäl.

- **Transparens:** Att känna till datas ursprung och eventuella ändringar gör det lättare att verifiera AI-genererade utdata, och en tydligare bild av datahistoriken säkerställer efterlevnad.
- **Spårbarhet:** Dataursprung gör det möjligt för organisationer att spåra källan till fel eller inkonsekvenser, vilket förenklar felsökning och korrigering.
- **Konsekvensanalys:** Att förstå hur data används av verktygen för generativ AI underlättar bedömningen av vilka effekter förändringar i datakällor och databehandlingsmetoder kan ha på utdatas korrekthet och företagsresultat.

Datakvalitet: Kvaliteten är avgörande för AI-svarens värde

Datakvaliteten påverkar direkt AI-utdatas tillförlitlighet. Högkvalitativa data ger AI-modellerna ett sammanhang, så att de kan leverera korrekta och användbara svar på användarnas frågor. Viktiga aspekter av datakvalitet är:

- **Korrekthet:** Data måste presentera verkliga förhållanden på ett korrekt sätt.
- **Fullständighet:** Alla nödvändiga uppgifter måste finnas där och redovisas.
- **Konsekvens:** Data måste vara konsekventa i olika system och över tid.
- **Snabbhet:** Data måste vara uppdaterade och tillgängliga när de behövs.

Datatillförlitlighet: Säkerställ att data är trovärdiga

Tillförlitlighet betyder att data alltid uppfyller vissa kvalitetsstandarder och är tillgängliga när de behövs. För AI-drivna verksamheter är tillförlitliga data viktiga för att främja en ökad tillit till AI-verktygen och de beslut de underbygger. Att säkerställa att data är tillförlitliga innebär bland annat:

- **Dataredundans:** Införa system för säkerhetskopiering som förhindrar dataförlust och ökar tillgängligheten.
- **Regelbunden säkerhetskopiering:** Utför säkerhetskopiering ofta för att förhindra datakorruption och förlust.
- **Övervakning och aviseringar:** Implementera övervakningssystem som identifierar problem med data och varnar intressenter i realtid.
- **Katastrofåterställningsplaner:** Utveckla och testa planer för att återställa data och snabbt återuppta verksamheten efter störningar.

Förhållandet mellan styrning, säkerhet och ansvarsfull AI

Tillsammans utgör datastyrning och säkerhet den ansvarsfulla AI-användningens ryggrad. Säkra, högkvalitativa data gör att AI jobbar effektivt och etiskt. Viktiga områden som bör utvärderas är dataklassificering, åtkomstkontroller, kryptering, incidentåtgärder och efterlevnad.

Dataklassificering

Dataklassificering är en viktig del av arbetet för att kontrollera hur AI-verktyg hanterar känslig information. Data och möten klassificeras oftast som "allmänt", "konfidentiellt" eller "mycket konfidentiellt". Om klassificeringen är korrekt får AI endast tillgång till lämplig information, vilket minskar risken för att obehöriga användare ska få åtkomst till känslig information.

Felaktig klassificering kan göra att AI behandlar data som borde varit avskärmd, vilket kan leda till säkerhetsöverträdelser och efterlevnadsproblem. Effektiv datastyrning med automatiserade verktyg eller slutanvändarpolicyer säkerställer att data är klassificerade på rätt sätt. Då skyddas känslig information, och AI-verktygens förmåga att leverera tillförlitliga utdata i enlighet med gällande lagar och föreskrifter främjas.

Åtkomstkontroller

Dessa kontroller avgör vem som kan komma åt AI-relevanta data, samt vilka program och identiteter som har behörighet att interagera med dem. Bristfällig åtkomstkontroll kan leda till att känslig information delas med obehöriga och ökar risken för dataläckor och datamissbruk.

Datastyrning upprätthåller åtkomstkontrollen genom att begränsa åtkomst till behöriga medarbetare och särskilda program, så att känsliga data hanteras på ett lämpligt sätt. Det gör att dataintegriteten skyddas och att AI-systemens datauppsättningar förblir säkra och betrodda – vilket ökar tillförlitligheten och säkerställer efterlevnad.

Kryptering

När data är krypterade som skydd mot avlyssning och manipulering kan verktygen för generativ AI grunda sina svar i rätt sammanhang – till exempel arbetsrelaterade data, filer, chattar och e-postmeddelanden – utan att riskera att en dataläcka sker.

Datastyrningspolicyer kan vara grunden till robusta krypteringsmetoder som skyddar data under hela livscykeln. Att använda den här metoden gör att verktygen för generativ AI kan leverera tillförlitliga svar, samtidigt som data skyddas och systemens trovärdighet upprätthålls.

Incidentsvar

Känsliga organisationsdata kan råka exponeras i incidenter med verktyg för generativ AI som ger obehöriga användare åtkomst till filer, e-postmeddelanden eller andra företagsdata som systemen använder för att generera svar.

I de här fallen är en proaktiv incidentsvarsplan avgörande. Utan en sådan riskerar organisationen inte bara att läcka konfidentiella data, utan också att förlita sig på felaktiga AI-utdata. Datastyrning innebär att ha detaljerade svarsprotokoll för att snabbt kunna åtgärda dataläckor, minimera dess konsekvenser och upprätthålla tilliten till AI-systemen.

Efterlevnad

AI-program måste respektera lagar och andra föreskrifter som reglerar dataskydd och sekretess, till exempel GDPR och CCPA. Bristande efterlevnad kan leda till allvarliga påföljder och urholka tilliten till tekniken. Det är också viktigt att veta var AI-verktygen behandlar data, då många kostnadsfria verktyg hanterar dem globalt eller utanför företagets vanliga lagringsplatser. Med en god datastyrningsstrategi kan du säkerställa att AI-program inte bara respekterar de juridiska ramarna utan också hanterar data inom rätt tjänstegränser, i linje med organisationens efterlevnadsstandarder. Den här metoden främjar en etisk AI-användning och ökar tilliten till tekniken.



4

Uppdatera ramverket för datastyrning för att underlätta införandet av AI-teknik

I den föränderliga AI-världen är det viktigt att identifiera vilka områden i ditt befintliga datastyrningsramverk som kan kräva extra uppmärksamhet. I stället för att stöpa om hela ramverket kan du fokusera på de områden där utvecklingen går som fortast, och riktade insatser för att skydda data kan förhöja värdet av AI-tekniken som mest. Här är några viktiga punkter att beakta:

Anpassa policyer och procedurer

AI medför nya typer av datainsamling, behandling och användning. Genom att uppdatera organisationens datapolicyer kan du tillgodose behovet av sekretess, efterlevnad och etisk användning. Till exempel kan krav på dataanonymisering skydda personuppgifter, så att det är säkrare att använda dem under hela AI-livscykeln.

Roller och ansvarsområden

Det är viktigt att all personal som jobbar med datastyrning är AI-redo. Medarbetare som har kunskap om datakraven för AI kan fungera som förvaltare och uppmuntra till förbättrad datakvalitet och efterlevnad. Tvärfunktionellt samarbete mellan juridikavdelningar och team för IT och datavetenskap kan bidra till att AI-specifika utmaningar hanteras på ett mer effektivt sätt.

Anpassa datastandarder och definitioner

Standardisering av dataformat, definitioner och kvalitetsmått förenklar införandet av policyer som styr användningen av AI-verktyg inom organisationen. Tydliga datastandarder gör det lättare att avgöra vilka datauppsättningar som AI-verktygen får resonera kring för att få tillgång till företagssammanhang, och vilka data som användare får ladda upp för analys. Det gör att AI-programmen använder de mest relevanta och betrodda data, ökar effektiviteten och främjar efterlevnad av organisationens policyer.

Kontinuerlig förbättring

Datastyrning är en ständigt pågående process, särskilt när det kommer till AI. Regelbundna granskningar och uppdateringar av styrningsramverket kan göra anpassningen till AI-utvecklingen och nya lagar och föreskrifter lättare. Själva AI-tekniken kan användas för att kontrollera och förbättra styrningsmetoderna, hitta luckor och föreslå förbättringar. Ett proaktivt tillvägagångssätt förbättrar efterlevnaden och ökar effektiviteten när AI-tekniken utvecklas.

Verktyg och tekniker för effektiv datastyrning

Anpassa till affärsmålen:

Se till att datastyrningsstrategin stöder organisatoriska mål för att förbättra beslutsfattandet och effektiviteten.

Automatisera rutinarbetet:

Automatisera repetitiva uppgifter som dataklassificering och åtkomsthantering för att minska förekomsten av manuella fel och öka säkerheten.

Se till att du har höga krav på korrekthet: Använd validerings- och rensningsverktyg för att främja dataintegriteten över tid.

Utbilda användarna: Erbjud utbildning om verktyg och procedurer för datastyrning för att förhindra felaktig hantering och säkerställa efterlevnad av företagspolicyer.

Genomför regelbundna granskningar: Granska datastrategin regelbundet för att se till att den håller jämna steg med juridiska och organisatoriska förändringar.

Avslutning

Effektiv datastyrning för AI med Microsoft 365

Det krävs en robust datastyrningsstrategi för att främja ansvarsfull AI-användning. Effektiv datastyrning gör data tillgängliga, korrekta och säkra – och gör det möjligt för AI att leverera tillförlitliga insikter och främja innovation. Att prioritera datakvalitet, efterlevnad och säkerhet förbättrar AI-funktionerna, leder till bättre beslut och skapar konkurrensfördelar.

Microsoft 365: Stärker AI-beredskapen

Microsoft 365 erbjuder förstklassiga produktivitetssappar med inbyggda verktyg för dataklassificering, kontroll och skydd. De här funktionerna stöder ditt datastyrningsramverk och främjar införandet av AI-teknik på ett säkert sätt – när du är redo. Microsoft 365 hjälper dig med:

- **Datakvalitet:** Främjar AI-utdatas korrekthet och tillförlitlighet.
- **Efterlevnad:** Följ lagar och andra föreskrifter och reducera den juridiska risken.
- **Zero Trust-säkerhet:** Skydda känslig information från obehörig åtkomst, dataläckor och cyberhot.

Upptäck heltäckande produktivitetssverktyg förstärkta med AI-tillval och ett robust skydd för att hjälpa din organisation att jobba effektivt och säkert.



Utforska Microsoft 365