kod szkolenia: DM-PRA-WdrAI / PL DL 2d

Wdrażam AI w marketingu. Etycznie i zgodnie z prawem

Sztuczna inteligencja staje się nieodłącznym elementem funkcjonowania nowoczesnych organizacji. Narzędzia oparte na AI, takie jak generatywne modele językowe czy systemy wspierające procesy biznesowe, oferują ogromny potencjał, ale równocześnie niosą ze sobą szereg wyzwań prawnych, etycznych i technologicznych. Brak wiedzy w tym obszarze może prowadzić do ryzyk prawnych, wizerunkowych i finansowych. Szkolenie zostało stworzone po to, by w praktyczny sposób wprowadzić uczestników w świat AI, wskazać możliwości i ograniczenia, a przede wszystkim przygotować do bezpiecznego i odpowiedzialnego wdrażania sztucznej inteligencji w firmie.

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla wszystkich, którzy chcą świadomie i praktycznie zrozumieć wyzwania oraz możliwości sztucznej inteligencji w biznesie:

- menedżerów i liderów zespołów odpowiedzialnych za wdrażanie nowych technologii,
- osób z działów prawnych, compliance i bezpieczeństwa IT,
- specjalistów marketingu, HR i komunikacji korzystających z narzędzi AI w codziennej pracy,
- przedsiębiorców i osób zarządzających firmami, które chcą wprowadzać AI w sposób bezpieczny i zgodny z prawem.

Korzyści

1. Modele AI w praktyce – poznasz różne modele AI (ML, LLM, GenAI) oraz ich zastosowanie w biznesie.
2. Ryzyka związane z AI – nauczysz się rozpoznawać i minimalizować ryzyka prawne, etyczne oraz związane z bezpieczeństwem danych w procesie korzystania z AI.
3. Odpowiedzialne wdrażanie AI – dowiesz się, jak odpowiedzialnie wdrażać AI w organizacji, od polityk

wewnętrznych po regulacje prawne, w tym AI Act.

4. Krytyczna ocena wyników AI – zdobędziesz umiejętność oceniania wyników generowanych przez AI, takich jak halucynacje czy ryzyko błędów.
5. Ochrona danych i IP – nauczysz się, jak chronić dane, własność intelektualną oraz know-how przed nieuprawnionym wykorzystaniem w modelach AI.
6. Etyczne wyzwania AI – poznasz aktualne wyzwania w obszarze etycznego wykorzystania AI oraz narzędzia do ograniczania biasu i dyskryminacji.

Program szkolenia

Dzień 1. Wprowadzenie do AI

- ML, LLM, GenAI – AI w różnych odsłonach: kluczowe różnice i opcje wykorzystania sztucznej inteligencji w firmie,
- przegląd najpopularniejszych GenAI (ChatGPT, Copilot, Gemini, Perplexity, Midjourney, Eleven Labs), różnice w zastosowaniu i funkcjonowaniu modeli AI,
- publiczne vs. lokalne modele AI: różnice w poziomie bezpieczeństwa, najważniejsze punkty regulaminów GenAI (analiza fragmentów), darmowe vs płatne wersje publicznych modeli – porównanie, najważniejsze elementy umowy z dostawcą AI.

Korzystanie z AI w firmie

AI Literacy – kompetencje i odpowiedzialność w korzystaniu z AI

- AI Literacy w organizacji: odpowiedzialność za wdrożenie jej w firmie, podstawowe zasady
- omówienie potencjalnych ryzyk biznesowych i prawnych związanych z korzystaniem i wdrażaniem AI w firmie

Bezpieczeństwo danych w procesie korzystania z AI

- tajemnica przedsiębiorstwa, know-how i dane osobowe a korzystanie z AI
- przetwarzanie danych w cyklu życia AI (od trenowania modelu do jego wykorzystania)
- kluczowe wymogi dot. danych osobowych w trakcie korzystania z AI (legalne przetwarzanie danych – case study)
- sposoby na ograniczenie ryzyka w zakresie danych osobowych: jasne zasady i wytyczne (wewnętrzna polityka AI, onboarding pracowników), monitoring, prywatność (anonimizacja, szyfrowanie danych)

Prawa autorskie do treści wygenerowanych przez GenAI

- określenie komu przysługują prawa autorskie do treści wygenerowanych przez GenAI, rodzaje współpracy ze sztuczną inteligencją, sposoby na uzyskanie praw autorskich
- korzystanie z modeli publicznych a prawa autorskie
- sposoby na ograniczenie ryzyk związanych z naruszeniem własności intelektualnej w procesie wykorzystywania GenAI
- legalne korzystanie z treści wygenerowanych – styl, inspiracja, plagiat („efekt Ghibli") – prawdziwe przykłady aktualnych sporów i ich rozstrzygnięć z zakresu praw autorskich

Cyberbepieczeństwo w cyklu życia AI

- ścieżka zrozumienia cyberryzyka (kontekst biznesu, podatności, ograniczenie ryzyk, planowanie odporności – bezpieczeństwo danych wejściowych i modelu)
- reagowanie na incydenty bezpieczeństwa
- inżynieria społeczna, deepfake – opis zjawiska (realne przykłady)
- ataki przy użyciu AI lub na modele – case study i omówienie monimalizacji ryzyka ich powodzenia

Halucynacje – krytyczna ocena outputu

- wprowadzenie do tematu halucynacji modelu
- sposoby na weryfikację outputu

Shadow AI w firmie

- odpowiedzialność pracowników i podwykonawców – konsekwencje złamania regulaminu i polityki AI firmy
- sposoby na przeciwdziałanie shadow AI

Dzień 2. AI Act a wdrożenie sztucznej inteligencji w firmie

- wprowadzenie do AI Actu: cel i zakres stosowania, wskazówki kwalifikacji wykorzystywanego AI jako systemu AI, rola korzystającego z AI w procesie wdrożenia i obowiązki
- zakazane praktyki – omówienie i przykłady
- kategorie ryzyka systemów AI: omówienie i przykłady, wymagania dla systemów wysokiego ryzyka w praktyce, case study wdrożeń i ich ocena pod kątem wymogów AI Actu
- systemy wchodzące w interakcję z ludźmi – wymogi dla wdrażających
- luki i niejasności w regulacjach i ich wpływ na wdrożenia AI – jak do tego podejść

Etyczna AI w firmie od strony praktycznej

- określenie ram (frameworku) etycznej AI w firmie: czym jest etyczna AI, zasady i wymogi godnej zaufania AI, metody realizacji wymogów
- główne wyzwania etyczne w ramach wdrożenia: bias, dyskryminacja, prywatność danych, ochrona praw podstawowych, środowisko
- sposoby ograniczenia ryzyk związanych z etyczną AI
- rodzaje szkód, które mogą zostać wyrządzone z użyciem AI (na osobach, organizacjach, ekosystemach)

Odpowiedzialność za błędy AI

- odpowiedzialność za błędy AI – podmioty, które mogą zostać pociągnięte do odpowiedzialności, zasady odpowiedzialności
- mechanizmy ludzkiego nadzoru a ograniczenie odpowiedzialności
- roszczenia wobec dostawcy AI – dostępne możliwości

Jak uciec przed AI?

- ochrona przed trenowaniem modelu na danych i własności intelektualnej: opcje opt-out (prawne i techniczne) oraz ich skuteczność

Test podsumowujący

Oczekiwane przygotowanie uczestnika

Nie jest wymagane specjalne przygotowanie uczestników.

Czas trwania

2 dni / 10 godzin

Język

Materiały: polski
Szkolenie: polski