Policy för ansvarsfull AI

INFORMATIONSTEKNIK | PUBLICERAD: 21 januari 2026 | Reviderad: N/A

Denna policy fastställer Magnas engagemang för ansvarsfull användning och utveckling av artificiell intelligens-lösningar i vår verksamhet, våra produkter och våra affärsprocesser. Dessa lösningar erbjuder möjligheter att skapa värde, men kan också skapa juridiska, anseendemässiga och andra risker för Magna, dess anställda och andra intressenter. Din nogsamma efterlevnad av denna policy är avgörande för att främja säker och ansvarsfull användning av artificiell intelligens för att maximera möjligheter och minimera dess risker.

TILLÄMPNING AV POLICYN

Denna policy gäller Magna International Inc. och alla dess operativa grupper, divisioner (inklusive kontrollerade joint ventures), dotterbolag och andra verksamheter globalt. Denna policy gäller även alla personer som agerar för Magnas räkning, inklusive heltids- och deltidsanställda hos Magna, fristående entreprenörer, tjänstemän, styrelseledamöter, konsulter och ombud – i denna policy hänvisar vi till alla sådana personer som ”du” eller ”Magna-personer"

Denna policy beskriver krav för ansvarsfull, etisk och säker användning och utveckling av dig av:

- alla **AI-lösningar**, inklusive **traditionella AI-system, generativ AI-system, AI-agenter** och **agentisk AI**; och
- alla **AI-utdata** genererad av en **AI-lösning**.

”**Användning**” av en **AI-lösning** innebär att du använder en befintlig **AI-lösning** som utvecklats av Magna eller en tredje part för att utföra:

- enkla uppgifter, som att skapa e-postmeddelande eller bild, sammanfatta text eller besvara en fråga; eller
- mer komplexa uppgifter, som att stödja Magnas produktutveckling, affärsprocesser och initiativ för tillverkningsautomation.

"**Utveckling**" av en **AI-lösning** innebär att du har en högre nivå av interaktion med lösningen, vilket omfattar något av följande:

- utveckla specifikationer för **AI-lösningen**;
- skapa, designa, förfina eller träna **AI-lösningens** modell och algoritm;
- insamling, bearbetning eller träning av datamängder som ligger till grund för **AI-lösningen**;
- testa eller validera **AI-lösningen**; eller
- använda tredjepartsverktyg för **utveckling**.

Utveckling av en **AI-lösning** kan vara:

- enbart för interna ändamål (t.ex. tillverkningsautomation);
- för användning av externa intressenter (t.ex. kunder, leverantörer eller andra affärspartners); eller
- för införlivande i Magnas produkter.

Dessutom kan **utveckling** av en **AI-lösning** göras:

- internt av Magna-personer (t.ex. genom användning av tredjepartsverktyg, som NVIDIA Isaac Sim, samt genom **AI-**funktioner i traditionella system som CATIA);
- av tredjepartspartner för eller på uppdrag av Magna; eller

- gemensamt av ett team som inkluderar Magna-personer och personal från tredjepartsutvecklare.

Förutom ”användning” och ”utveckling” förekommer andra viktiga termer i fetstil i denna policy. Definitioner av dessa nyckeltermer finns i **Bilaga A** till denna policy.

ANSVARSFULL AI PÅ MAGNA

Att uppnå produktivitetsfördelar med **AI** samtidigt som riskerna minimeras och våra medarbetare skyddas är viktigt för Magna. Du spelar en avgörande roll i att hjälpa Magna att uppnå dessa mål genom att nogsamt följa principerna och metoderna nedan:

1. Förstå och hantera riskerna i samband med användning av AI-lösningar

Användningen av **AI-lösningar** kan skapa risker som du behöver förstå och hjälpa till att hantera, inklusive:

- **Partiskhet:** **AI-lösningar** kan lära sig och förstärka fördomar i deras utbildningsdata vilket kan leda till snedvridna resultat och oavsiktliga konsekvenser, som diskriminerande anställningsmetoder. Du måste vara uppmärksam på risken för partiskhet och ska vara uppmärksam när du bedömer **AI-utdata** avseende partiskhet.
- **Hot mot cybersäkerhet:** **AI-lösningar** kan användas eller utnyttjas för att utföra cyberattacker, stjäla identiteter och äventyra säkerheten. Du bör aldrig använda en **AI-lösning** för dessa eller andra olagliga syften. Dessutom hjälper du till att skydda Magna mot cyberattacker och andra externa hot genom att inte installera obehöriga plugin-program, kopplingar, tillägg eller API:er i **AI-lösningar**.
- **Brist på transparens:** **AI-**algoritmer fungerar på sätt som inte är väl förstådda och producerar ofta bristfälliga **AI-utdata**. Som angivet vidare nedan måste du utöva tillsyn över **AI-utdata** för att säkerställa att de är korrekta, tillförlitliga, relevanta, opartiska och lämpliga för den avsedda användningen.
- **Sekretess och dataskydd:** Många **AI-lösningar** samlar in data allt eftersom de används vilket potentiellt ger utvecklare tillgång till konfidentiella och/eller rättsligt skyddade data och personlig information. Du måste välja bort att tillåta att ett tredjepartssystem från **Gen AI** använder **Magna-ägda eller -kontrollerade indata** (inklusive personuppgifter från Magna-personer) för att träna, utveckla eller revidera sin modell.
- **Immateriella rättigheter:** **Gen AI-system** kan skapa **AI-utdata** som gör intrång i tredje parts immateriella rättigheter. Exempel inkluderar användning av skriven text utan korrekt kreditering och citering, obehörig användning eller kopiering av bilder, konstverk, design, programkod eller annat material, att föreslå produktdesign eller processer som gör intrång i tredje parts patent.

  Du får inte använda **AI-lösningar** och **AI-utdata** på ett sätt som gör intrång i tredje parts immateriella rättigheter (inklusive upphovsrätt, patent, design och varumärken).

  Om du dessutom använder **AI-lösningar** för att skapa arbetsprodukter som Magna kan behöva skydda enligt lagar gällande immateriella rättigheter måste du samarbeta med Magnas juridiska team för immateriella rättigheter och säkerställa att Magna kan skydda arbetsprodukter som kan baseras på **AI-utdata**.

2. Övningsövervakning

AI-utdata kräver kritisk mänsklig granskning innan de slutförs, förlitas på och/eller delas internt eller externt. Eftersom du är ansvarig för alla **AI-utdata** som du använder i ditt arbete för Magna måste du tillämpa genomtänkt utvärdering, analytiskt tänkande och rimligt omdöme innan du förlitar dig på **AI-utdata**.

Förlita dig inte på **AI-utdata** som du vet genererades genom brott mot tillämplig lag eller någon annans rättigheter, eller som skulle kunna skada Magnas anseende. Exempel kan inkludera **AI-utdata** som bryter mot andras upphovsrätt eller varumärkesrättigheter.

Om du, efter att ha gjort rimliga ansträngningar, fortfarande är osäker på riktigheten i **AI-utdata**, förlita dig inte på den – särskilt i situationer som innebär betydande juridisk eller anseendemässig risk.

3. Använd Magnas godkända AI-lösningar

Magna har verifierat ett antal **AI-lösningar** för att säkerställa att vi följer våra cybersäkerhetsstandarder och våra policyer för sekretess och dataskydd. När det är möjligt ska du använda Magnas **Godkända AI-lösningar**, vilket inkluderar:

- **MAVIS**;
- Microsoft M365 Copilot och Copilot Chat-assistenter;

- GitHub Copilot kodnings- och programmeringsassistent;
- Microsoft Azure AI Foundry Models-plattformen;
- Amazon Bedrock-tjänsten för åtkomst till och hantering av grundmodeller; och
- Databricks-plattformen.

Om du vill använda en **AI-lösning** och du avser att använda den med **Magna-ägda eller kontrollerade indata** måste du först kontrollera att den är listad som en **godkänd AI-lösning** på **AI MagNET – AI-lösningar och teknologier**. Om verktyget inte redan är godkänt är du ansvarig för att föreslå det i **Magnet** och följa gällande godkännandeprocess.

Utgå alltid från att det inte finns någon sekretess för **indata** som matas in i en icke godkänd **AI-lösning**. Som ett resultat kan alla **indata** som används i en icke godkänd **AI-lösning** äventyra Magnas immateriella rättigheter.

4. Förbjudna användningsområden

Du får inte använda **AI-lösningar** för att utföra någon handling eller uppnå något resultat som är förbjudet enligt lag, eller som skulle skada Magnas anseende, inklusive genom någon form av bedrägeri, diskriminering, trakasserier, hot, mobbning eller annan skada. Inte heller får du använda **AI-lösningar** för att göra något av följande:

- manipulera beteendet eller utnyttja någons sårbarheter på ett skadligt sätt, inklusive sårbarheter relaterade till ålder, funktionsnedsättning eller specifik social eller ekonomisk situation;
- utvärdera eller klassificera en person på sätt som kan leda till diskriminering eller skada, inklusive baserat på socialt beteende eller personliga egenskaper;
- skapa databaser för ansiktsigenkänning (känsloigenkänning) genom oriktad skrapning av ansiktsbilder;
- känna igen en persons känslor på arbetsplatsen; eller
- kategorisera någon person baserat på känsliga eller lagligt skyddade personliga egenskaper, inklusive etnicitet, religion, ålder, sexuell läggning eller politiska åsikter, på ett sätt som kan orsaka diskriminering eller skada.

5. Inkludera AI-friskrivningar

Du bör lägga till en **AI-**friskrivning i alla situationer som rör **AI-lösningar** där underlåtenhet att göra det kan rimligen skada eller vilseleda andra.

- **Rättsligt krav:** I alla situationer där **Tillämplig lag** kräver att en ansvarsfriskrivning inkluderas, **måste** du använda en.
- **Bästa praxis:** För rutinmässiga ärenden, som vardagliga e-postmeddelanden, är en ansvarsfriskrivning i allmänhet onödig. I andra offentligt riktade eller affärskritiska situationer, som arbete som är mycket **AI**-genererat och/eller väsentligt skulle kunna påverka beslut, **ska** ansvarsfriskrivning beaktas.

Andra specifika omständigheter under vilka en **AI-**friskrivning **måste** användas är bland annat när:

- **AI-lösningar** interagerar direkt med människor (t.ex. chattbotar) och det inte är tydligt för en någorlunda informerad person att interaktionen involverar en **AI-lösning**;
- **AI-utdata** som du använder eller skickar inkluderar manipulerade bilder, ljud eller video som falskeligen verkar autentiska eller skulle kunna rimligen uppfattas som autentiska; och
- **AI-utdata** är avsedda att informera interna eller externa intressenter om frågor av allmänt intresse (t.ex. kommunikation om produkter, tjänster eller säkerhet som kan påverka kunder eller andra intressenter) när de presenteras som faktabaserade eller auktoritativa.

Ett förslag på ansvarsfriskrivning är: ”Följande innehåll genererades med hjälp av en artificiell intelligens-lösning.”

Vissa undantag gäller. Till exempel behöver inte **AI**-genererad text märkas om den har granskats och redigerats av en människa med redaktionellt ansvar. Dessutom behövs ingen ansvarsfriskrivning när det redan är tydligt att interaktionen involverar **AI**.

6. Förvärva eller utveckla en AI-lösning

Om du avser att förvärva (inklusive genom köp, licensiering eller prenumeration) eller utveckla/samutveckla en **AI-lösning** är du ansvarig för att följa Magnas godkännandeprocess för **AI-lösningar** via länken på **AI MagNET – AI-lösningar och teknologier**.

Denna process omfattar två distinkta steg:

- **Steg 1** spåra planerade **AI-**initiativ, idéer och användningsfall för att främja transparens, bedöma affärsvärde och ekonomisk genomförbarhet, minimera dubbelarbete samt stärka styrning och riskhantering; och
- **Steg 2** dokumentation, kategorisering och riskbedömning av **AI-lösningar** från tidigare steg som är godkända och genomförda.

Beroende på din roll i förhållande till den **AI-lösning** som förvärvas eller utvecklas kan du anses vara "utvecklare" av lösningen, inklusive i syfte att följa denna policy och Magnas. **Principer för ansvarsfull AI** såväl som **Procedurer för AI-utvecklare** och **EUAIA**.

7. AI-agenter

Du kan använda **AI-agenter** som har skapats för dina specifika arbetsbehov genom **Godkända AI-lösningar**. **AI-agenter** är **AI-lösningar** som helt och hållet omfattas av denna policy.

Om du är företagsägaren som använder en **AI-agent** för din egen eller ditt teams bruk, är du ansvarig för att inhämta förhandsgodkännande för **AI-agenten** genom den tvåstegsgodkännandeprocess som anges i avsnitt 6 ovan. Dessutom ansvarar du för att samarbeta med det tekniska teamet för nödvändig övervakning och tillsyn av dina **AI-agenter** under hela deras livscykel (dvs. från initial design till pensionering, inklusive kommunikation mellan agenter) vilket inkluderar efterlevnad av styrningskrav, organisatoriska IT-standarder och riktlinjer samt **RAI-principerna**. Slutligen måste du också följa alla andra krav som anges i **Procedurer för AI-utvecklare** när det gäller **AI-agenter**.

YTTERLIGARE INFORMATION

1. Efterlevnad av Magnas policyer och tillämplig lag

I alla situationer som involverar **användning** eller **utveckling** av **AI-lösningar** måste du följa **tillämplig lag**, Magnas **Principer för ansvarsfull AI** och andra relevanta Magna-policyer (t.ex. policy för konfidentiell information, dataskyddspolicy etc.). Se **Bilaga B** i denna policy för en lista med sådana lagar och relaterade Magna-policyer.

Dessutom ska Magnas och varje persons skyldigheter som denna policy gäller omfattas av **tillämplig lag** och i den mån det föreligger eventuella avvikelser ska de tolkas så nära kraven i denna policy som möjligt, samtidigt som de förblir i enlighet med **tillämplig lag**.

2. Efterlevnad av kund-, leverantörs-, försäljar- och andra tredjepartskrav samt sekretessavtal

Du måste beakta avtalsenliga begränsningar, restriktioner och förbud när du hanterar data och information från tredje part i en **AI-lösning**. I vissa fall kan det hända att du inte har tillstånd att använda och/eller mata in sådan tredjepartsdata i **AI-lösningen** eftersom det kan bryta mot ett sekretessavtal eller andra sekretessarrangemang. Du bör diskutera tillämpliga sekretessskyldigheter, begränsningar, förbud och andra avtalsbegränsningar med koncernens, regionala eller företagets jurist för att hjälpa Magna att undvika brott mot sina avtalsenliga åtaganden. Dessutom måste du följa Magnas sekretesspolicy.

3. Utbildning

Magna kommer att tillhandahålla resurser och utbildning för att hjälpa dig att bättre förstå **AI-lösningarnas** möjligheter och begränsningar. Du ansvarar för att genomföra all nödvändig utbildning i tid.

4. Rapportering

Övervaka, dokumentera och rapportera eventuella fel som du upplever när du utvecklar en **AI-lösning**, såväl som eventuella partiska, skadliga, felaktiga eller avvikande **AI-utdata**. I många fall kan sådan rapportering ske direkt i en **AI-**

lösning – i så fall bör du använda den rapporteringsfunktionen. I situationer där det inte finns någon rapporteringsfunktion i själva **AI-lösningen**, eller om du anser att riskerna/konsekvenserna är betydande, kan du rapportera via **Magna-jourlinjen** genom ”**Oro kring dataskydd/artificiell intelligens (AI)**”.

Om du blir medveten om misstänkta brott mot denna policy eller att Magnas immateriella rättigheter har kränkts, bör du rapportera det via **Magna Hotline**.

Beroende på region och omständigheter kan rapporter till behöriga myndigheter också vara nödvändiga; ingenting i denna policy hindrar dig från att kontakta myndigheter i din egen, personliga egenskap.

5. Övervakning av efterlevnad

Magna förbehåller sig rätten att övervaka att Magna-personer följer denna policy. Magna kommer att införa åtgärder för att förebygga, övervaka och reagera på incidenter som involverar **AI-lösningar**, inklusive fall av skada och partiska resultat, samt säkerhets-, sekretess- och dataskyddsintrång.

6. Ansvar för överträdelser av denna policy

Om du bryter mot villkoren i denna policy kan du bli föremål för disciplinära åtgärder, inklusive uppsägning.

7. Mer information:

För ytterligare information eller vägledning, kontakta din utsedda **Globala AI-ledare** eller e-posta **ai.governance@magna.com**.

Publicerad:	21 januari 2026
Reviderad:	n/a
Nästa granskning:	Q1 2027
Utfärdad av:	HR och Informationsteknik
Godkänd av:	HR och Informationsteknik

BILAGA A – DEFINITIONER

”**Agentisk AI**” avser **AI-lösningar** som kan planera, vidta åtgärder eller slutföra uppgifter med viss autonomi, samtidigt som de arbetar under mänsklig överinseende (dvs. **agentisk AI** är denna förmåga (AI som kan agera, planera eller driva ärenden)).

"**AI**" betyder artificiell intelligens.

”**AI-agenter**” avser specifika verktyg eller system som använder agentfunktioner för att utföra uppgifter eller arbetsflöden åt en användare inom kontrollerade parametrar (dvs. **AI-agenter** är de verktyg eller system som använder denna funktion för att utföra uppgifter i praktiken). Exempel omfattar: **AI-**agenter i Microsoft Teams för att hjälpa till att schemalägga möten eller svara på medarbetarnas frågor; specialiserade **AI-**assistenter etc.

”**AI-utvecklarprocedurer**” avser **Procedurer för AI-utvecklare**.

”**AI-utdata**” avser allt innehåll (inklusive text, bilder, ljud, video och programkod), resultat, rekommendationer, beslut och/eller annan utdata som genereras av en **AI-lösning**.

”**AI-lösning**” avser alla AI-system, funktioner, användningsområden, produkter, plattformar och verktyg, inklusive **traditionella AI-system**, **generativ AI-system**, **AI-agenter** och **Agentisk AI**.

"**Tillämplig lag**" som definierad i **Bilaga B**.

”**Godkända AI-lösningar**” avser **AI-lösningar** som uppfyller Magnas IT-säkerhetsprotokoll och sekretesskrav och har godkänts och driftsatts för användning i Magnas verksamhet. Lista med Magnas **godkända AI-lösningar** finns **här.**

"**Utveckling**" av en **AI-lösning** innebär att du har en högre nivå av interaktion med lösningen, vilket omfattar något av följande:

- utveckla specifikationer för **AI-lösning**;
- skapa, designa, förfina eller utbilda **AI-lösning**s modell och algoritm;
- samla in, bearbeta eller träna de datauppsättningar som ligger till grund för **AI-lösning**;
- testa eller validera **AI-lösning**; eller
- använda ett tredjepartsverktyg för **Utveckling**.

Utveckling av en **AI-lösning** kan ske:

- enbart för interna ändamål (t.ex. tillverkningsautomation);
- för användning av externa intressenter (t.ex. kunder, leverantörer eller andra affärspartners); eller
- för införlivande i Magnas produkter.

Dessutom kan **utveckling** av en **AI-lösning** göras:

- internt av Magna Persons (t.ex. genom användning av tredjepartsverktyg, som NVIDIA Isaac Sim, samt genom **AI-**funktioner i traditionella system som CATIA);
- av tredjepartspartner för eller på uppdrag av Magna; eller
- gemensamt av ett team som inkluderar Magna-personer och personal från tredjepartsutvecklare.

"**EUAIA**" betyder *EU AI Act*.

”**Generativ AI-system**” avser **AI-lösningar** som primärt är utformade för att generera nytt innehåll (t.ex. text, bilder, ljud, video eller programkod etc.) eller för att autonomt planera och genomföra flerstegsåtgärder mot mål baserat på mönster inlärda från data, snarare än att bara analysera eller klassificera befintliga data.

”**Indata**” avser alla indata, data, frågor, kommandon, information eller dokument som matas in i en **AI-lösning**.

”**Magna**” avser Magna International Inc. och alla av dess operativa grupper, divisioner (inklusive kontrollerade joint ventures), dotterbolag och annan verksamhet globalt.

”**Magna-ägda eller -kontrollerade indata**” avser data, information eller dokument som Magna har, besitter eller kontrollerar och som tillhör Magna, Magna-personer eller Magnas kunder, leverantörer eller andra affärspartners.

”**Magna-personer**” eller ”**du**” avser alla personer som agerar för Magnas räkning, inklusive: en heltids- eller deltidsmedarbetare hos Magna; fristående entreprenörer, tjänstemän, styrelseledamöter, konsulter och ombud.

”**MAVIS**” avser Magna AI Virtual Information System-assistenten.

”**RAI-principer**” avser **Principer för ansvarsfull AI**.

”**Traditionella AI-system**” avser **AI-lösningar** som använder statistiska/maskininlärningsmodeller och/eller regelbaserad logik för att analysera eller klassificera befintliga data och producera utdata som förutsägelser, rekommendationer eller beslut, och som inte primärt är utformade för att generera nytt innehåll eller för att autonomt planera och genomföra flerstegsåtgärder mot mål.

”**Användning**” av en **AI-lösning** innebär att du använder en befintlig **AI-lösning** som utvecklats av Magna eller en tredje part för att utföra:

- enkla uppgifter, som att skapa e-postmeddelande eller bild, sammanfatta text eller besvara en fråga; eller
- mer komplexa uppgifter, som att stödja Magnas produktutveckling och initiativ för tillverkningsautomation.

BILAGA B – TILLÄMPLIG LAG OCH MAGNA-POLICYER

Tillämplig lag

”**Tillämplig lag**” avser alla lagar, stadgar, förordningar, regler, bestämmelser, koder, direktiv, order, domar, riktlinjer och myndighetskrav som kan träda i kraft från tid till annan och som är relevanta för hur **AI-lösningar** väljs, används, utvecklas eller driftsätts, inklusive

- Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om fastställande av harmoniserade regler om artificiell intelligens (”EUAIA”)

Relevanta/relaterade Magna-policyer

- **Magnas konfidentiella informationnspolicy**
- **Magna International Inc. Policy för företagsoffentliggörande**
- **Magna International Inc. Policy, rutiner och riktlinjer för sekretess och dataskydd**
- **Magna informationsklassificeringspolicy**
- **Magna företagssäkerhetspolicy**
- **Magnas globala policy för e-post, internet/intranät och sociala medier**
- **Magna IT/OT-säkerhetspolicy**
- **Magna International Inc. Policy för hantering av cybersäkerhetsincidenter**
- **Magna hälso-, säkerhets- och miljöpolicy**