AI Literacy i Polityka AI – jak uporządkować korzystanie ze sztucznej inteligencji w MŚP? Część II

W poprzednim artykule pisałam o tym, kogo dotyczy AI Literacy z art. 4 AI Act, jak ją zrealizować w czterech krokach zaproponowanych przez AI Office oraz jakie pułapki, Shadow AI, RODO i halucynacje, pojawiają się w firmach najczęściej. Zakończyłam zapowiedzią, że Politykę AI, czyli dokument, który porządkuje cały ten proces w jednym miejscu, omówię osobno. Czas dotrzymać słowa! Jednak zanim przejdę do sedna, kilka słów o tym co zmieniło się w stanie prawnym…

Digital Omnibus on AI

W poprzednim artykule (części I) pisałam o Digital Omnibus jako akcie oczekującym na publikację. Ten etap mamy już za sobą. Wspomniany akt prawny został opublikowany w Dzienniku Urzędowym UE w dniu 24 lipca 2026 r. i wszedł w życie 27 lipca 2026 r. Dla przedsiębiorców istotne są cztery następujące zmiany.

Po pierwsze, zmieniono brzmienie art. 4 AI Act. Tak jak sygnalizowałam, dotychczasowa formuła, akcentująca zapewnienie wystarczającego poziomu kompetencji została zastąpiona formułą „podejmowania środków wspierających rozwój kompetencji". Nowy art. 4 ust. 2 AI Act zobowiązuje Komisję i państwa członkowskie do wspierania firm, w szczególności MŚP, praktycznymi przykładami i wytycznymi, a art. 4 ust. 3 przewiduje rekomendacje Rady ds. AI określające wspólne cele w zakresie AI Literacy.

Po drugie, przesunięto terminy dla systemów wysokiego ryzyka. Obowiązki dotyczące systemów samodzielnych z Załącznika III do AI Act (wszystkie omówiłam w artykule: Systemy wysokiego ryzyka) zaczną obowiązywać w przesuniętym terminie od 2 grudnia 2027 r., a systemów stanowiących elementy bezpieczeństwa produktów z Załącznika I do AI Act od 2 sierpnia 2028 r. Z kolei termin na uruchomienie przez państwa członkowskie krajowych piaskownic regulacyjnych przesunięto na 2 sierpnia 2027 r. (o piaskowniach regulacyjnych pisałam tutaj przy okazji omawiania polskiej ustawy o systemach sztucznej inteligencji: Ustawa o systemach sztucznej inteligencji i piaskownice regulacyjne).

Po trzecie i to co szczególnie istotne z uwagi na datę 2 sierpnia 2026 r., nie przesunięto obowiązków przejrzystości z art. 50 AI Act. Od 2 sierpnia 2026 r. szczególne znaczenie mają obowiązki przejrzystości z art. 50 AI Act. Trzeba przy tym odróżnić obowiązki dostawców od obowiązków podmiotów stosujących. Dostawcy systemów AI muszą m.in. projektować systemy w taki sposób, aby osoba fizyczna była informowana o interakcji z AI oraz zapewniać oznaczenia treści syntetycznych w przypadkach przewidzianych w przepisie. Podmioty stosujące muszą natomiast m.in. informować osoby poddane działaniu systemów rozpoznawania emocji lub kategoryzacji biometrycznej, ujawniać deepfake'i oraz oznaczać określone teksty wygenerowane lub zmanipulowane przez AI, jeżeli są publikowane w celu informowania opinii publicznej o sprawach leżących w interesie publicznym i nie przeszły ludzkiej weryfikacji ani kontroli redakcyjnej. Co pomocne, Komisja Europejska opublikowała wytyczne dotyczące art. 50 AI Act oraz dobrowolny kodeks postępowania w zakresie oznaczania treści generowanych przez AI. Warto do nich sięgnąć przy projektowaniu wewnętrznych zasad oznaczania treści, choć sam kodeks nie zastępuje obowiązków wynikających z AI Act.

Po czwarte, rozszerzono katalog praktyk zakazanych z art. 5 AI Act. Mianowicie dodano zakaz wykorzystywania systemów AI do generowania lub manipulowania materiałami intymnymi oraz materiałami przedstawiającymi seksualne wykorzystywanie małoletnich. Nowe zakazy stosuje się od 2 grudnia 2026 r.

Do tego warto odnotować, że 24 lipca Prezydent podpisał ustawę o systemach sztucznej inteligencji, powołującą Komisję Rozwoju i Bezpieczeństwa Sztucznej Inteligencji jako organ nadzoru. Przewodniczący KRiBSI ma zostać powołany w terminie dwóch miesięcy od wejścia w życie ustawy, a sama Komisja ma rozpocząć działalność w ciągu trzech miesięcy. Więcej o ustawie pisałam w artykule pod linkiem: Ustawa o systemach sztucznej inteligencji.

Co powinna zawierać Polityka AI?

Polityka AI jest praktycznym i dowodowym sposobem wykazania, że firma podjęła środki organizacyjne wspierające AI Literacy. Nie chodzi więc o tworzenie dokumentu dla samego dokumentu, lecz o uporządkowanie odpowiedzialności, narzędzi, danych, zasad weryfikacji wyników i reakcji na incydenty. Kolejność działań pozostaje ta sama, o której pisałam w części I, zatem najpierw budowanie świadomości i szkolenie, a potem Polityka AI jako ich utrwalenie.

Poniżej przedstawiam 10 elementów, które warto wprowadzić do Polityki AI dla małej i średniej firmy. Zakres tych elementów należy jednak każdorazowo dostosować do roli firmy w rozumieniu AI Act, inaczej będzie wyglądała polityka podmiotu wyłącznie stosującego gotowe narzędzia, a inaczej firmy, która rozwija, wdraża lub udostępnia własne systemy AI. Żaden przepis nie narzuca konkretnej treści takiego dokumentu, a przedstawione poniżej wyliczenie stanowi zestaw odpowiadający na mogące pojawić się pytania organów bądź kontrahentów.

1. Cel Polityki oraz kogo obowiązuje.

   Zakres podmiotowy powinien wprost obejmować nie tylko pracowników etatowych, ale również współpracowników B2B, stażystów, podwykonawców i dostawców usług, jeżeli korzystają z systemów AI w imieniu firmy lub w związku z realizacją powierzonych zadań, ponieważ art. 4 AI Act posługuje się formułą *„innych osób zajmujących się obsługą i użytkowaniem systemów AI w ich imieniu”*. W zakresie przedmiotowym warto przesądzić, że polityka dotyczy każdego korzystania z AI w celach służbowych, także z konta prywatnego i na sprzęcie prywatnym.

2. Jaką rolę pełni firma i z jakich narzędzi AI korzysta.

   Polityka powinna przesądzać, czy firma występuje jako podmiot stosujący, dostawca, importer, dystrybutor etc. czy też łączy kilka ról jednocześnie oraz zawierać rejestr używanych narzędzi AI, najlepiej w załączniku, aby jego aktualizacja nie wymagała zmiany całego dokumentu. Dla każdego narzędzia odnotowujemy: nazwę i dostawcę, cel stosowania, właściciela biznesowego, plan licencyjny, informację o tym, czy dane wejściowe są wykorzystywane do trenowania modelu, lokalizację przetwarzania danych oraz kategorię ryzyka według AI Act. Rejestr ten jest jednocześnie dowodem realizacji pierwszego i trzeciego kroku schematu AI Office opisanego w części I.

3. Tryb dopuszczania nowych narzędzi do użytku.

   Element najczęściej pomijany, a decydujący o tym, czy polityka przeżyje co najmniej sześć miesięcy. Rynek narzędzi AI zmienia się szybciej niż jakikolwiek dokument wewnętrzny, dlatego zamiast zamkniętej listy warto wprowadzić prostą procedurę: narzędzia dopuszczone (lista otwarta, aktualizowana przez wyznaczoną osobę), narzędzia wymagające zgody przed użyciem oraz narzędzia zakazane. Do tego krótki formularz zgłoszenia, czyli kilka pytań o cel, rodzaj danych i dostawcę oraz ścieżka akceptacji z

terminem odpowiedzi. Bez tego pracownicy nie przestaną sięgać po nowe narzędzia, a przestaną jedynie o nich mówić. Przy narzędziach wykorzystywanych w procesach dotyczących klientów, pracowników, rekrutacji, oceny wyników pracy, kredytowania, ubezpieczeń, edukacji lub bezpieczeństwa warto wprowadzić obowiązkową ścieżkę konsultacji prawnej lub compliance przed dopuszczeniem narzędzia.

4. Co wolno, a czego nie wolno wpisywać do AI.

   Zamiast ogólników w rodzaju „*należy zachować ostrożność*" warto nazwać konkretne kategorie informacji, których nie wolno wprowadzać do narzędzi zewnętrznych bez odrębnej zgody: dane osobowe klientów, kontrahentów i pracowników, treści objęte umowami o zachowaniu poufności, dane finansowe i cenniki, kod źródłowy, dokumentację techniczną, informacje stanowiące tajemnicę przedsiębiorstwa oraz dane o toczących się sporach i negocjacjach, chyba że korzystanie z danego narzędzia zostało wcześniej ocenione i dopuszczone pod kątem RODO, bezpieczeństwa informacji oraz umów z dostawcą. Równolegle warto wskazać zastosowania zalecane, np. redagowanie tekstów wewnętrznych, burza mózgów czy streszczanie materiałów jawnych, ponieważ polityka, która wyłącznie zakazuje, buduje Shadow AI zamiast go ograniczać.

5. Weryfikacja wyników i zasada „*ostatnie słowo zawsze należy do człowieka*".

   Zasada weryfikacji wyniku AI przez kompetentnego człowieka powinna być zapisana jako bezwzględny standard operacyjny, a nie zalecenie, pisałam o tym w części I przy okazji halucynacji. Warto wskazać procesy, w których weryfikacja jest obowiązkowa i udokumentowana, np. pisma procesowe, oferty handlowe, dokumentacja techniczna, komunikacja z klientem, treści publikowane. Osobno należy zapisać, że procesy prowadzące do decyzji wywołujących skutki prawne lub podobnie istotnie wpływających na osoby fizyczne wymagają szczególnej oceny pod kątem art. 22 RODO, w tym tego, czy nie dochodzi do niedopuszczalnego wyłącznie zautomatyzowanego podejmowania decyzji.

6. Kiedy trzeba oznaczyć, że treść powstała z AI.

   Polityka powinna określać, które obowiązki z art. 50 AI Act dotyczą firmy w jej konkretnej roli (dostawcy albo podmiotu stosującego, ew. obu tych ról). W praktyce może to obejmować m.in. informowanie użytkowników chatbota na stronie firmy, że rozmawiają z systemem AI, ujawnianie deepfake'ów, oznaczanie określonych tekstów wygenerowanych lub zmanipulowanych przez AI publikowanych w celu informowania opinii publicznej o sprawach leżących w interesie publicznym oraz zachowanie oznaczeń maszynowo odczytywalnych przy dalszej obróbce materiałów. Warto też wskazać, kto weryfikuje, czy nowo wdrażane narzędzie w ogóle takie oznaczenia generuje.

7. Co z danymi osobowymi i RODO?

   Polityka AI nie zastępuje dokumentacji RODO, ale musi być z nią spójna. Minimum to podstawa prawna przetwarzania tam, gdzie dane osobowe faktycznie trafiają do narzędzia, wymóg zawarcia umowy powierzenia z dostawcą, weryfikacja lokalizacji przetwarzania i transferów poza EOG, uwzględnienie narzędzi AI w rejestrze czynności przetwarzania oraz wskazanie przypadków wymagających oceny skutków dla ochrony danych (DPIA).

8. Kto w firmie odpowiada za AI.

AI Act nie wymaga powołania „*inspektora ds. AI*" ani żadnej szczególnej struktury zarządczej. Firma powinna jednak potrafić wykazać, kto odpowiada za aktualizację zasad, rejestr narzędzi i organizację działań szkoleniowych. Wystarczy wyznaczyć jedną osobę odpowiedzialną za rejestr narzędzi, akceptację nowych rozwiązań i coroczny przegląd dokumentu oraz punkt kontaktowy dla pracowniczych wątpliwości.

9. Co zrobić, gdy coś pójdzie nie tak?

   Polityka powinna opisywać, co zrobić, gdy narzędzie AI wygeneruje wynik błędny, szkodliwy lub dyskryminujący, gdy do modelu trafią dane, które nie powinny były tam trafić, albo gdy pojawi się podejrzenie naruszenia praw autorskich, praw do baz danych czy tajemnicy przedsiębiorstwa. Kluczowe są trzy rzeczy: komu zgłaszamy, w jakim terminie i jak dokumentujemy. Warto powiązać tę ścieżkę z procedurą naruszeń ochrony danych osobowych i zapisać zasadę braku sankcji wobec osoby, która zgłosi incydent samodzielnie i niezwłocznie, inaczej incydenty nie będą zgłaszane.

10. AI Literacy

    Ostatni rozdział zamyka klamrę z częścią I. Polityka powinna opisywać, kto, kiedy i w jakim zakresie przechodzi szkolenia, przewidywać moduł AI w onboardingu oraz nakazywać prowadzenie prostego rejestru działań szkoleniowych (data, temat, forma, lista uczestników, materiały). To właśnie rejestr działań szkoleniowych, materiały szkoleniowe i potwierdzenia udziału, a nie sama Polityka AI, będą najważniejszym dowodem podjęcia środków wymaganych przez znowelizowany art. 4.

Jak wdrożyć Politykę AI?

Sama treść to najwyżej połowa sukcesu, ponieważ o skuteczności polityki decyduje sposób jej wprowadzenia do organizacji. Punktem wyjścia jest formalna podstawa, polityka powinna być wprowadzona w sposób właściwy dla danej organizacji, z datą, wskazaniem osoby odpowiedzialnej i udokumentowanym zakomunikowaniem. Równie istotne jest zebranie od pracowników i współpracowników oświadczeń o zapoznaniu się z polityką, w formie papierowej lub elektronicznej, przechowywanych razem z rejestrem szkoleń.

Rozesłanie dokumentu w załączniku do wiadomości e-mail zwykle nie wystarczy, natomiast godzinne spotkanie, na którym omówione zostaną trzy realne przykłady z danej firmy, działa lepiej niż najdłuższe opracowanie, którego nikt nie otworzy. Trzeba też pamiętać o zapewnieniu alternatywy, jeżeli bowiem zakazujemy korzystania z darmowych kont prywatnych, musimy w zamian udostępnić narzędzie firmowe. Zakaz bez alternatywy generuje Shadow AI, a więc dokładnie to ryzyko, które chcemy ograniczyć. Na koniec warto spojrzeć poza własną organizację i rozważyć wprowadzenie do umów z podwykonawcami klauzuli zobowiązującej ich do stosowania polityki lub równoważnych zasad, co ma szczególne znaczenie w agencjach, branży IT oraz przy outsourcingu procesów.

Polityka AI nie jest dokumentem, który da się napisać raz i schować do segregatora, jest natomiast narzędziem porządkującym coś, co w firmach dzieje się już dziś, najczęściej poza jakąkolwiek kontrolą. Kilka dobrze napisanych stron, realnie omówionych z zespołem i przeglądanych raz do roku, daje więcej niż kilkudziesięciostronicowe opracowanie, którego nikt nie przeczytał.

Jeżeli mają Państwo wątpliwości jak wprowadzić obowiązki wynikające z AI Act czy jak wprowadzić Politykę AI w swojej organizacji, zapraszam do konsultacji.