PolisPoint

AI Agent Policy

PolisPoint B.V.

1. Doel en reikwijdte

Dit beleid geeft richting aan hoe PolisPoint B.V. omgaat met AI agents binnen de organisatie. Het waarborgt zorgvuldigheid in interne processen, bescherming van gevoelige gegevens en naleving van relevante wet- en regelgeving (waaronder de AI Act).

Het beleid geldt voor:
- alle medewerkers, stagiairs en externe partners die gebruikmaken van AI agents;
- alle interne werkzaamheden waarbij AI agents ondersteunend worden ingezet.

NB: AI wordt bij PolisPoint niet ingezet voor direct klantcontact of als chatbot. Alle klantcommunicatie verloopt uitsluitend via bevoegde medewerkers.

2. Toepassing van AI binnen PolisPoint

- Ondersteunend karakter: AI agents worden uitsluitend gebruikt voor interne controles, standaard werkzaamheden en procesoptimalisatie.
- Mens in de lead: Medewerkers blijven altijd eindverantwoordelijk voor de uitvoering van taken en de besluitvorming. AI wordt ingezet als hulpmiddel, nooit als beslissingsautoriteit.
- Geen klantinteractie: AI agents communiceren niet zelfstandig met klanten of externe partijen. Er worden geen chatbots of AI-gestuurde onderhandelingssystemen gebruikt.

3. Data beschikbaarheid voor externe crawler bots en AI agents

- Selectieve openstelling: Alleen niet-gevoelige en openbaar bedoelde data (bijvoorbeeld algemene productinformatie, publieke FAQ’s) mag beschikbaar worden gesteld aan externe AI agents of crawler bots.

- Doelbinding: Data mag uitsluitend gebruikt worden voor vooraf bepaalde en goedgekeurde doeleinden (zoals vindbaarheid of marketing).
- Voorwaarden: Toegang wordt alleen toegestaan indien er afspraken zijn over opslag, verwerking en naleving van de AVG en AI Act.

4. Onderscheid mens en machine bij gevoelige informatie

- Strikte scheiding: Bij het uitwisselen van gevoelige of vertrouwelijke informatie (zoals klantgegevens, interne financiële data of strategische documenten) wordt altijd onderscheid gemaakt tussen mens en AI agent.
- Beperkingen voor AI: AI agents krijgen geen toegang tot gevoelige gegevens, tenzij dit expliciet en gecontroleerd is toegestaan.
- Controle door medewerkers: Alleen medewerkers verwerken gevoelige informatie. AI kan hooguit geanonimiseerde of versleutelde data analyseren.

5. Transparantievereisten en AI Act

- Herleidbaarheid: AI agents moeten hun werking, datagebruik en beperkingen kunnen toelichten. Uitkomsten moeten controleerbaar zijn.
- Melding gebruik AI: Binnen de organisatie moet duidelijk zijn wanneer AI agents worden gebruikt.
- Risicoclassificatie: Conform de AI Act worden AI-toepassingen geclassificeerd (minimaal, beperkt, hoog of onacceptabel risico). Voor PolisPoint geldt momenteel: laag risico, omdat AI alleen intern en ondersteunend wordt gebruikt.
- Documentatieplicht: AI agents en hun gebruiksdoelen worden vastgelegd in een intern register.

6. Governance en naleving

- Verantwoordelijkheid: De directie is eindverantwoordelijk voor dit beleid; uitvoering ligt bij de aangewezen AI-beleidsfunctionaris en de CISO.
- Toetsing: Jaarlijks wordt dit beleid geëvalueerd op basis van nieuwe wetgeving, technologische ontwikkelingen en interne ervaringen.

- Sancties: Overtredingen kunnen leiden tot disciplinaire maatregelen, afhankelijk van de ernst.

7. Technische en organisatorische waarborgen

- IT-omgeving: Alle medewerkers werken op de nieuwste Lenovo-laptops met Microsoft 365 Pro.
- Dubbele authenticatie (2FA): Verplicht voor alle accounts.
- Wachtwoordbeheer: NordPass wordt gebruikt voor veilig wachtwoordbeheer.
- Gebruik van AI (ChatGPT): PolisPoint gebruikt een betaalde versie van ChatGPT, waarbij geen gegevens worden gedeeld voor trainingsdoeleinden. Dit waarborgt vertrouwelijkheid.
- Beveiligingsnormen: AI agents worden alleen gebruikt binnen de beveiligde Microsoft 365-omgeving of via vooraf goedgekeurde SaaS-oplossingen.

8. Conclusie

PolisPoint B.V. zet AI verantwoord en uitsluitend ondersteunend in. De mens staat altijd centraal bij besluitvorming en klantcontact, en AI dient uitsluitend ter ondersteuning van interne processen. Hiermee wordt innovatie omarmd, terwijl de bescherming van klanten, medewerkers en de organisatie voorop blijft staan.