Policy och riktlinjer för AI

1. Syfte och omfattning

Syfte

Syftet med denna policy är förutom att främja en ansvarsfull och säker integration av Artificiell Intelligens (AI) och andra digitala innovationer i vår verksamhet, även att möjliggöra en ökad konkurrenskraft. Genom att integrera AI strävar vi efter att effektivisera arbetsflöden och skapa värde för både kunder och medarbetare. På så sätt positionerar vi företaget i framkant av teknologisk innovation, samtidigt som vi upprätthåller en hög standard för integritet, användarsäkerhet och etik.

Omfattning

Denna policy gäller för alla anställda, uppdragstagare och samarbetspartners inom företaget.

2. Principer för användning av AI och ny teknik

Inköp och implementering

Alla AI-verktyg och digitala innovationer måste granskas och godkännas av VD före inköp och användning. Detta inkluderar en bedömning av teknikens pålitlighet, säkerhet och överensstämmelse med etiska riktlinjer.

Definition av AI och ny teknik

Denna policy har fokus främst på generativ AI och LLM (stora språkmodeller), som använder omfattande datamängder för att generera beslutsunderlag, texter och sammanfattningar. Denna teknologi, styrs av instruktioner från användarna, så kallade prompts, för att extrahera data och information. Exempel på dessa språkmodeller är Bing, ChatGPT och bildgenereringsprogram som DALL-E.

Användning och Godkännande

Användning av AI-verktyg kräver godkännande av medarbetarens närmaste chef. Anställda måste ta del av relevant information avseende användning av AI för att säkerställa korrekt användning av tekniken.

Ansvar för slutresultat och data

Den anställde är ansvarig för hur data används och det slutliga resultatet av en utförd arbetsuppgift. Den anställde ska vara transparent med om och hur AI använts i utförande av en arbetsuppgift och kunna förklara resultatet. Lojalitetsplikten i anställningsavtalet och lagar om sekretess och företagshemligheter gäller.

Vid användande av öppna AI-lösningar i arbetet, det vill säga AI-modeller som inte är företagsinterna, ska godkännande inhämtas av närmaste chef.

Kunddata får under inga som helst omständigheter matas in i öppna AI-lösningar. Inte heller intern företagsinformation (Wenell) som kan anses vara affärkritisk (utbildningsmaterial, ekonomi, persondata, etc.) får användas i öppna AI-lösningar.

3. Rättslig och etisk överensstämmelse

Lagar och förordningar

Användningen av AI-verktyg ska överensstämma med gällande lagstiftning, inklusive, men inte begränsat till, Dataskyddsförordningen (GDPR), Arbetsmiljölagen och Diskrimineringslagen.

Etiska Riktlinjer

All AI-användning ska följa företagets interna etiska riktlinjer och principer för ansvarsfull användning av teknologi. Användningen av AI ska vara transparent, spårbar och tillvägagångssättet och resultatet ska gå att förklara.

4. Risk- och möjlighetsanalys

Regelbundna analyser av möjliga risker och fördelar med AI-användning ska genomföras av företagets ledning. Rapporter och rekommendationer baserade på dessa analyser ska när så krävs ligga till grund för beslut och åtgärder.

5. Övervakning och rapportering

Övervakning av AI-användningen ska ske kontinuerligt för att säkerställa att denna policy och företagets övergripande mål efterlevs. Incidenter eller problem relaterade till AI ska rapporteras omedelbart till en överordnad chef.

En överträdelse av denna policy, oavsett om den är avsiktlig eller ett misstag, ska hanteras med både allvar och förståelse för den mänskliga faktorn i användningen av teknologi.

Omedelbar åtgärd vid misstag

Om en medarbetare inser att hen har matat in känslig information i ett AI-verktyg av misstag, är de första stegen att:

- Omedelbart avbryta alla pågående processer i verktyget.
- Informera sin närmaste chef och IT-ansvarig utan dröjsmål.
- Följa instruktioner för att säkert ta bort eller anonymisera den inmatade informationen, om möjligt.

En utredning ska inledas för att fastställa omfattningen av överträdelsen och identifiera eventuella säkerhetsbrister. Detta kommer att hjälpa till att förstå hur misstaget inträffade och hur liknande händelser kan förhindras i framtiden.

IT-ansvarig tillsammans med juridisk expertis ska granska incidenten för att bedöma eventuella risker för dataläckage och rättsliga konsekvenser. Om känslig information har

lämnat organisationens kontroll, måste en riskbedömning genomföras och lämpliga åtgärder vidtas enligt gällande lagstiftning, såsom GDPR. Om det finns en risk för att personuppgifter har kompromitterats, ska organisationen följa lagstadgade rapporteringskrav och underrätta berörda individer samt dataskyddsmyndigheter där så är nödvändigt.

6. Disciplinära åtgärder

Även om fokus ligger på utbildning och förhindrande av framtida misstag, kan upprepade eller grova överträdelser av policyn leda till åtgärder. Dessa åtgärder ska vara proportionerliga mot överträdelsens allvar och kan inkludera varning, omplacering, eller i särskilt allvarliga fall, uppsägning.

Dokumentation och feedback:

Alla incidenter och åtgärder ska dokumenteras noggrant. Denna dokumentation ska ses över för att kontinuerligt förbättra våra processer och policyer. Vi uppmuntrar feedback från medarbetare för att ytterligare utveckla vår förståelse och hantering av AI-verktyg.

Sammanfattning

Ledningen är positiva till användningen av AI i arbetet

Medarbetarna tillser att användningen sker i ordnade former med respekt för lagar, regler och policyn ovan

Medarbetaren har ansvaret för det slutliga resultatet

Kompetensutveckling sker genom samtal och utbildningar

Säkerhet och integritet prioriteras.

7. Policyuppdateringar

Denna policy är ett dynamiskt dokument som kommer att uppdateras regelbundet för att spegla den senaste utvecklingen inom teknik och lagstiftning.

Stockholm den 3 september 2024

……..

Tommy Olin, VD