PARP Grupa PFR / Centrum Rozwoju MŚP

Link do nagrania webinarium

SZTUCZNA INTELIGENCJA W SEKTORZE MŚP

Jak bezpiecznie i legalnie wykorzystywać sztuczną inteligencję dla rozwoju biznesu?

Katarzyna Krzywicka, LL.M

13.10.2026

Webinarium zostało zrealizowane przez Polską Agencję Rozwoju Przedsiębiorczości,
w ramach projektu Centrum Rozwoju Małych i Średnich Przedsiębiorstw.

PARP Grupa PFR / Centrum Rozwoju MŚP

Plan prezentacji:

1. AI w codziennej pracy firmy - przegląd narzędzi i prawny punkt widzenia. Jak legalnie korzystać ze sztucznej inteligencji, aby wspierać wzrost biznesu i nie łamać prawa?
2. Gdzie kryje się haczyk? Analiza umów i regulaminów dostawców AI. Jak dostawcy popularnych narzędzi przenoszą odpowiedzialność na użytkownika i na co bezwzględnie uważać przed kliknięciem „akceptuję”?
3. Prawa autorskie i dane osobowe w erze generatywnego AI. Do kogo należą wygenerowane treści i grafiki oraz jak chronić tajemnice firmy i dane klientów (RODO) przy wpisywaniu promptów?
4. Polityka bezpiecznego korzystania z AI Jak krok po kroku stworzyć i wdrożyć jasne zasady dla pracowników, które zabezpieczą firmę przed wyciekiem danych i stratami finansowymi?
5. Aktualne zmiany w prawie i Unijny Akt o AI (AI Act) Spojrzenie z perspektywy przedsiębiorcy na regulacje obowiązujące od 2 sierpnia 2026 roku, co realnie zmienia się dla sektora MŚP i jak przygotować na to firmę?
6. Sesja Q&A.

PARP Grupa PFR / Centrum Rozwoju MŚP

Link do agendy

Sztuczna inteligencja w sektorze MSP

Jak bezpiecznie i legalnie wykorzystywać AI dla rozwoju biznesu?

PRODUKTYWNOŚĆ => BEZPIECZEŃSTWO

AI przyspiesza pracę. Ale czy firma nadąża z ochroną danych?

- AI zwiększa produktywność i skraca czas wykonywania powtarzalnych zadań.
- Pomaga analizować informacje, tworzyć treści, przygotowywać zestawienia i wspierać obsługę klientów.
- Dla wielu firm AI staje się elementem codziennej pracy.

- Jednocześnie rośnie obawa o dane, poufność, bezpieczeństwo i odpowiedzialność prawną.
- Największym wyzwaniem nie jest samo wdrożenie AI, lecz wdrożenie jej w sposób kontrolowany.

Dwie drogi korzystania z AI w firmie:

Jawnie i transparentnie firma wie:

- z jakich narzędzi korzystają pracownicy,
- określa dopuszczalne cele i zakres użycia,
- zapewnia odpowiednie konta, dostęp i szkolenia.

Nieformalnie i poza kontrolą pracownicy korzystają z narzędzi na własną rękę:

- używają prywatnych kont,
- przesyłają dane bez wiedzy firmy,
- firma dowiaduje się o tym dopiero po wystąpieniu problemu.

Jeżeli firma nie ustali zasad korzystania z AI, pracownicy ustalą je sami

Brak oficjalnych narzędzi nie oznacza braku korzystania z AI.

→ Pracownik, który chce szybciej wykonać zadanie, może sięgnąć po ogólnodostępny chatbot, generator grafiki lub narzędzie do analizy dokumentów.

Problemem nie jest wyłącznie to, że pracownik korzysta z AI. Problemem jest to, że firma często nie wie:

- z jakiego narzędzia,
- w jakim celu i na jakich danych korzysta pracownik.

Shadow AI – niewidzialna warstwa technologiczna firmy

Shadow AI to korzystanie z narzędzi sztucznej inteligencji bez formalnej zgody, wiedzy lub kontroli organizacji.

Narzędzie może być używane:

- na prywatnym koncie pracownika,
- bez weryfikacji regulaminu dostawcy,
- bez oceny, gdzie trafiają dane,
- bez ustalenia, kto ponosi odpowiedzialność za wynik.

Shadow AI często zaczyna się niewinnie: od chęci zaoszczędzenia kilku minut.

Shadow AI w praktyce: prywatne konto pracownika

- Firma nie udostępniła pracownikom zatwierdzonych narzędzi AI.
- Pracownica chciała usprawnić wysyłkę wiadomości do wielu kontaktów.
- Skorzystała z prywatnego konta w narzędziu AI.
- Wprowadziła dane potrzebne do przygotowania tabeli i organizacji wysyłki.

Firma nie miała kontroli nad:

- zakresem wprowadzonych danych,
- ustawieniami konta,
- okresem przechowywania informacji,
- możliwością wykorzystania danych przez dostawcę.

Trzy typowe scenariusze ryzyka shadow AI

- Prywatne konto i dane firmowe pracownik wprowadza do chatbota dane klientów, kontrahentów lub pracowników.
- Nieznana integracja pracownik podłącza narzędzie AI do poczty, dysku, kalendarza lub systemu CRM, nie wiedząc, jaki zakres danych uzyskuje aplikacja.
- Automatyzacja bez kontroli AI przygotowuje wiadomości, zestawienia lub rekomendacje, które są wysyłane dalej bez weryfikacji człowieka.

W każdym z tych przypadków firma może utracić kontrolę nad danymi, komunikacją i decyzją biznesową.

Najdroższy błąd AI często zaczyna się od niewinnego promptu

„Przygotuj tabelę z tymi klientami”.

„Przeanalizuj tę umowę”.

„Napisz odpowiedź na reklamację”.

„Podsumuj wyniki pracowników”.

„Oceń, który kandydat najlepiej pasuje do stanowiska”.

Każde z tych poleceń może oznaczać przekazanie danych osobowych, informacji poufnych albo tajemnicy przedsiębiorstwa.

Dane osobowe to nie tylko imię i nazwisko

Zgodnie z art. 4 pkt 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, czyli RODO, danymi osobowymi są informacje o osobie zidentyfikowanej lub możliwej do zidentyfikowania bezpośrednio albo pośrednio.

Mogą to być między innymi:

- imię i nazwisko,
- adres e-mail,
- numer telefonu,
- numer klienta,
- adres IP lub identyfikator internetowy,
- dane lokalizacyjne,
- informacje o sytuacji ekonomicznej,
- informacje o zdrowiu, zachowaniu lub relacjach zawodowych.

Dane osobowe mogą wynikać również z kontekstu, a nie tylko z pojedynczej informacji.

Jeżeli połączenie kilku informacji pozwala ustalić, kogo dotyczą, nadal może chodzić o dane osobowe.

Prompt jest również operacją na danych

- Wklejenie dokumentu do narzędzia AI może oznaczać:
  - zebranie danych,
  - ich przesłanie,
  - przechowywanie,
  - analizowanie,
  - połączenie z innymi informacjami.

RODO szeroko definiuje przetwarzanie danych osobowych - obejmuje ono między innymi wykorzystywanie, przeglądanie, modyfikowanie, przesyłanie i udostępnianie danych.

Przed wpisaniem danych do narzędzia trzeba zadać pytanie: czy te dane są niezbędne? kto otrzyma te dane? jak długo będą przechowywane?

Zasada minimalizacji danych

Do narzędzia AI przekazujemy wyłącznie dane niezbędne do wykonania konkretnego zadania.

- Nie wklejamy całego dokumentu, jeżeli wystarczy jego fragment.
- Nie wklejamy danych osobowych.
- Usuwamy informacje, które nie mają znaczenia dla polecenia.

RODO wymaga, aby dane były adekwatne, stosowne i ograniczone do tego, co niezbędne dla celu przetwarzania.

Minimalizacja danych powinna być pierwszym filtrem przed każdym promptem.

Anonimizacja – kiedy dane przestają być danymi osobowymi?

Anonimizacja ma prowadzić do trwałego uniemożliwienia identyfikacji osoby.

Samo usunięcie imienia i nazwiska nie zawsze wystarcza. Należy usunąć lub zmienić również informacje, które w połączeniu mogą wskazać konkretną osobę.

Trzeba uważać na:

- unikalne stanowisko,
- dokładną datę i miejsce zdarzenia,
- numer klienta,
- charakterystyczny opis sytuacji,
- połączenie kilku pozornie nieistotnych informacji.

Pseudonimizacja to nie anonimizacja

Pseudonimizacja polega na zastąpieniu identyfikatorów innymi oznaczeniami, na przykład numerem lub kodem.

Jeżeli dzięki dodatkowym informacjom można ponownie przypisać dane do konkretnej osoby, dane nadal pozostają danymi osobowymi.

Przykład: „Jan Kowalski” zostaje zastąpiony oznaczeniem „Klient 001”, ale firma nadal posiada tabelę pozwalającą ustalić, kim jest „Klient 001”.

Pseudonimizacja zmniejsza ryzyko.

Bezpieczne techniki pracy z danymi

- Maskowanie danych.
- Praca na danych syntetycznych.
- Generalizacja danych.
- Dodawanie szumów losowych.
- Tokenizacja.

Ochrona danych już na etapie projektowania

Bezpieczeństwo powinno być uwzględnione przed uruchomieniem narzędzia AI, a nie dopiero po incydencie.

Firma powinna ustalić:

- jakie dane mogą być wprowadzane,
- do jakich narzędzi,
- przez których pracowników,
- w jakich celach,
- z jakimi ograniczeniami.

RODO wymaga uwzględniania ochrony danych już przy projektowaniu sposobu przetwarzania oraz stosowania domyślnej ochrony danych.

Pseudonimizacja, ograniczenie dostępu i minimalizacja danych powinny być elementem procesu, a nie reakcją kryzysową.

Zasady gry dla AI.

Firma powinna stworzyć prostą i praktyczną politykę korzystania z AI.

Polityka powinna odpowiadać na pięć pytań:

- z jakich narzędzi wolno korzystać?
- jakich danych nie wolno wprowadzać?
- kiedy konieczna jest zgoda lub konsultacja?
- kto weryfikuje wynik AI?
- co zrobić w przypadku błędu lub incydentu?

Pracownik powinien wiedzieć nie tylko, czego nie wolno robić. Powinien również wiedzieć, jak bezpiecznie wykonać zadanie z użyciem AI.

Minimalny model odpowiedzialnego korzystania z AI

- Zidentyfikuj cel - po co używasz AI?
- Ogranicz dane - jakie informacje są naprawdę konieczne?
- Sprawdź narzędzie - kto jest dostawcą i co dzieje się z danymi?
- Zweryfikuj wynik - czy odpowiedź AI jest prawidłowa, kompletna i zgodna z prawem?
- Zachowaj kontrolę człowieka - AI wspiera proces, ale nie przejmuje odpowiedzialności.

Firma odpowiada za sposób, w jaki korzysta z AI

Administrator powinien wdrożyć środki techniczne i organizacyjne odpowiednie do ryzyka oraz być w stanie wykazać ich stosowanie.

Ochrona danych obejmuje nie tylko system informatyczny, lecz także:

- uprawnienia,
- pracowników,
- szkolenia,
- procedury,
- kontrolę dostępu,
- reagowanie na incydenty,
- wybór dostawcy.

Podsumowanie: od shadow AI do odpowiedzialnego AI

AI może wspierać wzrost biznesu, ale tylko wtedy, gdy firma zachowuje kontrolę.
Największe ryzyka dotyczą:

- danych osobowych,
- tajemnicy przedsiębiorstwa,
- poufności komunikacji,
- halucynacji,
- niekontrolowanych integracji (API)i.

Najbezpieczniejszy kierunek to:

- zatwierdzone narzędzia,
- minimalizacja danych,
- odpowiednie zabezpieczenia,
- szkolenia,
- jasna odpowiedzialność.

Link do agendy

Gdzie kryje się haczyk?

Regulamin dostawcy AI nie jest wyłącznie instrukcją obsługi. To często połączenie:

- warunków korzystania z usługi,
- zasad dotyczących danych,
- polityki prywatności,
- zasad wykorzystania treści,
- ograniczeń odpowiedzialności,
- warunków płatności i rozwiązania umowy.

Kliknięcie „akceptuję” może oznaczać zawarcie umowy na warunkach, których użytkownik nigdy dokładnie nie przeczytał.

Nie analizujemy konkretnego regulaminu. Analizujemy mechanizm

Regulaminy dostawców AI szybko się zmieniają. Zmieniają się również:

- funkcje narzędzi,
- modele rozliczeń,
- zasady przechowywania danych,
- ustawienia dotyczące trenowania modeli,
- rozwiązania techniczne i lokalizacja infrastruktury.

Dlatego ważniejsza od zapamiętania jednego regulaminu jest umiejętność zadawania właściwych pytań.

Najpierw ustalmy: z jakiego rozwiązania korzystamy?

Czy jest to:

- publiczny chatbot,
- narzędzie dla użytkowników biznesowych,
- rozwiązanie wdrażane lokalnie,
- model open source,
- narzędzie podłączone do systemów firmy.

Najpierw ustalmy: z jakiego rozwiązania korzystamy?

Czy narzędzie działa samodzielnie, czy ma dostęp do:

- poczty elektronicznej,
- dysku firmowego,
- CRM,
- kalendarza,
- systemu księgowego,
- dokumentów pracowników i klientów?

Im więcej integracji, tym większy zakres ryzyka i tym dokładniej trzeba ustalić przepływ danych.

Regulamin to nie wszystko

Oprócz głównych warunków korzystania trzeba sprawdzić:

- politykę prywatności,
- politykę przechowywania danych,
- dokumentację bezpieczeństwa,
- warunki dla klientów biznesowych,
- umowę powierzenia przetwarzania danych,
- listę podwykonawców,
- zasady korzystania z API,
- zasady zmian dokumentacji.

AI przyspiesza pracę. Ale czy firma nadąża z ochroną danych?

Pierwsze pytanie brzmi: co dzieje się z naszymi danymi? Czy dane są:

- przechowywane,
- analizowane,
- wykorzystywane do poprawy usługi,
- wykorzystywane do trenowania modelu,
- przekazywane podwykonawcom?

Czy dostawca rozróżnia:

- dane wprowadzane przez użytkownika,
- prompty,
- załączniki,
- wygenerowane odpowiedzi,
- dane techniczne i logi?

Czy dane są wykorzystywane wyłącznie do wykonania usługi, czy także do innych celów?

Czy można wyłączyć trenowanie danych?

W regulaminie lub ustawieniach trzeba sprawdzić:

- czy dane użytkownika są wykorzystywane do trenowania modeli,
- czy można wyłączyć takie wykorzystanie,
- czy wyłączenie działa domyślnie czy dopiero po zmianie ustawień,
- czy dotyczy wszystkich danych, czy tylko części funkcji,
- czy dotyczy również danych przekazywanych przez API,
- czy obejmuje dane historyczne.

Samo zapewnienie, że „dane są chronione”, nie odpowiada jeszcze na pytanie, czy są wykorzystywane do rozwoju modelu.

Wyłączenie trenowania danych powinno być sprawdzone, skonfigurowane i udokumentowane.

Dane wejściowe, dane wyjściowe i dane techniczne

Dane wejściowe:

- prompty,
- dokumenty,
- pliki,
- obrazy,
- nagrania,
- informacje wpisywane przez pracownika.

Dane wejściowe, dane wyjściowe i dane techniczne

Dane wyjściowe:

- tekst,
- grafika, video, głos
- kod,
- analiza,
- rekomendacja,
- automatycznie wygenerowany dokument.

Dane wejściowe, dane wyjściowe i dane techniczne

Dane techniczne:

- identyfikator konta,
- adres IP,
- informacje o urządzeniu,
- historia korzystania,
- logi bezpieczeństwa.

Każda z tych kategorii może podlegać innym zasadom przechowywania, usuwania i wykorzystywania.

Gdzie znajdują się serwery i kto przetwarza dane?

Trzeba sprawdzić:

- gdzie znajduje się infrastruktura dostawcy,
- gdzie mogą być przechowywane dane,
- z jakich państw działają podwykonawcy,
- czy dane są przekazywane poza Europejski Obszar Gospodarczy,
- jakie mechanizmy transferowe stosuje dostawca.

Należy ustalić, czy dostawca działa jako:

- administrator danych,
- podmiot przetwarzający,
- niezależny dostawca usługi przetwarzający określone dane we własnych celach.

W przypadku przetwarzania danych osobowych umowa i konfiguracja usługi powinny odpowiadać wymogom RODO, w tym zasadzie bezpieczeństwa przetwarzania.

Chmura czy rozwiązanie lokalne?

Rozwiązanie chmurowe:

dane są przekazywane do infrastruktury dostawcy, firma musi przeanalizować dostęp dostawcy i jego podwykonawców, ważne są zasady retencji, transferu i usuwania danych.

Rozwiązanie lokalne lub prywatne:

większa kontrola nad infrastrukturą, większa odpowiedzialność za aktualizacje, bezpieczeństwo i utrzymanie, konieczność samodzielnego zarządzania dostępem i logami. Lokalizacja serwera nie rozwiązuje automatycznie wszystkich problemów prawnych. Kontrola nad infrastrukturą jest ważna, ale równie ważna jest kontrola nad procesem korzystania z narzędzia.

Do kogo należą dane wyjściowe?

Regulamin może:

- przyznawać użytkownikowi określone prawa do outputu,
- przyznawać je „w zakresie dopuszczalnym przez prawo”,
- nie regulować tej kwestii wprost,
- zastrzegać, że podobny output może otrzymać inny użytkownik.

Trzeba odróżnić:

- prawa wynikające z umowy z dostawcą,
- prawa autorskie do konkretnego rezultatu,
- możliwość uzyskania ochrony prawnoautorskiej,
- ryzyko, że output przypomina cudzy utwór.

Zgodnie z art. 1 ustawy o prawie autorskim i prawach pokrewnych utworem jest przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci.

Sam fakt wygenerowania treści przez narzędzie nie przesądza więc automatycznie o powstaniu pełnych praw autorskich do rezultatu.

„Masz prawa do outputu” nie znaczy „output jest wolny od ryzyka”

Dostawca może przyznać użytkownikowi prawa umowne do korzystania z wygenerowanego rezultatu.

Nie oznacza to automatycznie, że:

- rezultat jest oryginalny,
- nie przypomina cudzego utworu,
- nie narusza znaku towarowego,
- nie wykorzystuje chronionego wizerunku,
- może być bezpiecznie użyty w reklamie lub produkcie.

Autorskie prawa majątkowe obejmują wyłączne prawo do korzystania z utworu, rozporządzania nim i wynagrodzenia za korzystanie. Dlatego output przed publikacją powinien zostać zweryfikowany przez człowieka.

Dane treningowe i prawa twórców

Modele generatywne mogą być trenowane na dużych zbiorach tekstów, obrazów, nagrań i innych materiałów.

- W prawie Unii Europejskiej dyskutuje się, w jakim zakresie trenowanie modeli mieści się w eksploracji tekstów i danych oraz kiedy wymagany jest legalny dostęp do wykorzystywanych treści - dyrektywa DSM.
- AI Act nakłada na dostawców modeli AI ogólnego przeznaczenia obowiązek prowadzenia polityki zgodności z prawem autorskim oraz respektowania zastrzeżeń praw, czyli mechanizmów opt-out.
- Dostawcy takich modeli mają również sporządzać i publikować streszczenia treści wykorzystanych do trenowania modelu.
- Dla użytkownika oznacza to potrzebę sprawdzenia, czy dostawca przedstawia jakiekolwiek informacje o źródłach danych i polityce praw autorskich.

Czy dostawca bierze odpowiedzialność za naruszenia?

Trzeba sprawdzić, czy regulamin zawiera:

- gwarancję dostawcy dotyczącą legalności usługi,
- zobowiązanie do obrony użytkownika przed roszczeniami,
- obowiązek pokrycia kosztów lub odszkodowania,
- wyłączenia odpowiedzialności za output,
- ograniczenie odpowiedzialności do wysokości opłat.

Jeżeli dostawca wyłącza odpowiedzialność, ryzyko pozostaje po stronie firmy korzystającej z narzędzia.

Odpowiedzialność użytkownika za dane i rezultat

Użytkownik może odpowiadać za:

- legalność danych wejściowych,
- posiadanie odpowiednich praw do dokumentów,
- zgodność promptów z prawem,
- sposób wykorzystania outputu,
- publikację wygenerowanych treści.

Nie należy zakładać, że dostawca sprawdzi każdy dokument lub wynik wygenerowany przez AI.

Czy dostawca gwarantuje poufność?

Regulamin powinien odpowiedzieć na pytania: kto ma dostęp do danych,

- czy pracownicy dostawcy mogą przeglądać treści,
- kiedy możliwy jest dostęp administracyjny,
- czy dane są szyfrowane,
- jak długo przechowywane są logi,
- czy dostawca może ujawnić dane organom publicznym,
- czy firma zostanie poinformowana o takim żądaniu.

Jeżeli narzędzie będzie przetwarzało dane osobowe, środki techniczne i organizacyjne powinny odpowiadać ryzyku.

Co dzieje się po usunięciu konta?

Trzeba sprawdzić:

- czy dane są usuwane,
- w jakim terminie,
- czy kopie zapasowe są również usuwane,
- czy dane pozostają w logach,
- czy dostawca może zachować dane ze względów prawnych,
- czy firma może wyeksportować prompty i outputy.

Warto ustalić procedurę na wypadek:

- zakończenia współpracy,
- zmiany dostawcy,
- incydentu bezpieczeństwa,
- zamknięcia konta,
- przejęcia dostawcy przez inną spółkę.

Brak procedury wyjścia może oznaczać uzależnienie firmy od jednego dostawcy.

Dostępność usługi i awarie

Regulamin powinien określać:

- dostępność usługi,
- czas reakcji na awarię,
- wsparcie techniczne,
- sposób zgłaszania incydentów,
- zasady rekompensaty,
- odpowiedzialność za utratę danych.

Czy dostawca może jednostronnie zmienić regulamin?

Trzeba sprawdzić:

- w jaki sposób dostawca informuje o zmianach,
- z jakim wyprzedzeniem,
- czy zmiana może objąć dane już przekazane,
- czy firma może wypowiedzieć umowę,
- co dzieje się przy braku akceptacji nowych warunków.

Ważne jest ustalenie wersji dokumentów obowiązujących w momencie uruchomienia usługi.

Regulamin dostawcy AI - checklista

Model usługi publiczny, biznesowy, API, lokalny czy zintegrowany?

- Dane co jest zbierane, przechowywane i analizowane?
- Trenowanie czy można wyłączyć wykorzystanie danych do treningu?
- Lokalizacja gdzie są serwery i podwykonawcy?
- RODO kto jest administratorem, a kto podmiotem przetwarzającym?
- Prawa do inputu i outputu jakie licencje otrzymuje dostawca i jakie prawa ma użytkownik?
- Odpowiedzialność kto ponosi ryzyko błędu, naruszenia lub wycieku?
- Bezpieczeństwo jakie są zabezpieczenia, audyty i procedury incydentowe?
- Wyjście z usługi czy można odzyskać dane i usunąć je z systemu?

Nie pytajmy tylko: „Czy możemy korzystać z tego narzędzia?”

Pytajmy również:

- na jakich danych?
- w jakim celu?
- na jakich warunkach?
- kto ponosi ryzyko?
- co stanie się w przypadku błędu?
- czy możemy bezpiecznie odejść od dostawcy?

Dopiero odpowiedzi na te pytania pozwalają ocenić, czy narzędzie jest odpowiednie dla firmy.

Podsumowanie części drugiej

Regulamin dostawcy AI trzeba analizować z perspektywy:

- danych,
- praw autorskich,
- poufności,
- odpowiedzialności,
- bezpieczeństwa,
- ciągłości działania.

Największe ryzyko pojawia się wtedy, gdy firma:

- nie wie, jakie dane przekazuje,
- nie sprawdza zasad trenowania,
- zakłada, że output zawsze jest legalny,
- akceptuje szerokie wyłączenie odpowiedzialności,
- nie ma planu zakończenia współpracy.

Przed kliknięciem „akceptuję” trzeba wiedzieć nie tylko, co narzędzie potrafi, ale również co firma oddaje dostawcy.

Link do agendy

III CZĘŚĆ

Prawa autorskie i dane osobowe w erze generatywnej AI

- Do kogo należy treść wygenerowana przez AI?
- Czy prompt może być utworem?
- Kiedy człowiek tworzy utwór przy wykorzystaniu AI?
- Jak chronić dane osobowe, informacje poufne i tajemnice przedsiębiorstwa?
- AI może być narzędziem twórczym, ale nie zastępuje człowieka jako twórcy.

Czym jest utwór?

Utworem jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci.

Ochrona obejmuje sposób wyrażenia, a nie sam pomysł, metodę, procedurę czy ideę.

Utwór może mieć formę:

- tekstu,
- grafiki,
- zdjęcia,
- muzyki,
- filmu,
- programu komputerowego,
- projektu lub prezentacji.

Ochrona powstaje bez konieczności rejestracji lub spełnienia formalności.

Nie wszystko, co wygenerowane, jest utworem

Sam rezultat działania algorytmu nie przesądza jeszcze o powstaniu utworu.

- Kluczowe pytanie brzmi: czy w rezultacie można dostrzec twórcze i indywidualne decyzje człowieka?
- Jeżeli człowiek nie miał rzeczywistego wpływu na sposób wyrażenia rezultatu, ochrona prawnoautorska może być kwestionowana.
- Jeżeli człowiek dokonał twórczych wyborów, rezultat może podlegać ochronie – każdorazowo wymaga to indywidualnej oceny.

Człowiek, AI i rezultat twórczy

AI może pełnić funkcję:

- narzędzia,
- asystenta,
- generatora wersji roboczych,
- źródła inspiracji,
- elementu procesu twórczego.

Człowiek, AI i rezultat twórczy

Człowiek może zachować twórczy charakter pracy poprzez:

- wybór koncepcji,
- opracowanie struktury,
- dobór parametrów,
- selekcję rezultatów,
- redakcję,
- montaż,
- postprodukcję,
- połączenie outputu z własnymi elementami.

Im większa kontrola człowieka nad ostatecznym kształtem, tym silniejszy argument za istnieniem ludzkiego wkładu twórczego.

Prompt nie zawsze jest tylko poleceniem

Krótki prompt typu:

- „napisz reklamę produktu”,
- „stwórz logo”,
- „podsumuj dokument”, zwykle nie będzie samodzielnym utworem.

Rozbudowany prompt może jednak zawierać: oryginalną koncepcję,

- twórczą strukturę,
- charakterystyczny styl,
- szczegółową kompozycję,
- indywidualny sposób opisania oczekiwanego rezultatu.

W takim przypadku prompt może samodzielnie spełniać przesłanki utworu, jeżeli jest przejawem twórczej działalności o indywidualnym charakterze.

Prompt może być częścią procesu twórczego, ale nie każdy prompt jest utworem

O ochronie nie decyduje długość promptu. Decyduje jego twórczy i indywidualny charakter.

Warto zachowywać:

- wersje promptów,
- daty ich utworzenia,
- kolejne modyfikacje,
- wybrane rezultaty,
- informacje o własnej redakcji i postprodukcji.

Taka dokumentacja może pomóc wykazać zakres ludzkiego wkładu w powstanie końcowego rezultatu.

Co oznacza „postprodukcja”?

Postprodukcja może obejmować:

- wybór fragmentów wygenerowanego materiału,
- zmianę kompozycji,
- redakcję tekstu,
- stworzenie własnego układu,
- montaż obrazu lub dźwięku,
- dodanie własnych elementów,
- korektę kolorystyczną,
- opracowanie typografii,
- połączenie kilku materiałów w nową całość.

Jeżeli te czynności mają twórczy charakter, mogą prowadzić do powstania chronionego rezultatu. Sama techniczna korekta błędów nie zawsze będzie wystarczająca.

Przykład: tekst wygenerowany przez AI

Firma zleca AI przygotowanie artykułu. Pracownik:

- opracowuje własną tezę,
- buduje strukturę tekstu,
- wybiera argumenty,
- usuwa błędne fragmenty,
- dodaje własne przykłady,
- nadaje tekstowi indywidualny styl.

Ochrona może dotyczyć ludzkiego wkładu i ostatecznej kompozycji, a nie samego automatycznie wygenerowanego surowego outputu.

Nie można jednak automatycznie uznać całego tekstu za utwór pracownika bez zbadania jego rzeczywistego wkładu.

Przykład: grafika wygenerowana przez AI

Firma generuje kilkadziesiąt propozycji grafiki. Następnie człowiek:

- wybiera jeden wariant,
- zmienia układ elementów,
- dodaje własne ilustracje,
- modyfikuje kolory i typografię,
- łączy grafikę z własnym projektem.

Prawnie istotny może być twórczy wkład w końcową kompozycję.

Ryzyko pozostaje wtedy, gdy wygenerowana grafika przypomina cudzy utwór, znak towarowy lub charakterystyczną twórczość konkretnego artysty.

Prawo do outputu nie jest tym samym co pewność ochrony

Regulamin dostawcy może przyznawać użytkownikowi określone prawa umowne do korzystania z outputu.

Nie oznacza to automatycznie, że:

- output jest utworem,
- użytkownik jest jego twórcą,
- rezultat jest oryginalny,
- rezultat nie narusza cudzych praw.

Prawo autorskie przysługuje twórcy, a autorskie prawa majątkowe obejmują wyłączne korzystanie z utworu i rozporządzanie nim.

Umowa z dostawcą nie może sama stworzyć ochrony prawnoautorskiej tam, gdzie brakuje twórczego wkładu człowieka.

Output może naruszać cudze prawa

Wygenerowana treść może:

- przypominać istniejący utwór,
- zawierać cudzy fragment tekstu,
- wykorzystywać charakterystyczny styl lub kompozycję,
- przedstawiać cudzy wizerunek,
- zawierać lub naśladować znak towarowy,
- zawierać chroniony element.

Output może naruszać cudze prawa

Przed publikacją trzeba sprawdzić:

- źródła wykorzystane przez człowieka,
- podobieństwo do znanych utworów,
- prawa do zdjęć, grafik, muzyki etc.

Podobieństwo nie zawsze oznacza naruszenie!

Czy można używać cudzych materiałów jako promptu?

Samo posiadanie dostępu do tekstu, zdjęcia lub grafiki nie oznacza posiadania prawa do “wklejenia” treści do AI.

Link do agendy

IV CZĘŚĆ

Do okienka konwersacyjnego można wpisać dane osobowe, nawet jeśli nie wpisujemy imienia i nazwiska

Dane osobowe mogą być ukryte w:

- treści reklamacji,
- historii choroby,
- umowie,
- korespondencji e-mail,
- nagraniu rozmowy,
- tabeli wyników pracowników.

Przed wysłaniem materiału do AI trzeba ocenić całość kontekstu, a nie tylko pojedyncze pola.

Dane wejściowe, dane treningowe i output

W systemach AI mogą występować różne kategorie danych:

- dane treningowe,
- dane walidacyjne i testowe,
- dane wejściowe,
- dane referencyjne,
- dane wyjściowe.

Prompt lub załączony dokument może zostać: przetworzony, poddany tokenizacji, zwektoryzowany, połączony z historią rozmowy, zapisany w logach, wykorzystany zgodnie z ustawieniami usługi.

Dlatego nie należy zakładać, że dane znikają natychmiast po wygenerowaniu odpowiedzi.

Co dzieje się z danymi po ich wprowadzeniu do AI?

Tracimy nad nimi kontrolę.

Pseudonimizacja nie oznacza, że RODO przestaje działać

Zastąpienie imienia i nazwiska “kodem” nie wystarcza, jeżeli firma zachowuje możliwość ponownego przypisania kodu do osoby.

Tajemnica przedsiębiorstwa to nie tylko dane osobowe

Do narzędzia AI można przypadkowo przekazać:

- strategię cenową,
- listę klientów,
- warunki negocjowanych umów,
- know-how,
- kod źródłowy,
- plany produktowe,
- dane finansowe,
- informacje o trwających sporach,
- niepubliczne wyniki sprzedaży.

Informacja może nie być daną osobową, ale nadal mieć wysoką wartość gospodarczą.

PARP Grupa PFR / Centrum Rozwoju MŚP

Jak chronić tajemnicę przedsiębiorstwa przy korzystaniu z AI?

Stosować techniki pracy z danymi.

Techniki ograniczania ryzyka

- Minimalizacja – przekazujemy tylko dane niezbędne do celu.
- Maskowanie – ukrywamy część informacji.
- Pseudonimizacja – zastępujemy identyfikatory kodami.
- Anonimizacja – usuwamy możliwość identyfikacji osoby.
- Agregacja – przekazujemy dane zbiorcze zamiast rekordów jednostkowych.
- Dane syntetyczne – korzystamy ze sztucznie wygenerowanych danych testowych.
- Szyfrowanie – chronimy dane podczas przesyłania i przechowywania.

Anonimizacja nie jest magicznym przyciskiem „usuń ryzyko”

Anonimizacja musi uniemożliwiać identyfikację osoby w sposób trwały i realny.

AI a halucynacje

AI może:

- pomylić fakty,
- stworzyć nieistniejące źródło,
- błędnie zinterpretować dokument,
- pominąć istotny fragment,
- powielić błąd z danych treningowych, w tym bias.

Dokumentujmy ludzki wkład

Warto zachować:

- pierwotny pomysł,
- prompt,
- kolejne wersje,
- własne materiały,
- decyzje,
- redakcję i poprawki,
- finalną wersję.

Polityka bezpiecznego korzystania z AI

- Jak stworzyć zasady korzystania ze sztucznej inteligencji w organizacji?
- Jak przyjmować nowe narzędzia, jak wygląda proces weryfikacji?
- Jak chronić dane, informacje poufne i interesy firmy?
- Jak szkolić pracowników i monitorować stosowanie zasad?
- Art. 4 AI ACI - tzw. klauzula kompetencyjna.

Czym jest polityka bezpiecznego korzystania z AI?

To wewnętrzny dokument określający:

- jakie narzędzia AI mogą być używane - listy, weryfikacja,
- to nie jest polityka incydentów RODO,
- kto może je wdrażać i zatwierdzać,
- jak kontrolujemy ich działanie.

Polityka łączy: zasady prawne, cyberbezpieczeństwo, ochronę danych, wartości organizacji i odpowiedzialność biznesową.

Powinna być zrozumiała dla pracowników i możliwa do zastosowania w codziennej pracy.

Czym polityka AI nie jest?

- Nie jest polityką ochrony danych osobowych.
- Nie zastępuje dokumentacji wymaganej przez RODO.
- Nie jest wyłącznie procedurą reagowania na incydenty.
- Nie jest instrukcją informatyczną dla działu IT.

Nie twórzmy dokumentu do szuflady, czyli największy grzech polityki…

Polityka AI powinna odpowiadać na rzeczywiste problemy pracowników.

Polityka powinna wynikać z rozmowy z organizacją

Nie powinna być narzucona wyłącznie przez dział prawny lub IT.

Najpierw pytamy, jak ludzie pracują.
Dopiero potem piszemy zasady.

Polityka powinna być oparta na praktyce organizacji, a nie na abstrakcyjnym katalogu zakazów.

Warto przeprowadzić anonimową ankietę:

- z jakich narzędzi korzystasz?
- do jakich zadań?
- na jakich danych?
- czy używasz prywatnego konta?
- czego potrzebujesz, aby korzystać z AI bezpiecznie?

Incydenty związane z AI

Incydentem może być:

- ujawnienie danych w promptach,
- użycie prywatnego konta,
- nieuprawniona integracja,
- wygenerowanie błędnej informacji dla klienta,
- naruszenie praw autorskich,
- dyskryminujący rezultat - HR!
- utrata kontroli nad kontem,
- podejrzana aktywność narzędzia.

Incydenty związane z AI

Polityka powinna wskazywać:

- komu zgłosić incydent,
- w jakim czasie,
- jakie informacje przekazać,
- kto ocenia skutki,
- kiedy należy odłączyć narzędzie,
- kiedy uruchomić procedurę naruszenia ochrony danych.

Art. 4 AI ACT

Szkolenia powinny obejmować zasady bezpiecznego korzystania z AI, obsługa narzędzie to zdecydowanie za mało.

Szkolenia:

Szkolenie powinno być dopasowane do roli:

- zarząd potrzebuje wiedzy o odpowiedzialności i ryzyku,
- pracownicy operacyjni potrzebują zasad promptowania oraz aspektów prawnych,
- IT potrzebuje zasad bezpieczeństwa (prawo do kodu) i integracji.

AI Act wiąże kompetencje AI z rozumieniem możliwości, ograniczeń, ryzyk, prywatności, błędów algorytmicznych i deepfake'ów.

Kto odpowiada za politykę?

Zarząd - odpowiada za politykę.

Managerowie: pilnują przestrzegania zasad przez zespoły.

Pracownicy: korzystają z AI zgodnie z polityką i zgłaszają incydenty.

Właściciel polityki

Należy wyznaczyć osobę lub zespół odpowiedzialny za:

- aktualizację dokumentu,
- przegląd rejestru narzędzi,
- przyjmowanie zgłoszeń,
- organizację szkoleń,
- kontakt z dostawcami,
- raportowanie do zarządu.

W komentarzach do AI Act wskazuje się na przydatność wewnętrznego przedstawiciela ds. AI, który może łączyć kompetencje techniczne, prawne, etyczne i biznesowe.

Funkcja ta nie musi być odrębnym stanowiskiem, ale odpowiedzialność musi być jasno przypisana.

Link do agendy

AI Act – regulacja oparta na ryzyku

AI Act nie wprowadza jednej zasady dla wszystkich narzędzi. Obowiązki zależą między innymi od:

- rodzaju systemu,
- jego przeznaczenia,
- poziomu ryzyka,
- roli podmiotu w łańcuchu AI,
- wpływu systemu na prawa osób.

W organizacji trzeba odróżnić:

- dostawcę systemu,
- podmiot stosujący system,
- dostawcę modelu ogólnego przeznaczenia,
- użytkownika końcowego.

Art. 50 AI Act – przejrzystość interakcji

Jeżeli osoba fizyczna wchodzi w interakcję z systemem AI, powinna otrzymać informację, że ma do czynienia z AI.

Dotyczy to w szczególności:

- chatbotów,
- voicebotów,
- wirtualnych asystentów,
- automatycznej obsługi klienta,
- narzędzi komunikujących się z klientem lub pracownikiem.

Informacja powinna być przekazana w sposób jasny i odpowiednio wcześnie.

Użytkownik nie powinien być wprowadzany w błąd co do tego, czy rozmawia z człowiekiem, czy z systemem AI.

Przykład: chatbot na stronie internetowej

- Przed pierwszą interakcją z osobą fizyczną.
- Użytkownik wie, że odpowiedzi są generowane automatycznie, dostępna jest możliwość kontaktu z człowiekiem.
- “Rozmawiasz z wirtualnym asystentem AI” - nazwa asystenta nie powinna tworzyć mylnego wrażenia, że jest to konkretna osoba.

Art. 50 AI Act – pomidory i latające smoki

AI Act przewiduje obowiązki przejrzystości dotyczące treści syntetycznych.

W przypadku sztucznie wygenerowanych lub zmanipulowanych:

- obrazów,
- nagrań audio,
- nagrań wideo,
- innych materiałów przedstawiających rzeczywiste osoby, miejsca lub zdarzenia, należy rozważyć odpowiednie ujawnienie ich sztucznego charakteru.

Celem jest ograniczenie ryzyka, że odbiorca uzna materiał wygenerowany przez AI za autentyczny.

Tekst wygenerowany przez AI - czy zawsze trzeba go oznaczać?

Nie każdy tekst przygotowany z pomocą AI będzie wymagał identycznego oznaczenia.

Należy ocenić:

- czy tekst jest publikowany jako informacja dla odbiorców,
- czy dotyczy spraw publicznych - ważny jest kontekst,
- odpowiedzialność redakcyjna oraz weryfikacja tekstu (profesjonalny osąd).

Wyjątek: treść poddana kontroli człowieka

W przypadku tekstów publikowanych w celu informowania odbiorców znaczenie ma charakter materiału i zakres ludzkiej redakcji.

Jeżeli człowiek:

- samodzielnie opracował treść,
- zweryfikował informacje,
- nadał materiałowi ostateczny kształt,
- ponosi odpowiedzialność za publikację, zakres obowiązku oznaczenia może wymagać indywidualnej oceny.

Oznaczenie cyfrowe - odczyt maszynowy

- AI Act przewiduje również techniczne rozwiązania zwiększające wykrywalność treści wygenerowanych przez AI.
- Dostawcy systemów generujących treści powinni dążyć do tego, aby wyniki były oznaczane w formacie odpowiednim do odczytu maszynowego.
- Taki znacznik nie zastępuje czytelnej informacji dla człowieka.

Oznaczenie dla maszyny nie zastępuje oznaczenia dla odbiorcy

Metadane mogą zostać:

- usunięte,
- zmienione,
- utracone przy konwersji pliku,
- niewidoczne dla odbiorcy.

Dlatego organizacja powinna rozróżniać:

- oznaczenie widoczne dla człowieka,
- oznaczenie techniczne,
- dokumentację procesu tworzenia treści.

Przy publikacji trzeba ustalić, jakie informacje odbiorca powinien otrzymać i w jakiej formie.

Co art. 50 AI Act zmienia?

- Oznaczenia deepfaków.
- Oznaczenia tekstów.
- Chatboty, emailboty i voiceboty.
- Umowy z dostawcami!

Kodeks bezpiecznego korzystania z AI

- Korzystamy tylko z zatwierdzonych narzędzi.
- Nie wpisujemy do AI danych, których firma nie może ujawnić.
- Minimalizujemy, maskujemy i anonimizujemy dane.
- Sprawdzamy regulamin i zasady dostawcy.
- Weryfikujemy każdy istotny output.
- Nie podejmujemy decyzji wyłącznie dlatego, że tak zasugerowała AI.
- Oznaczamy interakcję z AI, jeżeli odbiorca powinien o niej wiedzieć.
- Oznaczamy treści syntetyczne i deepfake’i.
- Dokumentujemy ludzki wkład i proces zatwierdzania.
- Każdy incydent zgłaszamy, nawet jeżeli początkowo wydaje się nieistotny.

SESJA Q&A

PARP Grupa PFR / Centrum Rozwoju MŚP

Dziękuję za udział w webinarium, które zostało zrealizowane w ramach projektu Centrum Rozwoju Małych i Średnich Przedsiębiorstw.

Kontakt:

Katarzyna Krzywicka

tel.: +48 794509753

e-mail: kontakt@krzywicka.pl