Grant Thornton

Jak wdrożyć Agenta AI do transkrypcji spotkań zgodnie z RODO i AI Act?

Agenci AI do transkrypcji spotkań rewolucjonizują pracę zespołową, ale ich wdrożenie wiąże się z poważnymi ryzykami prawnymi, szczególnie w kontekście RODO i nadchodzącego AI Act. Automatyczne rejestrowanie i przetwarzanie rozmów, często zawierających dane wrażliwe, wymaga stosowania odpowiednich środków bezpieczeństwa i kontrolowania dostępu do informacji.

Agenci AI wspierający transkrypcję spotkań stają się coraz bardziej popularnym elementem pracy zespołowej. Dołączają do spotkań online jako widoczny uczestnik lub działają poprzez wtyczki w przeglądarce, rejestrując dźwięk, identyfikując rozmówców i generując transkrypcje w czasie rzeczywistym. Po zakończeniu spotkania automatycznie tworzą podsumowania, listy zadań i kluczowych ustaleń, a dzięki integracjom z CRM czy Slackiem potrafią wpisywać te informacje bezpośrednio do firmowych systemów.

Dla wielu użytkowników ich obecność jest wręcz niezauważalna – agenci bywają skonfigurowani tak, aby automatycznie dołączać do spotkań zapisanych w kalendarzu. Ich pojawienie się w organizacjach przynosi wymierne korzyści: poprawę dokładności notatek, ułatwienie pracy osobom z niepełnosprawnościami oraz wsparcie uczestników, którzy nie mogli pojawić się na spotkaniu. Jednocześnie jednak korzystanie z takich narzędzi wiąże się z istotnymi ryzykami prawnymi i organizacyjnymi, w szczególności w kontekście ochrony prywatności. Zrozumienie działania tych narzędzi jest kluczowe, aby świadomie oceniać, jakie dane są przez nie zbierane i jakie obowiązki wynikają z ich stosowania.

Topowe narzędzia AI do transkrypcji spotkań

Oprócz agentów wbudowanych w popularne aplikacje biurowe, na rynku dostępni są również wyspecjalizowani dostawcy, w tym firmy europejskie – według rankingów Fangoweb **do najpopularniejszych narzędzi AI do transkrypcji spotkań należą Otter.ai, Fireflies.ai, Fathom, Sembly AI oraz tl;dv**. Ranking ten oparty jest na liczbie aktywnych użytkowników oraz dostępności kluczowych funkcji wspierających transkrypcję i analizę spotkań online.

Agenci AI do transkrypcji spotkań a RODO

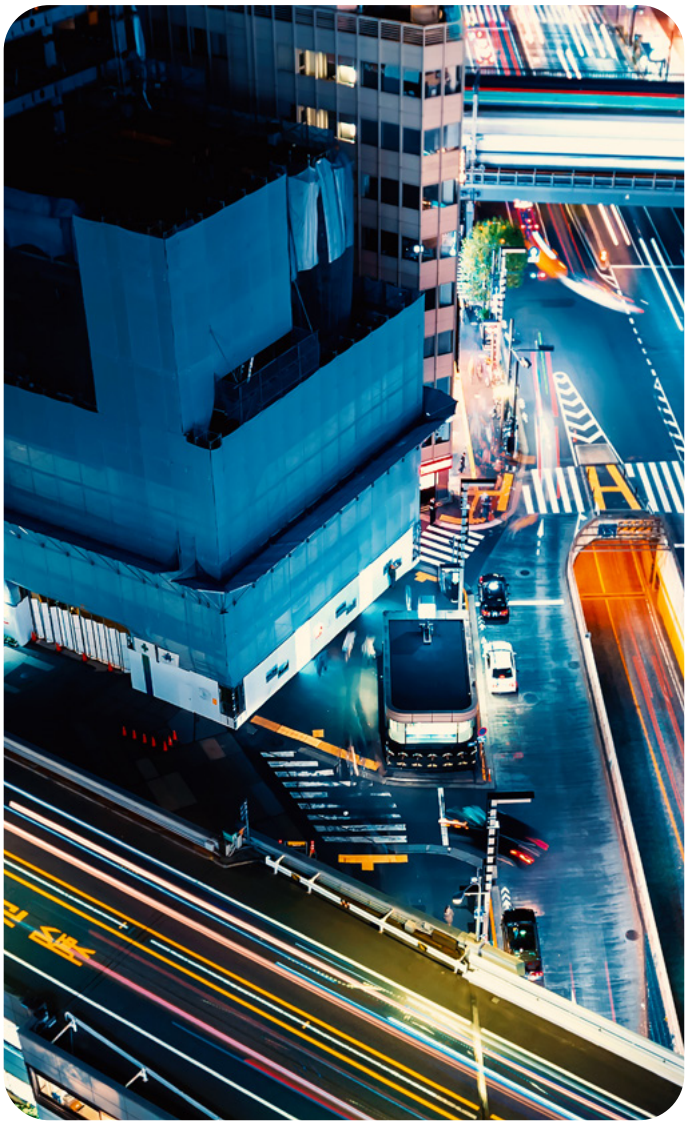
Agenci transkrypcyjni niemal zawsze przetwarzają dane osobowe. Obejmuje to nie tylko głosy mówców, lecz także całą treść rozmów, które nierzadko zawierają poufne informacje. To powoduje szereg obowiązków wynikających z przepisów prawa, w szczególności RODO, które błędnie są postrzegane jako bariera dla rozwoju. W rzeczywistości regulacja ta pomaga uporządkować sposób, w jaki nowe technologie przetwarzają dane osobowe, wprowadzając jasne zasady odpowiedzialności, przejrzystości oraz kontroli nad danymi. Gdy zrozumiemy, w jaki sposób wymogi RODO przekładają się na konkretne rozwiązania, to wdrażanie takich technologii staje się znacznie prostsze i bezpieczniejsze.

1. Poufność i bezpieczeństwo

Transkrybowane rozmowy bardzo często zawierają informacje wykraczające poza podstawowe informacje identyfikacyjne uczestników. Mogą to być dane klientów, informacje handlowe, wewnętrzne strategie, dane finansowe, a także treści dotyczące zdrowia, zatrudnienia lub ocen pracowniczych. W momencie, gdy agent AI zapisuje te informacje w formie transkrypcji, dochodzi do ich utrwalenia i dalszego przetwarzania, co znacząco podnosi poziom ryzyka. Z punktu widzenia RODO oznacza to obowiązek zapewnienia odpowiednich środków technicznych i organizacyjnych, w szczególności:

- **Ograniczenia dostępu do transkrypcji** – dostęp powinny mieć wyłącznie osoby, które faktycznie potrzebują treści nagrania do realizacji swoich zadań.
- **Szyfrowania danych** – – zarówno w trakcie transmisji (in transit), jak i ich przechowywania (at rest), aby minimalizować ryzyko nieautoryzowanego dostępu.
- **Kontroli uprawnień** – w tym regularnego przeglądu ról i poziomów dostępu oraz mechanizmów uwierzytelniania
- **Określenia jasnych okresów retencji** – ustalenia, jak długo transkrypcje są przechowywane oraz wdrożenia procedury ich bezpiecznego usuwania po upływie tego okresu.

Organizacja powinna również rozważyć, czy każda kategoria spotkań faktycznie wymaga transkrypcji, ponieważ zasada minimalizacji danych wymaga, aby agent AI przetwarzał wyłącznie informacje niezbędne do jasno określonego celu.



2. Obowiązek informacyjny wobec uczestników

Drugim istotnym aspektem jest konieczność poinformowania uczestników o tym, że w spotkaniu uczestniczy agent AI dokonujący transkrypcji. Zasada przejrzystości przetwarzania danych, będąca jednym z filarów RODO, wymaga, aby osoby, których dane są przetwarzane, miały świadomość tego faktu oraz rozumiały jego zakres i cel. W praktyce oznacza to, że uczestnicy spotkania powinni zostać poinformowani przed rozpoczęciem transkrypcji, że rozmowa będzie utrwalana przez system AI, w jakim celu tworzona jest transkrypcja, jak długo dane będą przechowywane oraz kto będzie miał do nich dostęp. Taka informacja powinna być sformułowana w sposób jasny i zrozumiały. Brak odpowiedniego poinformowania uczestników może prowadzić do uznania przetwarzania za niezgodne z prawem

3. Administrator i podmiot przetwarzający

Trzecim obszarem, który często budzi wątpliwości, są kwestie związane z powierzeniem przetwarzania i dostępem do danych. W kontekście agentów AI do transkrypcji kluczowe znaczenie ma ustalenie, kto faktycznie dostarcza technologię, kto pełni rolę administratora danych, a kto jest podmiotem przetwarzającym. W większości przypadków administratorem danych pozostaje organizacja, której przedstawiciel decyduje o uruchomieniu transkrypcji, natomiast dostawca agenta AI działa jako procesor, przetwarzając dane w imieniu administratora. Taki model wymaga umowy powierzenia, która precyzyjnie określa zakres danych, środki bezpieczeństwa, zasady ich usuwania danych oraz ewentualne dalsze podpowierzenie. Równie istotne jest ustalenie, gdzie dane są przechowywane, a w szczególności, czy pozostają na terenie Unii Europejskiej lub czy są przekazywane do państw trzecich, ponieważ w tym drugim przypadku może być konieczne zastosowanie dodatkowych mechanizmów ochrony danych, takich jak standardowe klauzule umowne, oraz weryfikacja, czy poziom ochrony zapewniany przez dostawcę odpowiada wymogom RODO.

4. Weryfikacja dostawcy

Przed wykorzystaniem agentów AI do transkrypcji organizacja powinna zweryfikować, czy dostawca przeprowadził odpowiednie testy bezpieczeństwa dotyczące agentów AI do transkrypcji oraz danych przetwarzanych w ramach ich działania. W kontekście agentów AI wbudowanych w narzędzia pracy szczególnego znaczenia nabiera odporność na nieautoryzowany dostęp do transkrypcji, możliwość odtworzenia treści spotkań przez osoby trzecie oraz zabezpieczenia przed nadużyciami wewnętrznymi. Organizacja powinna opierać się nie tylko na ogólnych zapewnieniach dostawcy, lecz również na dostępnej dokumentacji technicznej i prawnej opisującej sposób działania agenta AI oraz stosowane środki ochrony danych. Fakt, że agent AI do transkrypcji stanowi funkcjonalność dostarczaną przez zewnętrznego dostawcę, nie eliminuje obowiązków administratora wynikających z RODO. To organizacja decyduje bowiem w jakim zakresie i w jakim celu dana funkcja AI jest wykorzystywana w jej procesach biznesowych, a tym samym ponosi odpowiedzialność za zgodność przetwarzania danych osobowych z przepisami.

W praktyce oznacza to konieczność samodzielnej weryfikacji kluczowych informacji udostępnianych przez dostawcę, a nie jedynie akceptacji marketingowych deklaracji o „zgodności z RODO". Przed uruchomieniem lub udostępnieniem agentów AI użytkownikom organizacja powinna zweryfikować, czy dostawca udostępnia co najmniej:

- **Dokumentację prawną:**
  - Umowę powierzenia przetwarzania danych (DPA) lub jej wzór – często dostępny w sekcji Trust Center, Legal lub Compliance na stronie dostawcy.
  - Politykę prywatności / Data Protection Addendum, opisującą role stron, cele przetwarzania i kategorie danych.
  - Informacje dotyczące transferów danych poza UE, w tym stosowania standardowych klauzul umownych lub innych mechanizmów transferowych.
- **Dokumentację bezpieczeństwa:**
  - Opis stosowanych środków technicznych i organizacyjnych (TOMs), np. szyfrowania danych, kontroli dostępu, logowania zdarzeń.
  - Informacje o certyfikatach lub standardach bezpieczeństwa, takich jak ISO/IEC 27001, SOC 2 lub równoważnych.
  - Dane dotyczące testów bezpieczeństwa, audytów lub ocen odporności systemu na nieautoryzowany dostęp.

Takie podejście pozwala organizacjom korzystać z agentów AI do transkrypcji w sposób świadomy i kontrolowany, bez konieczności projektowania własnych systemów AI. Jednocześnie umożliwia spełnienie obowiązków wynikających z RODO oraz budowanie zaufania uczestników spotkań, pracowników i partnerów biznesowych wobec rozwiązań opartych na sztucznej inteligencji.

Transparentność i obowiązki informacyjne podczas stosowania agentów AI do transkrypcji spotkań

W przypadku korzystania z agentów transkrypcyjnych należy pamiętać, że na organizacji ciążą nie tylko obowiązki informacyjne wynikające z RODO, ale również dodatkowe wymogi związane z rozporządzeniem AI Act. Oba te akty prawne nakładają odrębne obowiązki: RODO skupia się na ochronie danych osobowych i prawach osób, których dane dotyczą, natomiast AI Act wprowadza specyficzne zasady dotyczące transparentności, klasyfikacji ryzyka oraz odpowiedzialności przy wdrażaniu systemów opartych na sztucznej inteligencji. W praktyce oznacza to, że oprócz poinformowania uczestników o przetwarzaniu danych przez agenta AI, konieczne jest także spełnienie wymogów dotyczących transparentności i bezpieczeństwa technologii AI wskazanych w AI Act, zwłaszcza w przypadku stosowania rozwiązań o podwyższonym ryzyku, takich jak rozpoznawanie emocji czy przetwarzanie danych biometrycznych.

Podczas korzystania z agentów transkrypcyjnych należy:

1. **Przed rozpoczęciem rejestracji danych należy poinformować uczestników spotkania, że agent AI bierze udział w wydarzeniu oraz dokonuje przetwarzania danych.**

   Uczestnicy powinni być świadomi interakcji z rozwiązaniami opartymi na sztucznej inteligencji. Warto podkreślić, że obowiązek ten wynika nie tylko z RODO – które nakłada wymóg informowania o przetwarzaniu danych osobowych – ale w tym przypadku szczególnie istotne jest zaznaczenie, iż przetwarzanie odbywa się z wykorzystaniem technologii AI.

   Takie rozwiązania mogą wiązać się z dodatkowymi ryzykami i wymaganiami w zakresie transparentności, określonymi nie tylko przez RODO, ale również przez przepisy AI Act. Dlatego komunikat dla uczestników powinien jednoznacznie wskazywać, że za przetwarzanie danych odpowiada system oparty na sztucznej inteligencji, co pozwala na spełnienie obowiązków informacyjnych oraz budowanie zaufania wobec stosowanej technologii.

2. **W sytuacji, gdy podczas spotkania wykorzystywana jest technologia rozpoznawania emocji lub przetwarzania cech i danych biometrycznych (np. analiza głosu), na organizacji spoczywa szczególny obowiązek transparentnego informowania uczestników o zakresie i celu takich działań.**

   Uczestnicy muszą otrzymać jasną informację, że ich dane biometryczne lub emocjonalne będą analizowane przez system oparty na sztucznej inteligencji, a także jak te dane będą wykorzystywane, przechowywane oraz kto będzie miał do nich dostęp.

   Takie działania są wymagane zarówno przez RODO – które traktuje dane biometryczne jako szczególną kategorię danych osobowych podlegającą podwyższonej ochronie – jak i przez AI Act, który nakłada dodatkowe wymogi w zakresie transparentności i oceny ryzyka dla systemów wykorzystujących tego typu technologie. Informacja powinna obejmować m.in. podstawę prawną przetwarzania, możliwe konsekwencje dla uczestników, a także opis zabezpieczeń chroniących przed nieuprawnionym dostępem do tych danych. Wskazane jest również, aby uczestnicy mieli możliwość zadania pytań dotyczących przetwarzania ich danych biometrycznych oraz wyrażenia zgody (jeśli jest wymagana) na takie działania.

   Przekazanie pełnej i zrozumiałej informacji w tym zakresie nie tylko realizuje obowiązki wynikające z przepisów prawa, ale także buduje zaufanie do stosowanych rozwiązań technologicznych i pozwala uniknąć potencjalnych konsekwencji prawnych w przypadku kontroli lub zgłoszenia naruszenia praw uczestników spotkania.

3. **Zaleca się wdrożenie stałego komunikatu informacyjnego (np. w zaproszeniu, banerze, polityce spotkań): „Spotkanie będzie wspierane przez agenta AI generującego transkrypcję i podsumowanie."**

   Dla zapewnienia zgodności z przepisami RODO oraz AI Act, rekomendowany komunikat powinien zostać rozbudowany o szczegółowe informacje dotyczące zakresu działania agenta AI, celów przetwarzania danych oraz potencjalnych konsekwencji dla uczestników spotkania. Przykładowo, komunikat może przybrać następującą formę:

   „Informujemy, że spotkanie będzie wspierane przez agenta AI, który będzie generował transkrypcję oraz podsumowanie przebiegu wydarzenia. Oznacza to, że wypowiedzi uczestników będą rejestrowane i analizowane przez system oparty na sztucznej inteligencji. Przetwarzanie danych odbywa się w celu dokumentacji spotkania, ułatwienia komunikacji oraz usprawnienia procesu podejmowania decyzji. Dane będą przechowywane zgodnie z polityką bezpieczeństwa organizacji, a dostęp do nich będą mieli wyłącznie upoważnieni pracownicy. W przypadku wykorzystania dodatkowych rozwiązań AI, takich jak rozpoznawanie emocji lub analiza cech biometrycznych (np. głosu, mimiki), uczestnicy zostaną o tym poinformowani w osobnym komunikacie. Przysługuje Państwu prawo do zadawania pytań dotyczących sposobu przetwarzania danych oraz wyrażenia zgody na konkretne działania, jeśli będzie to wymagane."

   Taki komunikat nie tylko spełnia obowiązki informacyjne wynikające z RODO i AI Act, ale również zwiększa przejrzystość procesu. Warto zadbać o to, aby informacja była dostępna na różnych etapach organizacji spotkania – w zaproszeniu, na banerach informacyjnych, w polityce spotkań, a także podczas rozpoczęcia wydarzenia. W przypadku spotkań online, komunikat może być wyświetlany w formie pop-up lub umieszczony na stronie logowania do wydarzenia. Dobrą praktyką jest także umożliwienie uczestnikom łatwego kontaktu z osobą odpowiedzialną za ochronę danych osobowych lub administratorem systemu AI, co pozwoli na szybką reakcję w razie pojawienia się pytań lub wątpliwości.

Ocena poziomu ryzyka narzędzi transkrypcyjnych w świetle AI Act

Zgodnie z przepisami AI Act, nie można automatycznie zakwalifikować narzędzia do transkrypcji jako systemu AI niskiego lub wysokiego ryzyka. Ostateczny poziom ryzyka zależy od konkretnych funkcji, sposobu wykorzystania narzędzia oraz kontekstu jego wdrożenia. Kluczowe jest zatem każdorazowe przeprowadzenie oceny, która uwzględni wszystkie aspekty techniczne i organizacyjne danego rozwiązania. Ocena poziomu ryzyka narzędzia do transkrypcji powinna być elementem każdego wdrożenia systemu AI w organizacji.

Kluczowe jest:

- przeprowadzenie wstępnej analizy funkcjonalności narzędzia,
- dostosowanie poziomu ochrony i obowiązków do rzeczywistego zakresu zastosowania,
- regularne monitorowanie działania systemu oraz aktualizowanie procedur zgodnie z obowiązującymi przepisami prawa,
- zapewnienie pracownikom i uczestnikom spotkań jasnej informacji o funkcjonowaniu oraz potencjalnych konsekwencjach korzystania z narzędzi AI.

Właściwa klasyfikacja poziomu ryzyka oraz wdrożenie odpowiednich środków ochronnych pozwala nie tylko na legalne i bezpieczne korzystanie z narzędzi transkrypcyjnych, ale również na budowanie zaufania do nowoczesnych technologii w środowisku pracy.

Kiedy narzędzie do transkrypcji jest systemem niskiego ryzyka?

Za system AI niskiego ryzyka można uznać narzędzie do transkrypcji, które **służy wyłącznie do automatycznego zapisywania wypowiedzi uczestników spotkania w formie tekstowej**, bez dodatkowej analizy, klasyfikacji czy ingerencji w dane osobowe poza minimalnym zakresem. Przykładem jest prosty rejestrator głosu, który nie wykorzystuje funkcji analizy emocji, nie przetwarza danych biometrycznych (np. cech głosu, mimiki), ani nie służy do oceny pracowniczej.

W przypadku takich narzędzi głównym obowiązkiem organizacji jest zapewnienie zgodności z RODO, a więc m.in. poinformowanie uczestników o przetwarzaniu danych, określenie celu i zakresu przetwarzania oraz zagwarantowanie odpowiednich środków bezpieczeństwa. Wymogi AI Act ograniczają się tutaj do zapewnienia podstawowej transparentności i monitorowania bezpieczeństwa stosowanego rozwiązania.

Kiedy narzędzie do transkrypcji staje się systemem wysokiego ryzyka?

Narzędzie do transkrypcji zostanie zakwalifikowane jako system AI wysokiego ryzyka, jeśli jego funkcje wykraczają poza prosty zapis głosu i obejmują działania takie jak:

- ocena pracownicza lub wspieranie decyzji kadrowych (np. automatyczna ocena efektywności na podstawie analizy wypowiedzi),
- analiza emocji, nastroju lub zachowań uczestników,
- przetwarzanie danych biometrycznych, takich jak cechy głosu, mimika twarzy, odciski palców lub inne dane umożliwiające identyfikację uczestników na podstawie ich cech fizycznych,
- zastosowanie w procesach regulowanych (np. w sektorze finansowym, zdrowotnym, prawnym).

W takich przypadkach pojawiają się istotne dodatkowe obowiązki prawne:

- przeprowadzenie szczegółowej oceny ryzyka oraz wdrożenie mechanizmów zarządzania ryzykiem,
- zapewnienie wysokiego poziomu transparentności działania narzędzia (m.in. jasna informacja o analizowanych danych i ich przeznaczeniu),
- wdrożenie środków technicznych i organizacyjnych minimalizujących ryzyko naruszenia praw uczestników,
- prowadzenie dokumentacji dotyczącej działania systemu i podejmowanych działań naprawczych,
- możliwość audytu i zgłaszania systemu do właściwych organów nadzoru.

Legalność korzystania i warunki wdrożenia

Należy pamiętać, że zakwalifikowanie narzędzia transkrypcyjnego jako systemu wysokiego ryzyka nie oznacza automatycznego zakazu jego stosowania. Legalność korzystania z takiego narzędzia jest możliwa pod warunkiem spełnienia wszystkich wymogów przewidzianych przez AI Act oraz RODO. Obejmuje to m.in. przygotowanie odpowiedniej dokumentacji, wdrożenie procedur bezpieczeństwa, regularne audyty oraz możliwość reagowania na incydenty związane z naruszeniem ochrony danych.

W przypadku narzędzi niskiego ryzyka obowiązki są ograniczone głównie do zapewnienia transparentności i bezpieczeństwa podstawowego, natomiast dla systemów wysokiego ryzyka konieczne jest spełnienie kompleksowych wymagań dotyczących zarządzania ryzykiem, ochrony praw osób oraz raportowania działań do organów nadzorczych.

„Shadow AI”

Shadow AI odnosi się do sytuacji, w której pracownicy korzystają z narzędzi sztucznej inteligencji bez zgody, wiedzy i nadzoru ze strony organizacji. Według badań przeprowadzonych przez PWC w 2025 roku, nawet 32% zatrudnionych wykorzystuje rozwiązania AI w sposób niejawny, a aż 70% spośród nich robi to bez właściwej autoryzacji.

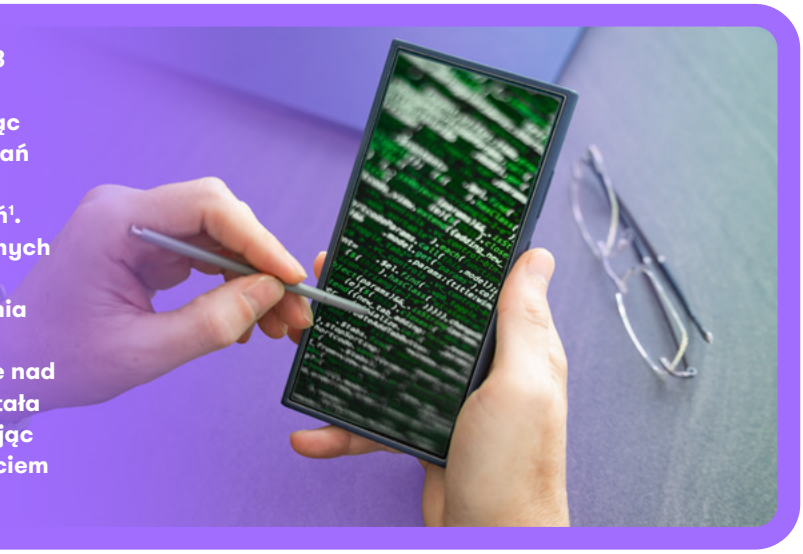
Takie praktyki generują istotne ryzyka.

Zewnętrzne narzędzia AI mogą przesyłać dane poza obszar Unii Europejskiej bez wiedzy firmy, co niesie ryzyko naruszenia zasad ochrony danych osobowych oraz wymogów RODO – chociaż sam transfer nie jest automatycznie nielegalny, to niewłaściwe zabezpieczenie i brak kontroli nad przepływem danych mogą prowadzić do poważnych konsekwencji prawnych, w tym potencjalnych kar ze strony organów nadzorczych.

Obowiązek odpowiedniego uświadamiania pracowników w zakresie zagrożeń i procedur dotyczących wykorzystania narzędzi AI (AI literacy) jest powszechnym wymogiem prawnym dla każdej firmy korzystającej ze sztucznej inteligencji. Choć brak spełnienia tego wymogu nie zawsze wiąże się z bezpośrednimi sankcjami, może prowadzić do niepożądanych skutków, takich jak błędne decyzje pracowników, wyciek danych czy nawet utrata ochrony ubezpieczeniowej w przypadku incydentu cybernetycznego. W razie incydentu firma może zostać pociągnięta do odpowiedzialności za niedopełnienie obowiązków informacyjnych oraz brak odpowiednich szkoleń.

Naruszenie tajemnicy zawodowej lub poufności może wystąpić, gdy pracownicy wykorzystują narzędzia AI bez odpowiedniej kontroli i autoryzacji, na przykład kopiując lub przesyłając poufne dane do zewnętrznych systemów. Takie działania prowadzą do ryzyka trwałego wycieku informacji chronionych, których ujawnienie może skutkować poważnymi konsekwencjami dla firmy, zarówno prawno-finansowymi, jak i reputacyjnymi. W przypadku incydentu organizacja może zostać pociągnięta do odpowiedzialności za naruszenie tajemnicy zawodowej, zwłaszcza jeśli nie wdrożyła odpowiednich procedur zabezpieczających oraz nie przeprowadziła szkoleń dla pracowników w zakresie ochrony poufności danych. Dlatego kluczowe jest, aby każda firma korzystająca z AI regularnie monitorowała przepływ informacji i dbała o świadomość zespołu w zakresie zagrożeń związanych z nieautoryzowanym użyciem technologii.

Przykładem działania shadow AI jest incydent z 2023 roku, podczas którego pracownicy firmy Samsung nieświadomie udostępnili poufne informacje, kopiując fragmenty kodu źródłowego oraz transkrypcje spotkań do publicznej wersji ChatGPT w celu usprawnienia procesów debugowania oraz tworzenia podsumowań[1]. Ponieważ dane te były przechowywane na zewnętrznych serwerach, doszło do trwałego wycieku firmowej własności intelektualnej. Po ujawnieniu tego zdarzenia firma Samsung natychmiast wprowadziła zakaz korzystania z generatywnej AI oraz rozpoczęła prace nad własnym, bezpiecznym rozwiązaniem. Sytuacja ta stała się globalnym sygnałem ostrzegawczym, unaoczniając skalę zagrożeń związanych z niekontrolowanym użyciem sztucznej inteligencji przez pracowników.



Halucynacje AI — ryzyko błędnych ustaleń

Systemy AI wykorzystywane do transkrypcji spotkań mogą generować treści, które brzmią wiarygodnie, ale nie zawsze wiernie odzwierciedlają faktyczne ustalenia. W praktyce prowadzi to do powstawania tzw. „fałszywych faktów organizacyjnych”, czyli błędnych podsumowań, decyzji lub zadań, które zaczynają funkcjonować w firmie jako oficjalne ustalenia. Takie nieścisłości mogą skutkować podejmowaniem decyzji w oparciu o nieprawdziwe informacje, eskalacją sporów odpowiedzialności lub realizacją działań, które nigdy nie zostały zatwierdzone. Dodatkowym zagrożeniem jest nadmierne zaufanie do technologii — wygenerowane podsumowania bywają traktowane jako bardziej „obiektywne” niż notatki uczestników spotkania. Dlatego treści tworzone przez agentów AI powinny mieć charakter wyłącznie pomocniczy, a ich wykorzystanie wymaga zachowania nadzoru człowieka i jasnych zasad weryfikacji przed dalszym użyciem w organizacji.

1. Źródło: Bloomberg, “Samsung Bans ChatGPT Use After Staff Leak Sensitive Data”, 2023

Jak wdrożyć politykę korzystania z agentów AI w Twojej firmie?

Inwentaryzacja używanych narzędzi.

Przeprowadź przegląd wszystkich narzędzi AI wykorzystywanych w organizacji, zarówno oficjalnych, jak i tych używanych nieformalnie przez pracowników. Pozwoli to na identyfikację potencjalnych zagrożeń oraz określenie obszarów wymagających szczególnej kontroli.

Weryfikacja dostawcy.

Zweryfikuj wiarygodność dostawców narzędzi AI oraz zadbaj o podpisanie odpowiednich umów powierzenia przetwarzania danych.

Polityka AI.

Opracuj jasne zasady korzystania z AI, określając, jakie działania są dozwolone, a jakie zabronione, oraz w jakich przypadkach wymagana jest dodatkowa autoryzacja. Polityka powinna być łatwo dostępna i zrozumiała dla wszystkich pracowników.

Edukacja pracowników.

Regularnie szkól zespół z zasad bezpiecznego korzystania z AI oraz potencjalnych zagrożeń związanych z shadow AI. Świadomi pracownicy to klucz do skutecznego wdrożenia polityki i ograniczenia ryzyka błędnych decyzji opartych na halucynacjach AI.

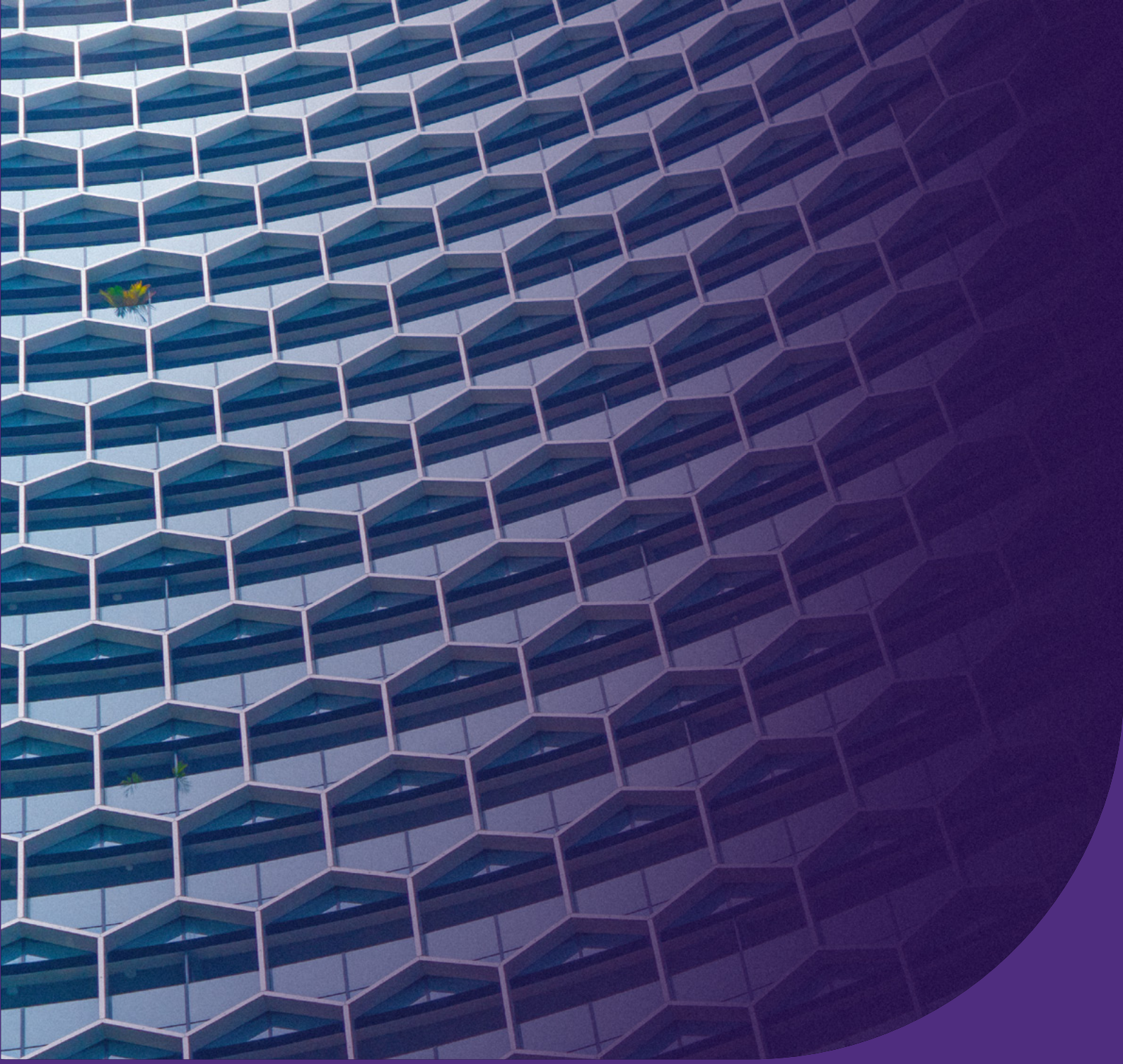
Kontakt

Wojciech Biernacki
Senior Associate,
Doradztwo Grant Thornton
M: +48 601 722 023
E: wojciech.biernacki@pl.gt.com

Emilia Martynowicz-Mamajek
Associate,
Doradztwo Grant Thornton
M: +48 667 778 891
E: emilia.martynowicz-mamajek@pl.gt.com

Paulina Klisowska
Junior Associate,
Doradztwo Grant Thornton
M: +48 669 007 862
E: paulina.klisowska@pl.gt.com

Krzysztof Jeromin
Junior Associate,
Doradztwo Grant Thornton
M: +48 785 640 434
E: krzysztof.jeromin@pl.gt.com



Na co dzień dzielimy się wiedzą na:

www.GrantThornton.pl

Kilka słów o nas

Grant Thornton to jedna z wiodących organizacji audytorsko-doradczych na świecie. W Polsce działamy od 1993 roku. Zatrudniamy zespół ponad 1200 osób, posiadamy biura w 7 kluczowych aglomeracjach, a rocznie obsługujemy ponad 2,5 tys. Klientów. Na świecie jesteśmy obecni w 156 krajach i zatrudniamy ponad 76 tys. pracowników, a historia firmy sięga 1904 roku.