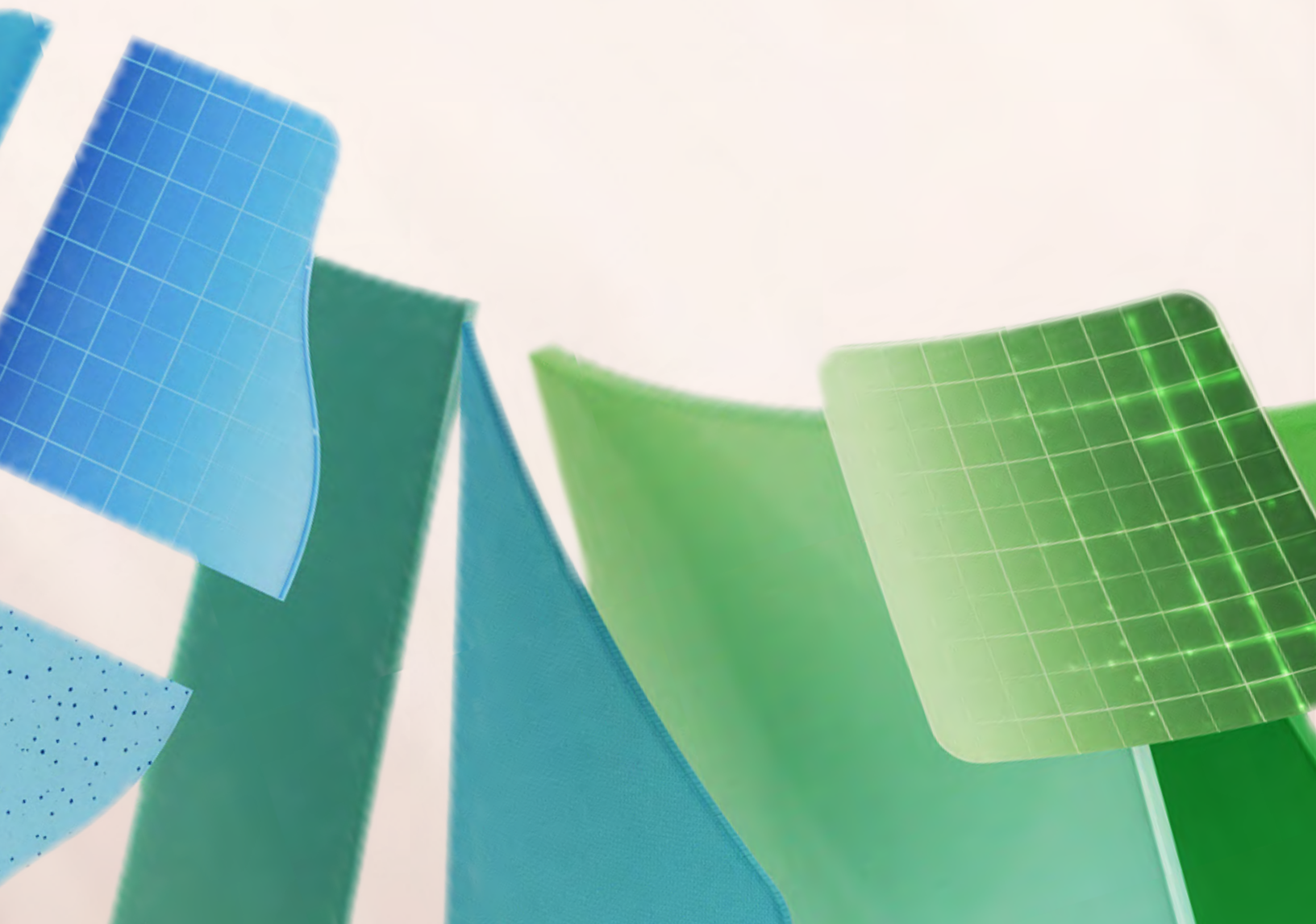


Dane pod kontrolą

Skuteczne zarządzanie danymi kluczem
do osiągnięcia sukcesu w zakresie AI



Spis treści

Wprowadzenie

Zarządzanie danymi jest podstawą bezpiecznego wdrażania rozwiązań opartych na AI

Generatywna AI może wprowadzić znaczne zmiany w przedsiębiorstwie, ale w dużej mierze zależy to od jakości i dostępności danych biznesowych.

AI może zapewnić konkurencyjną przewagę organizacjom stawiającym na solidne zarządzanie danymi. Pomaga ono zapewnić poprawność, bezpieczeństwo i kontrolę danych przesyłanych do AI i przez nią generowanych.

Jakość i dostępność danych:

Systemy AI opierają się na dużych, wysokiej jakości zestawach danych, aby zapewnić najlepszą możliwą reakcję w odpowiednim kontekście opartym na unikatowych przepływach pracy w danej organizacji. Lepsza jakość danych prowadzi do skuteczniejszych analiz i prognoz opartych na AI.

Zgodność z przepisami: solidne zarządzanie danymi zapewnia zgodność z wymogami regulacyjnymi, zmniejszając tym samym ryzyko problemów prawnych i grzywien.

Bezpieczeństwo: odpowiednie oznaczanie danych i zarządzanie nimi chroni informacje wrażliwe przed nieuprawnionym dostępem, niewłaściwym udostępnianiem i naruszeniami.

Zaufanie: wiarygodne zarządzanie danymi zwiększa zaufanie zainteresowanych stron do wyników generowanych przez AI, sprzyjając szerszemu wdrażaniu i wspieraniu inicjatyw związanych z AI.

Ten e-book zawiera opis najważniejszych praktyk w zakresie zarządzania danymi, które przygotowują organizację na rozwiązania oparte na AI. Obejmuje sposób określania solidnych standardów jakości danych, zapewniania zgodności z wymogami regulacyjnymi oraz wdrażania środków ochrony i bezpieczeństwa danych. Niezależnie od tego, czy chodzi o zapobieganie udostępnianiu poufnych treści podczas spotkań z osobami z zewnątrz, czy o zabezpieczenie przed naruszeniami ochrony danych, poznasz strategie budowania zaufania do systemów opartych na AI i udostępniania danych w celu uzyskiwania praktycznych wniosków. Dzięki wdrożeniu tych praktyk Twoja organizacja może wykorzystać cały potencjał AI do ciągłego wprowadzania innowacji i uzyskania stałej przewagi konkurencyjnej.

Przykłady użycia generatywnej AI

Przyspieszona komunikacja: szybsze tworzenie spersonalizowanych treści, aby mieć więcej czasu na budowanie relacji i współpracę.

Poprawa wydajności: ograniczanie czasu spędzanego na wykonywaniu rutynowych zadań, większa produktywność oraz obniżenie kosztów.

Budowa kultury innowacji: wspieranie generowania pomysłów i propozycji dotyczących nowych produktów i usług.

Spersonalizowana obsługa klienta: dostosowanie treści i rekomendacji w celu zwiększenia lojalności i zaangażowania klientów.

Lepsze zarządzanie danymi w celu dokonania transformacji opartej na AI

Każde przedsiębiorstwo ma własne zasady i procesy regulujące wykorzystanie danych. Ramy zarządzania danymi różnią się pod względem dojrzałości i kompleksowości, ale niewiele z nich zostało w pełni zoptymalizowanych pod kątem AI. Chociaż wiele najlepszych praktyk w zakresie zarządzania danymi, takich jak zapewnienie dokładności i spójności danych, nie ulega zmianie, inne aspekty wymagają aktualizacji w celu zmaksymalizowania inwestycji w AI. Przyjrzyjmy się kilku kluczowym obszarom.

Widoczność danych

Szczegółowa wiedza na temat przepływu danych w systemach opartych na AI umożliwia wykrywanie i ograniczanie nieupoważnionego lub niewłaściwego użycia. Taka widoczność pomaga w zapewnieniu bezpieczeństwa i zgodności z przepisami, chroniąc w ten sposób dane wrażliwe w celu maksymalizacji wartości uzyskanej dzięki AI.

Tradycyjne zarządzanie danymi koncentruje się na wiedzy o miejscu przechowywania danych i kontrolowaniu dostępu. Jednak w miarę jak AI staje się w coraz większym stopniu zintegrowana z operacjami biznesowymi, zarządzanie danymi musi nadążać za zmieniającymi się potrzebami w zakresie bezpieczeństwa. Na przykład

w przypadku wprowadzania bardzo wrażliwych produktów zarządzanie musi teraz obejmować treści generowane przez AI, zapewniając bezpieczeństwo dokumentów projektowych, komunikacji i spostrzeżeń tworzonych przez AI. Oznacza to wdrożenie zabezpieczeń gwarantujących, że tylko upoważnieni członkowie zespołu mogli uzyskać dostęp do AI i wykorzystywać ją do analizowania lub podsumowywania informacji o projekcie.

Ponadto dzięki zarządzaniu wolumenami przetwarzanych i magazynowanych danych organizacje mogą lepiej kontrolować koszty operacyjne związane z AI.

Jakość danych

AI zwiększa znaczenie wysokiej jakości danych, ponieważ ich zła jakość wpływa bezpośrednio na wyniki generowane przez AI. Stosując narzędzia oparte na AI do wykonywania zapytań o dane biznesowe, należy mieć pewność, że dane są aktualne i wiarygodne. Równie ważne jest zrozumienie pochodzenia i jakości danych wykorzystywanych przez zespół do tworzenia własnych modeli AI i aplikacji opartych na AI. Regularne audyty danych, rygorystyczne procesy sprawdzania poprawności oraz proaktywne zarządzanie pomagają zapewnić integralność danych. Koncentrując się na tych obszarach, organizacje mogą osiągać wiarygodne wyniki w zakresie AI, które stymulują podejmowanie lepszych decyzji i wprowadzanie innowacji.

Zarządzanie użytkownikami

Dzięki AI użytkownicy w wyszukany sposób korzystają z danych. Komunikują się z systemami opartymi na AI, takimi jak Microsoft 365 Copilot, za pomocą promptów w języku naturalnym. Wyposażona w uprawnienia i zabezpieczenia AI ma dostęp za pośrednictwem wtyczek do odpowiednich kontekstów wynikających z danych — takich jak pliki, czaty i wiadomości e-mail — wraz ze źródłami zewnętrznymi w celu generowania odpowiedzi.

Monitorowanie danych wykorzystywanych w tych procesach ma kluczowe znaczenie dla zapewnienia generowania prawidłowych i uzasadnionych odpowiedzi przez AI. Zapewnienie przejrzystości poprzez przytaczanie przypisów lub linków do oryginalnych źródeł pomaga użytkownikom weryfikować informacje, zmniejszając ryzyko niewłaściwego wykorzystania danych i zapewniając zgodność z przepisami.

Zgodność z przepisami i eDiscovery

Pojawienie się AI wprowadza nowe wyzwania w zakresie zgodności z przepisami i eDiscovery (systemu do obsługi danych w postępowaniach prawnych), zwłaszcza w zakresie zarządzania danymi generowanymi przez AI i dostosowywania się do zmieniających się wymagań prawnych. Aktualizacja ram zarządzania danymi w celu sprostania tym wyzwaniom obejmuje opracowanie zasad dotyczących treści generowanych przez AI, takich jak zapewnienie, że dokumenty lub komunikaty tworzone przez AI są śledzone, klasyfikowane i bezpiecznie przechowywane. Konieczne może być na przykład zaktualizowanie zasad w celu zagwarantowania, że wiadomości e-mail lub raporty generowane przez AI są odpowiednio otagowane i zarchiwizowane w celu późniejszego pobrania.

Zwiększenie możliwości systemu eDiscovery obejmuje integrację narzędzi opartych na AI, które mogą wyszukiwać i identyfikować treści generowane przez AI na różnych platformach. Na przykład podczas prowadzenia dochodzenia prawnego narzędzia eDiscovery muszą być w stanie znaleźć i pobrać określone dokumenty wygenerowane przez AI, podsumować odpowiednią komunikację i zapewnić jasne ścieżki audytu w celu potwierdzenia zgodności z przepisami. Dzięki aktualizacji tych funkcji organizacje mogą lepiej zarządzać danymi podczas audytów prawnych lub dochodzeń, zapewniając, że wszystkie istotne informacje generowane przez AI są dostępne i możliwe do obrony w sądzie.

Bezpieczeństwo danych

Zabezpieczanie operacji opartych na AI powinno obejmować zasady Zero Trust na poziomie tożsamości, co minimalizuje ryzyko nieupoważnionego dostępu. Regularne aktualizacje urządzeń klienckich, w tym urządzeń i aplikacji, zmniejszają luki w zabezpieczeniach, które mogą zostać wykorzystane. Znajomość narzędzi opartych na generatywnej AI używanych w organizacji pozwala na blokowanie nieakceptowanych lub niezabezpieczonych aplikacji, co z kolei zapobiega potencjalnym naruszeniom zabezpieczeń. Ograniczając dostęp do narzędzi i danych AI tylko do zaufanego personelu, organizacje mogą osiągnąć większą integralność danych i chronić działania operacyjne w zakresie AI przed potencjalnymi zagrożeniami.

Co to jest Zero Trust?

Zero Trust to model bezpieczeństwa, który koncentruje się na weryfikowaniu każdego żądania tak, jakby pochodziło z niezaufanej sieci. Zamiast zakładać, że wszystko w obrębie zapory korporacyjnej jest bezpieczne, w podejściu tym przyjęto zasadę „nigdy nie ufaj, zawsze weryfikuj”.

Zasady Zero Trust

Jawna weryfikacja: zawsze uwierzytelniaj i autoryzuj na podstawie wszystkich dostępnych punktów danych.

Przydzielanie dostępu z minimalnymi uprawnieniami: ograniczaj dostęp użytkowników z zastosowaniem metodyki „just-in-time” (dokładnie na czas) i „just-enough-access” (minimalne uprawnienia dostępu) (JIT/JEA), adaptacyjnych zasad bazujących na analizie ryzyka oraz ochrony danych.

Zakładanie wystąpienia naruszenia: ograniczaj szkody, kontroluj dostęp, zapewnij szyfrowanie i używaj danych do wykrywania zagrożeń i wzmacniania zabezpieczeń.

Rola zarządzania danymi w transformacji opartej na AI: pochodzenie, jakość i wiarygodność

W miarę, jak organizacje wdrażają AI w celu wspomagania decyzji biznesowych, muszą zadbać o to, aby systemy te mogły zapewnić prawidłowe i wiarygodne wyniki. Odpowiedzi AI oparte na danych muszą być dostępne, spójne i dobrze udokumentowane.

Zarządzanie danymi stanowi jeden z istotnych elementów wiarygodnej AI poprzez wdrażanie zasad zarządzania, które śledzą pochodzenie danych, sprawdzają ich jakość oraz zapewniają ich rzetelność i dokładność. Praktyki te stanowią podstawę systemów opartych na AI, które dostarczają wiarygodnych informacji, umożliwiając tym samym podejmowanie świadomych i dobrze uzasadnionych decyzji.

Pochodzenie danych: zrozumienie pochodzenia i zmian informacji

Analiza pochodzenia danych służy do śledzenia ich przepływu przez organizację, w tym do dokumentowania źródła pochodzenia, dokonanych przekształceń i miejsc docelowych danych. W przypadku przedsiębiorstw korzystających z AI zrozumienie pochodzenia danych jest niezbędne z następujących kilku powodów:

- **Transparentność:** wiedza o pochodzeniu danych i ich zmianach pomaga potwierdzić dokładność wyników generowanych przez AI i zapewnia zgodność z przepisami dzięki jasnemu zrozumieniu historii danych.
- **Identyfikowalność:** analiza pochodzenia danych umożliwia organizacjom śledzenie błędów lub niespójności u źródła, co upraszcza rozwiązywanie problemów i korygowanie danych.
- **Analiza wpływu:** zrozumienie sposobu wykorzystania danych przez narzędzia oparte na generatywnej AI pomaga ocenić potencjalny wpływ zmian w źródłach danych lub metodach przetwarzania na dokładność danych wyjściowych i wyniki biznesowe.

Jakość danych: jakość decyduje o wartości odpowiedzi AI

Jakość danych ma bezpośredni wpływ na wiarygodność danych wyjściowych generowanych przez AI. Dane o wysokiej jakości stanowią kontekst dla modeli AI do dostarczania prawidłowych i wartościowych odpowiedzi na dane wejściowe pochodzące od użytkowników. Kluczowe aspekty jakości danych to:

- **Dokładność:** dane muszą prawidłowo przedstawiać rzeczywiste warunki.
- **Kompletność:** wszystkie niezbędne dane muszą być obecne i rozliczone.
- **Spójność:** dane muszą być spójne w różnych systemach i w czasie.
- **Terminowość:** dane muszą być aktualne i dostępne w razie potrzeby.

Wiarygodność danych: zapewnienie wiarygodnych danych

Wiarygodność danych oznacza, że dane stale spełniają standardy jakości i są dostępne w razie potrzeby. W przypadku przedsiębiorstw korzystających z AI wiarygodne dane mają kluczowe znaczenie dla budowania zaufania do narzędzi opartych na AI i podejmowanych przez nie decyzji. Zapewnienie wiarygodności danych obejmuje:

- **Nadmiarowość danych:** wdrażanie systemów tworzenia kopii zapasowych, które zapobiegają utracie i zwiększają dostępność.
- **Regularne tworzenie kopii zapasowych:** wykonywanie częstych kopii zapasowych w celu ochrony przed uszkodzeniem lub utratą danych.
- **Monitorowanie i alerty:** konfigurowanie systemów monitorowania w celu wykrywania problemów z danymi i powiadamiania zainteresowanych stron w czasie rzeczywistym.
- **Plany przywracania po awarii:** opracowywanie i testowanie planów szybkiego przywracania danych i wznowiania operacji po awariach.

Relacja między zarządzaniem, bezpieczeństwem i odpowiedzialną sztuczną inteligencją

Zarządzanie danymi i bezpieczeństwo tworzą podstawę odpowiedzialnego korzystania z AI. Bezpieczne dane o wysokiej jakości zapewniają etyczne i skuteczne działanie AI. Kluczowe obszary do oceny to: klasyfikacja danych, kontrola dostępu, szyfrowanie, reagowanie na incydenty i zgodność z przepisami.

Klasyfikacja danych

Klasyfikacja danych jest kluczowym elementem kontroli sposobu, w jaki narzędzia oparte na AI obsługują informacje wrażliwe. Zazwyczaj dane i spotkania są klasyfikowane jako ogólne, poufne lub wysoce poufne. Prawidłowa klasyfikacja zapewnia, że AI ma dostęp tylko do odpowiednich informacji, co zmniejsza ryzyko ujawnienia danych wrażliwych nieupoważnionym użytkownikom.

Niewłaściwe klasyfikowanie może natomiast prowadzić do ograniczenia przetwarzania danych przez AI, a w konsekwencji do naruszeń zabezpieczeń lub problemów ze zgodnością z przepisami. Skuteczne zarządzanie danymi, czy to za pośrednictwem zautomatyzowanych narzędzi, czy zasad dotyczących użytkowników końcowych, gwarantuje, że dane są klasyfikowane prawidłowo, zabezpiecza informacje wrażliwe i zwiększa zdolność AI do dostarczania wiarygodnych i zgodnych wyników.

Środki kontroli dostępu

Te środki kontroli regulują, kto może uzyskać dostęp do danych związanych z AI i które aplikacje lub tożsamości mają uprawnienia do korzystania z tych danych. Niewystarczające środki kontroli dostępu mogą prowadzić do nieuprawnionego ujawnienia informacji wrażliwych, zwiększając ryzyko naruszeń i niewłaściwego użycia.

Zarządzanie danymi odgrywa kluczową rolę w egzekwowaniu tych środków kontroli poprzez ograniczenie dostępu do danych tylko dla upoważnionych pracowników i określonych aplikacji, zapewniając odpowiednie postępowanie z danymi wrażliwymi. Nie tylko chroni to integralność danych, ale także zapewnia działanie systemów AI na bezpiecznych, zaufanych zestawach danych, zwiększając tym samym ich wiarygodność i zgodność z przepisami.

Szyfrowanie

Zabezpieczenie danych przed przechwyceniem i naruszeniem przy użyciu szyfrowania pomaga zapewnić, że narzędzia oparte na generatywnej AI mogą zakotwiczyć swoją odpowiedź na odpowiednim kontekście — takim jak związane z pracą dane, pliki, czaty i wiadomości e-mail — bez ryzyka wycieku danych.

Zasady zarządzania danymi mogą narzucać niezawodne praktyki szyfrowania, chroniąc dane w całym cyklu ich życia. Takie podejście zapewnia, że narzędzia oparte na AI mogą dostarczać niezawodne odpowiedzi, jednocześnie zapewniając bezpieczeństwo danych i zaufanie.

Reagowanie na incydenty

Dane wrażliwe organizacji mogą być ujawniane podczas incydentów z użyciem narzędzi opartych na generatywnej AI, zapewniających nieupoważniony dostęp do plików, wiadomości e-mail lub innych danych biznesowych używanych przez systemy do generowania odpowiedzi.

Proaktywny plan reagowania na incydenty ma kluczowe znaczenie w tych scenariuszach. Bez takiego planu organizacja ryzykuje nie tylko ujawnienie danych wrażliwych, ale także korzysta z wadliwych danych wygenerowanych przez AI. Zarządzanie danymi obejmuje posiadanie szczegółowych protokołów reagowania w celu szybkiego usuwania naruszeń, minimalizowania ich skutków i zachowania niezawodności systemów AI.

Zgodność z przepisami

Aplikacje oparte na AI muszą być zgodne z przepisami, takimi jak RODO lub CCPA, dotyczącymi ochrony danych i prywatności. Nieprzestrzeganie przepisów może prowadzić do nałożenia wysokich kar i podważyć zaufanie. Ważne jest również, aby zrozumieć, gdzie narzędzia oparte na AI przetwarzają dane, ponieważ wiele bezpłatnych narzędzi może obsługiwać dane globalnie lub poza miejscami, w których firma zazwyczaj przechowuje dane. Zarządzanie danymi zapewnia, że aplikacje oparte na AI działają nie tylko w ramach prawnych, ale także przechowują dane w odpowiednich granicach usług, dostosowując je do standardów zgodności organizacji. Takie podejście wspiera etyczne korzystanie z AI i pomaga budować zaufanie do jej technologii.



Aktualizacja ram zarządzania danymi w celu bardziej efektywnego wdrażania AI

W ewoluującym środowisku AI ważne jest, aby zidentyfikować określone obszary istniejących ram zarządzania danymi, które mogą wymagać dodatkowej uwagi. Zamiast gruntownego przeglądu całych ram, można skupić się na obszarach, które prawdopodobnie będą ulegać zmianie, kierując wysiłki na działania mogące w największym stopniu zwiększyć wartość AI, jednocześnie zapewniając ochronę i bezpieczeństwo danych. Oto kilka kluczowych kwestii do rozważenia:

Dostosowywanie zasad i procedur

AI obejmuje nowe rodzaje zbierania, przetwarzania i wykorzystywania danych. Aktualizacja zasad dotyczących danych może pomóc w zaspokojeniu potrzeb związanych z prywatnością, zgodnością z przepisami i etycznym wykorzystaniem danych. Na przykład wymóg anonimizacji danych w określonych przypadkach może chronić dane osobowe, dzięki czemu korzystanie z nich w całym cyklu życia AI jest bezpieczniejsze.

Role i obowiązki

Konieczne jest uwzględnienie gotowości wszystkich ról związanych z zarządzaniem danymi do wdrażania rozwiązań opartych na AI. Pracownicy zaznajomieni z wymaganiami dotyczącymi danych AI mogą pełnić rolę osób odpowiedzialnych za jakość danych i ich zgodność z przepisami. Międzydyscyplinarna współpraca zespołów ds. prawnych, IT i analityki danych może pomóc w skuteczniejszym radzeniu sobie z wyzwaniami związanymi z AI.

Dostosowanie standardów i definicji danych

Standaryzacja formatów danych, definicji i wskaźników jakości upraszcza wdrażanie zasad regulujących korzystanie z narzędzi opartych na AI w organizacji. Jasne standardy w zakresie danych ułatwiają wybór zestawów danych wykorzystywanych przez narzędzia AI do zapewniania kontekstu biznesowego i przesyłanych przez użytkowników do analizy. Gwarantuje to, że aplikacje oparte na AI korzystają z najbardziej odpowiednich i wiarygodnych danych, zwiększając ich efektywność przy jednoczesnym zapewnieniu zgodności z zasadami obowiązującymi w organizacji.

Ciągłe doskonalenie

Zarządzanie danymi jest procesem ciągłym, szczególnie w przypadku AI. Regularne audyty i aktualizacje ram zarządzania mogą pomóc w dostosowaniu ich do nowych rozwiązań opartych na AI i zmian przepisów. AI jako taka może służyć do sprawdzania i ulepszania praktyk w zakresie zarządzania, wykrywania potencjalnych luk i sugerowania usprawnień. To proaktywne podejście zwiększa zgodność z przepisami i wydajność wraz z rozwojem technologii AI.

Narzędzia i techniki skutecznego zarządzania danymi

Dostosowanie do celów biznesowych:

upewnij się, że Twoja strategia zarządzania danymi wspiera cele organizacyjne, aby usprawnić podejmowanie decyzji i zwiększyć wydajność.

Automatyzacja rutynowych zadań:

używaj automatyzacji do wykonywania powtarzalnych zadań, takich jak klasyfikacja danych i zarządzanie dostępem, w celu zmniejszenia liczby ręcznych błędów i poprawy bezpieczeństwa.

Zapewnienie wysokich standardów

dokładności: używaj narzędzi do sprawdzania poprawności i czyszczenia w celu zapewnienia integralności danych w czasie.

Szkolenie użytkowników: oferuj szkolenia w zakresie narzędzi i procedur zarządzania danymi w celu zapobiegania niewłaściwemu zarządzaniu i zapewnienia zgodności z zasadami.

Przeprowadzanie regularnych

audytów: przeglądaj regularnie praktyki dotyczące danych, aby dopasować je do zmian zachodzących w przepisach i organizacji.

Wnioski

Wykorzystanie Microsoft 365 do efektywnego zarządzania danymi w celu wdrożenia rozwiązań opartych na AI

Odpowiedzialne korzystanie z AI wymaga solidnego zarządzania danymi. Efektywne zarządzanie danymi zapewnia dostępność, dokładność i bezpieczeństwo danych, umożliwiając AI dostarczanie wiarygodnych informacji i wspieranie innowacji. Nadanie priorytetu jakości danych, zgodności z przepisami i bezpieczeństwu zwiększa możliwości AI, usprawnia podejmowanie decyzji i pozwala zachować przewagę nad konkurencją.

Microsoft 365: zwiększanie gotowości na rozwiązania oparte na AI

Microsoft 365 oferuje najlepsze w swojej klasie aplikacje zwiększające produktywność z wbudowanymi narzędziami do klasyfikacji, kontroli i ochrony danych. Funkcje te wspierają ramy zarządzania danymi, ułatwiając wdrożenie AI w firmie w momencie, gdy jest na to gotowa. Microsoft 365 pozwala zapewnić:

- **Jakość danych:** zapewnienie dokładności i niezawodności danych wyjściowych generowanych przez AI.
- **Zgodność z przepisami:** przestrzeganie wymogów regulacyjnych i mniejsze ryzyko prawne.
- **Bezpieczeństwo Zero Trust:** ochrona informacji wrażliwych przed nieupoważnionym dostępem, naruszeniami i cyberzagrożeniami.

Odkryj kompleksowe narzędzia zwiększające produktywność, wzbogacone o opcje AI i solidną ochronę, które pomogą Twojej organizacji pracować wydajnie i bezpiecznie.



Poznaj rozwiązanie Microsoft 365