Dział Transformacji
Cyfrowej i Procesów

POLITYKA KORZYSTANIA Z NARZĘDZI SZTUCZNEJ INTELIGENCJI

OBOWIĄZUJE OD:
23 października 2026

w ENERGOPROJEKT-KATOWICE SA z siedzibą w Katowicach

§1. Cel i zakres

1. Polityka określa zasady korzystania z Narzędzi AI przez pracowników, współpracowników, osoby świadczące usługi na rzecz Firmy oraz podmioty zewnętrzne, w tym dostawców i podmioty przetwarzające, w zakresie, w jakim korzystają z Narzędzi AI do Celów służbowych albo uzyskują dostęp do informacji, danych lub systemów EPK w związku z takim korzystaniem.
2. Celem Polityki jest bezpieczne i zgodne z prawem wykorzystanie Narzędzi AI w działalności Firmy, w tym realizacja obowiązków wynikających z AI Act, w szczególności w zakresie kompetencji w obszarze AI (art. 4) oraz przejrzystości (art. 50).
3. Polityka obejmuje każde Narzędzie AI używane do Celów służbowych – także narzędzia bezpłatne, przeglądarkowe oraz funkcje AI wbudowane w inne oprogramowanie.
4. Polityka dotyczy korzystania z Narzędzi AI w roli podmiotu stosującego w rozumieniu AI Act. W przypadku gdy Firma tworzy własne systemy AI lub wprowadza je do obrotu (rola dostawcy), stosuje się odrębne procedury.
5. Objęcie danego rozwiązania Polityką nie przesądza o jego kwalifikacji jako systemu AI w rozumieniu AI Act. Kwalifikacji na potrzeby AI Act dokonuje się odrębnie, z uwzględnieniem definicji ustawowej i konkretnego sposobu zastosowania.
6. Jeżeli Polityka Bezpieczeństwa Informatycznego, przepisy prawa, umowa z klientem, umowa o zachowaniu poufności (NDA), wymagania sektorowe, instrukcja projektu albo inne wiążące Firmę wymagania przewidują zasady bardziej restrykcyjne niż niniejsza Polityka, stosuje się zasady bardziej restrykcyjne.
7. Politykę stosuje się niezależnie od miejsca korzystania z Narzędzia AI, rodzaju urządzenia, sposobu połączenia z siecią oraz tego, czy używane jest Konto firmowe czy Konto prywatne. Użycie Konta prywatnego, prywatnego urządzenia lub bezpłatnej wersji narzędzia nie wyłącza stosowania Polityki, jeżeli korzystanie następuje do celów służbowych. Objęcie korzystania z prywatnego urządzenia lub Konta prywatnego zakresem Polityki nie oznacza zgody Firmy na ich używanie do celów służbowych.

Zgoda na korzystanie z Konta prywatnego może wynikać wyłącznie z wyraźnego wpisu w Rejestrze narzędzi i zastosowań AI.

8. Polityka nie zastępuje zasad określonych w Polityce Bezpieczeństwa Informatycznego ani obowiązujących w Firmie zasad ochrony danych osobowych, kontroli dostępu, zarządzania jakością, zatwierdzania dokumentów, zarządzania zmianą, korzystania z urządzeń i sieci oraz wymagań wynikających z konkretnych umów, i projektów.

9. Niniejsza Polityka stanowi regulację szczegółową wobec obowiązującej w Firmie Polityki Bezpieczeństwa Informatycznego. W zakresie bezpieczeństwa systemów i danych, kont, uprawnień, urządzeń, sieci, oprogramowania, logowania zdarzeń, retencji, kopii zapasowych, monitorowania oraz obsługi Incydentów stosuje się również Politykę Bezpieczeństwa Informatycznego. W razie sprzeczności pierwszeństwo ma Polityka Bezpieczeństwa Informatycznego, chyba że niniejsza Polityka ustanawia ograniczenie dalej idące.

§2. Definicje

1. **Polityka** – niniejsza Polityka korzystania z Narzędzi sztucznej inteligencji.

2. **Firma lub EPK** – BSPiR „ENERGOPROJEKT-KATOWICE" SA z siedzibą w Katowicach.

3. **System AI** – system sztucznej inteligencji w rozumieniu art. 3 pkt 1 AI Act, tj. system maszynowy, „który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który na potrzeby wyraźnych lub dorozumianych celów wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne".

4. **Narzędzie AI** – System AI, a także każda inna aplikacja, funkcja lub usługa, która jest oparta na generatywnej sztucznej inteligencji albo która wykorzystuje bezpośrednio lub pośrednio System AI, jego elementy lub inne komponenty oparte na generatywnej sztucznej inteligencji, ujęta w rejestrze narzędzi i zastosowań AI, w szczególności generująca tekst, obraz, dźwięk, wideo lub kod albo wspierająca analizę danych i podejmowanie decyzji (np. asystenci konwersacyjni typu czat, generatory treści, narzędzia do transkrypcji, asystenci programowania, a także funkcje AI wbudowane w inne oprogramowanie) – niezależnie od tego, czy samo stanowi System AI w rozumieniu AI Act.

5. **Dane chronione** – wszystkie dane podlegające ochronie w rozumieniu Polityki Bezpieczeństwa Informatycznego, w szczególności dane osobowe, dane projektowe i techniczne, informacje dotyczące realizowanych kontraktów, informacje finansowe nieujawnione publicznie, dane dostępowe i informacje o konfiguracji IT, informacje stanowiące tajemnicę przedsiębiorstwa lub przewagę konkurencyjną Firmy albo jej kontrahentów, informacje niejawne, informacje objęte NDA oraz inne informacje wewnętrzne lub oznaczone jako poufne. W przypadku wątpliwości dane traktuje się jako Dane chronione.

6. **Rejestr narzędzi i zastosowań AI** – wykaz Narzędzi AI, ich zatwierdzonych zastosowań, kategorii danych, grup Użytkowników i warunków korzystania, stanowiący Załącznik nr 1.

7. **Polityka Bezpieczeństwa Informatycznego** – dokument pn. „Polityka Bezpieczeństwa Informatycznego Energoprojekt-Katowice S.A. (EPK)", określający zasady bezpieczeństwa informacji i systemów teleinformatycznych w Firmie; przez Politykę Bezpieczeństwa Informatycznego rozumie się każdorazowo jej aktualnie obowiązujące wydanie. Dokument ten jest nadrzędny wobec niniejszej Polityki w zakresie bezpieczeństwa informacji i systemów teleinformatycznych.

8. **Cele służbowe** – wykorzystanie Narzędzia AI w związku z wykonywaniem pracy lub świadczeniem usług na rzecz Firmy, w szczególności do wytwarzania, przetwarzania lub przekazywania treści, kodu, danych lub dokumentów związanych z działalnością Firmy albo jej klientów, jak również do wspierania analizy lub podejmowania decyzji w tej działalności niezależnie od wykorzystywanego urządzenia, miejsca i pory korzystania oraz od tego, czy korzystanie jest odpłatne. Za korzystanie do Celów służbowych uważa się w każdym przypadku takie, w którym do Narzędzia AI wprowadza się informacje dotyczące Firmy, jej

działalności, jej pracowników, współpracowników, klientów, potencjalnych klientów, podwykonawców. Korzystania wyłącznie w celach prywatnych niezwiązanego z działalnością Firmy i nieobejmującego informacji, o których mowa w zdaniu poprzedzającym nie uważa się za korzystanie do Celów służbowych.

9. **AI Act** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany niektórych aktów prawodawczych Unii (akt w sprawie sztucznej inteligencji) (Dz. Urz. UE L z 12.07.2024).
10. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
11. **Użytkownik** – osoba objęta Polityką, która korzysta z Narzędzia AI do Celów służbowych albo wykorzystuje wynik pracy Narzędzia AI w związku z działalnością Firmy.
12. **Agent AI** – Narzędzie AI skonfigurowane do wykonywania określonych zadań albo sekwencji działań na podstawie poleceń Użytkownika, przy wykorzystaniu wskazanych danych, źródeł, funkcji, wtyczek, konektorów lub integracji.
13. **Agent osobisty** – Agent AI utworzony przez Użytkownika na własne potrzeby służbowe, niewspółdzielony z innymi Użytkownikami i niewykonujący działań w imieniu Firmy poza zakresem pracy tego Użytkownika.
14. **Agent firmowy** – Agent AI zatwierdzony do użycia przez więcej niż jednego Użytkownika, zespół, projekt, komórkę organizacyjną, klienta lub proces biznesowy.
15. **Publiczne Narzędzie AI** – ogólnodostępne Narzędzie AI, w szczególności udostępniane bezpłatnie albo za pośrednictwem konta prywatnego, które nie jest objęte firmowym systemem zarządzania kontami, licencjami, konfiguracją i bezpieczeństwem. Publiczne Narzędzie AI może być używane do celów służbowych wyłącznie wtedy, gdy konkretne narzędzie, zastosowanie, sposób dostępu, grupa Użytkowników i kategorie danych zostały wyraźnie dopuszczone w Rejestrze narzędzi i zastosowań AI.
16. **Dane publicznie dostępne** – dane zgodnie z prawem udostępnione nieograniczonemu kręgowi odbiorców, których wykorzystanie nie narusza praw osób trzecich, warunków licencji, umów, obowiązków poufności ani interesu Firmy lub jej kontrahentów.
17. **Incydent** – zdarzenie związane z korzystaniem z Narzędzia AI, które spowodowało lub mogło spowodować naruszenie prawa, Polityki, bezpieczeństwa informacji, ochrony danych osobowych, obowiązków umownych, praw osób trzecich, jakości, ciągłości działania albo interesu Firmy lub jej kontrahentów.
18. **Prompt injection** – technika polegająca na umieszczeniu w danych wejściowych, dokumentach, wiadomościach, stronach internetowych lub innych treściach instrukcji mających skłonić Narzędzie AI do pominięcia obowiązujących zasad, ujawnienia danych, zmiany sposobu działania lub wykonania niepożądanej czynności.
19. **Opiekun Polityki** – Dział Transformacji Cyfrowej i Procesów (TCP).
20. **Konto firmowe** – konto w Narzędziu AI utworzone lub udostępnione przez Firmę do celów służbowych, powiązane z firmową tożsamością Użytkownika i objęte zasadami Firmy dotyczącymi dostępu, bezpieczeństwa, konfiguracji, licencjonowania oraz nadzoru.
21. **Konto prywatne** – konto w Narzędziu AI założone przez Użytkownika poza systemem zarządzania Firmy, w szczególności z wykorzystaniem prywatnego adresu e-mail lub prywatnych danych logowania. Konto pozostaje prywatne niezależnie od tego, czy Użytkownik korzysta z niego na urządzeniu firmowym lub w sieci Firmy.

§3. Narzędzia dopuszczone i zakazane

1. Do Celów służbowych wolno korzystać wyłącznie z Narzędzi AI oraz zastosowań ujętych w Rejestrze narzędzi i zastosowań AI, zgodnie z określonymi w nim kategoriami danych, grupami Użytkowników i warunkami korzystania.
2. Wniosek o dopisanie nowego Narzędzia AI lub nowego zastosowania do Rejestru narzędzi i zastosowań AI składa się do Opiekuna Polityki. Do czasu zatwierdzenia wpisu korzystanie z narzędzia lub zastosowania do Celów służbowych jest niedozwolone.
3. Zakazane jest korzystanie z Narzędzi AI:
   a. w sposób naruszający prawo, w tym w ramach praktyk zakazanych w rozumieniu art. 5 AI Act, w szczególności w celu stosowania technik podprogowych, celowych technik manipulacyjnych lub wprowadzających w błąd, wykorzystywania słabości osób, scoringu społecznego albo rozpoznawania emocji w miejscu pracy;
   b. do samodzielnego podejmowania lub istotnego wspierania decyzji dotyczących zatrudnienia, rekrutacji, awansu, wynagrodzenia, oceny pracy, rozwiązania współpracy albo innych decyzji wywołujących istotne skutki wobec osób, chyba że dane zastosowanie zostało objęte odrębną procedurą zatwierdzoną przez Zarząd;
   c. do Celów służbowych za pośrednictwem Kont prywatnych, chyba że Rejestr narzędzi i zastosowań AI wyraźnie dopuszcza konkretne Narzędzie AI, zastosowanie, sposób dostępu, grupę Użytkowników i kategorie danych. Dopuszczenie korzystania z Konta prywatnego może obejmować wyłącznie dane publicznie dostępne i nie może obejmować danych chronionych ani informacji dotyczących niepublicznych spraw Firmy, jej klientów, kontrahentów, pracowników lub projektów;
   d. z Publicznych Narzędzi AI, jeżeli dane Narzędzie AI, zastosowanie lub sposób dostępu nie zostały ujęte w Rejestrze narzędzi i zastosowań AI albo korzystanie wykracza poza zakres określony w odpowiednim wpisie;
   e. przy użyciu prywatnego urządzenia lub z wykorzystaniem dostępu do sieci EPK z naruszeniem zasad dotyczących urządzeń, sieci, VPN i dostępu określonych w Polityce Bezpieczeństwa Informatycznego.
4. Przed dopisaniem Narzędzia AI do Rejestru Opiekun Polityki ocenia odrębnie dla każdego zastosowania, czy stanowi ono praktykę zakazaną w rozumieniu art. 5 AI Act, system wysokiego ryzyka w rozumieniu art. 6 AI Act, zastosowanie objęte obowiązkami przejrzystości, w szczególności określonymi w art. 50 AI Act, czy pozostałe zastosowanie. Wynik oceny wraz z zatwierdzonym celem użycia odnotowuje się w Rejestrze. Praktyki zakazane nie mogą zostać dopuszczone. Systemy wysokiego ryzyka wymagają odrębnych procedur i nie mogą zostać dopuszczone wyłącznie na podstawie Polityki.
5. Wyliczenia zastosowań zakazanych w ust. 3 mają charakter przykładowy. Brak danego zastosowania na liście nie oznacza jego dopuszczalności; w przypadku wątpliwości, w szczególności co do zastosowań dotyczących osób, wymagane jest uzyskanie dopuszczenia Opiekuna Polityki.
6. Fakt udostępnienia Narzędzia AI w środowisku Firmy nie oznacza, że do Narzędzia AI wolno wprowadzać każdą informację dostępną Użytkownikowi. Użytkownik każdorazowo ocenia dopuszczalność danych, cel ich wykorzystania i ograniczenia wynikające z prawa, umów, NDA, wymagań klienta oraz instrukcji projektu.
7. Opiekun Polityki może dopuścić w Rejestrze narzędzi i zastosowań AI korzystanie z określonego Publicznego Narzędzia AI wyłącznie na Danych publicznie dostępnych, przy użyciu wskazanego Konta firmowego, Konta prywatnego, licencji, przestrzeni roboczej albo innej konfiguracji określonej w Rejestrze. Wpis do Rejestru określa co najmniej zatwierdzony cel użycia, sposób dostępu, grupę Użytkowników, dopuszczone kategorie danych oraz warunki i ograniczenia korzystania. Takie dopuszczenie nie obejmuje danych chronionych ani informacji dotyczących niepublicznych spraw Firmy, jej klientów, kontrahentów, pracowników lub projektów.

8. Udostępnienie Agenta AI innej osobie, zespołowi, projektowi, komórce organizacyjnej, klientowi lub procesowi biznesowemu wymaga uprzedniego zatwierdzenia go jako Agenta firmowego i ujęcia w Rejestrze narzędzi i zastosowań AI zgodnie z procedurą określoną w punkcie 10 jn.

9. Agent AI, wtyczka, konektor, rozszerzenie, API ani automatyzacja nie mogą rozszerzać dostępu Użytkowników do danych ponad ich faktyczne uprawnienia biznesowe ani wykonywać działań wywołujących skutki prawne, finansowe, kadrowe, administracyjne, projektowe lub techniczne.

10. Narzędzie AI lub jego zastosowanie może zostać ujęte w Rejestrze narzędzi i zastosowań AI po przeprowadzeniu oceny koordynowanej przez Opiekuna Polityki oraz po uzyskaniu akceptacji Kierownika Działu IT albo osoby przez niego upoważnionej. Ocena Działu IT obejmuje w szczególności bezpieczeństwo, architekturę, licencjonowanie, ewidencję oprogramowania, konta, uprawnienia, integracje, logowanie zdarzeń, retencję, kopie zapasowe, ciągłość działania i warunki techniczne.

11. Jeżeli planowane zastosowanie obejmuje przetwarzanie danych osobowych, Opiekun Polityki przeprowadza konsultację z Inspektorem Ochrony Danych. Jeżeli zastosowanie obejmuje dokumentację klientów, zobowiązania umowne, własność intelektualną albo zastosowanie wymagające podwyższonej oceny ryzyka, w ocenie uczestniczy również obsługa prawna oraz właściwy właściciel biznesowy zastosowania.

12. Wpis do Rejestru uzyskuje status „Zatwierdzone” dopiero po zatwierdzeniu celu i warunków biznesowych przez Opiekuna Polityki oraz po uzyskaniu pozytywnej akceptacji technicznej Działu IT. Negatywna ocena Działu IT uniemożliwia zatwierdzenie Narzędzia AI lub jego zastosowania.

§4. Zasady bezpieczeństwa danych

1. Z zastrzeżeniem ust. 2, do Narzędzi AI nie wolno wprowadzać danych chronionych, w szczególności danych osobowych klientów i pracowników, treści umów i dokumentów objętych poufnością, kodu źródłowego objętego zobowiązaniami wobec kontrahentów oraz danych finansowych nieujawnionych publicznie.

2. Dane chronione mogą być przetwarzane wyłącznie w Narzędziach AI, dla których Rejestr narzędzi i zastosowań AI wyraźnie dopuszcza daną kategorię danych, grupę Użytkowników oraz zastosowanie. Dopuszczenie może mieć charakter ogólny dla wskazanego zastosowania i nie wymaga uzyskiwania przez Użytkownika odrębnej zgody przed każdą interakcją.

3. Do Narzędzia AI przekazuje się wyłącznie dane niezbędne do realizacji zatwierdzonego celu. Jeżeli cel może zostać osiągnięty bez danych identyfikujących osoby lub bez pełnego zakresu informacji, dane należy odpowiednio zanonimizować, ograniczyć albo spseudonimizować. Pseudonimizacja nie powoduje utraty przez dane statusu danych osobowych.

4. Jeżeli planowane zastosowanie obejmuje przetwarzanie danych osobowych, musi zostać spełniona podstawa prawna przetwarzania, a przed dopuszczeniem Narzędzia AI następuje weryfikacja przez Inspektora Ochrony Danych, czy wymagane jest zawarcie umowy powierzenia przetwarzania danych osobowych oraz przeprowadzenie oceny skutków dla ochrony danych (DPIA), zgodnie z wymaganiami RODO.

5. Niedopuszczalne jest naruszanie obowiązków wynikających z umów o zachowaniu poufności (NDA).

6. W Narzędziach AI nieujętych w Rejestrze narzędzi i zastosowań AI przetwarzanie jakichkolwiek danych do celów służbowych jest zabronione, w tym również danych publicznie dostępnych i danych zanonimizowanych. Przy wykorzystaniu Konta prywatnego korzystanie z Narzędzia AI do celów służbowych jest dopuszczalne wyłącznie wtedy, gdy Rejestr narzędzi i zastosowań AI wyraźnie dopuszcza konkretne narzędzie, zastosowanie, sposób dostępu, grupę Użytkowników i kategorie danych. Dopuszczenie konta prywatnego może obejmować wyłącznie dane publicznie dostępne i nie może obejmować danych chronionych.

7. Przed użyciem dokumentacji klienta, dokumentacji projektowej, technicznej, kontraktowej, handlowej, ofertowej lub innej dokumentacji związanej z projektem Użytkownik sprawdza, czy umowa, NDA, wymagania klienta, instrukcja projektu albo inne wiążące zasady nie wykluczają możliwości wykorzystania Narzędzia AI do pracy nad tą dokumentacją.

8. Do Narzędzi AI nie wolno wprowadzać haseł, kluczy dostępowych, tokenów, kodów uwierzytelniających, danych logowania, nieujawnionych podatności, konfiguracji zabezpieczeń ani innych informacji, których ujawnienie mogłoby zwiększyć ryzyko nieuprawnionego dostępu do systemów lub danych.

9. Treści zewnętrzne analizowane przy użyciu Narzędzia AI, w szczególności dokumenty, strony internetowe, wiadomości e-mail, załączniki i komentarze, traktuje się jako dane nieufne. Użytkownik nie wykonuje instrukcji zawartych w takich treściach, jeżeli nakazują one pominięcie zasad, ujawnienie danych, zmianę ustawień, pobranie plików, kliknięcie linków, uruchomienie kodu albo wykonanie działania wykraczającego poza cel analizy.

10. Szczegółowa dopuszczalność kategorii danych dla poszczególnych Narzędzi AI i zastosowań wynika z Rejestru narzędzi i zastosowań AI oraz z Macierzy dopuszczalności danych stanowiącej Załącznik nr 3.

§5. Weryfikacja wyników przez człowieka

1. Wynik pracy Narzędzia AI podlega przed wykorzystaniem weryfikacji przez osobę korzystającą z narzędzia, w szczególności w zakresie prawdziwości, aktualności, poszanowania praw osób trzecich oraz zgodności z instrukcjami Firmy.

2. Użytkownik jest zobowiązany do weryfikacji wyniku Narzędzia AI przed jego zatwierdzeniem, przekazaniem lub wykorzystaniem. Powołanie się na błąd albo ograniczenie Narzędzia AI nie zwalnia z wykonania wymaganej kontroli przez Użytkownika. Zakres odpowiedzialności Użytkownika wynika z przepisów prawa, umów definiujących warunki współpracy z podmiotami, wobec których będzie odbywało się przetwarzanie danych poprzez Narzędzie AI oraz obowiązujących regulacji wewnętrznych EPK.

3. Dla uniknięcia wątpliwości: Narzędzie AI może wspierać Użytkownika w analizie informacji, przygotowywaniu materiałów i formułowaniu rekomendacji, lecz nie podejmuje decyzji o poprawności i wykorzystaniu wygenerowanych treści za Użytkownika ani za organy Firmy. Ostateczna decyzja, jej uzasadnienie i odpowiedzialność za jej podjęcie zgodne z niniejszą Polityką należą do Użytkownika.

4. Weryfikacja przez Użytkownika treści wygenerowanych przez AI obejmuje w szczególności sprawdzenie pod kątem poprawności faktów, liczb, obliczeń, źródeł, cytatów, norm, przepisów, wymagań kontraktowych, dat, nazw własnych, kompletności i zgodności z dokumentami źródłowymi.

5. Zakazane jest wprowadzanie do Narzędzi AI cudzych utworów bez podstawy prawnej oraz generowanie treści naśladujących twórczość konkretnych osób w sposób mogący naruszać ich prawa. Nie przyjmuje się, że wynik Narzędzia AI jest wolny od praw osób trzecich; przed wykorzystaniem wyniku Użytkownik weryfikuje ryzyko naruszenia tych praw, a w przypadku kodu także zgodność z licencjami open source.

6. Kod, skrypty, makra, zapytania, konfiguracje, polecenia, integracje i automatyzacje wygenerowane przez AI mogą zostać użyte w środowisku Firmy dopiero po ich przeglądzie i przetestowaniu zgodnie z obowiązującymi zasadami bezpieczeństwa i zarządzania zmianą. Przegląd i testy nie stanowią zgody na instalację, wdrożenie ani uruchomienie w środowisku produkcyjnym. Stosuje się zasady kontroli oprogramowania, nadawania uprawnień i zarządzania zmianą określone w Polityce Bezpieczeństwa Informatycznego oraz właściwych procedurach IT.

7. W przypadku materiałów, dla których znaczenie ma możliwość wykazania autorstwa, oryginalności lub przebiegu prac, Użytkownik zachowuje dokumentację swojego istotnego wkładu twórczego w zakresie wymaganym przez procedurę jakościową, umowę, klienta albo instrukcję projektu.

8. Weryfikacja wyniku Narzędzia AI ani oznaczenie udziału AI nie zastępują zatwierdzenia dokumentu, materiału lub komunikatu zgodnie z obowiązującymi w Firmie procedurami.

§6. Oznaczanie treści tworzonych z AI

1. Treści wygenerowane lub istotnie zmienione przez Narzędzia AI, przeznaczone do udostępnienia poza Firmę, oznacza się w sposób widoczny dla odbiorcy, jeżeli zachodzi co najmniej jedna z następujących okoliczności:

   a. obowiązek oznaczenia wynika z prawa, w tym z art. 50 AI Act;

   b. charakter treści może wprowadzać odbiorcę w błąd co do jej pochodzenia lub autentyczności;

   c. obowiązek oznaczenia dla danego zastosowania określił Opiekun Polityki.

   Czysto pomocnicze użycie Narzędzia AI, takie jak korekta językowa, nie wymaga oznaczenia.

2. Przed uruchomieniem Systemu AI przeznaczonego do bezpośredniej interakcji z osobami fizycznymi Firma zapewnia, że odbiorca jest w jasny i widoczny sposób informowany o interakcji z Systemem AI, chyba że jest to oczywiste w danych okolicznościach. Zakres odpowiedzialności Firmy ustala się z uwzględnieniem jej roli w rozumieniu AI Act.

3. W przypadku generowania lub modyfikowania przy pomocy Narzędzia AI obrazów, nagrań audio lub wideo przedstawiających istniejące osoby, miejsca lub zdarzenia w sposób mogący wprowadzać w błąd (deepfake) Użytkownik ujawnia, że treść została sztucznie wygenerowana lub zmanipulowana.

4. Niezależnie od obowiązków określonych w niniejszym paragrafie treści przygotowane z istotnym udziałem Narzędzia AI oznacza się również wtedy, gdy wymaga tego umowa, klient, procedura jakościowa, instrukcja projektu albo decyzja Opiekuna Polityki.

5. Obowiązek oznaczenia treści nie zastępuje obowiązku uzyskania wymaganej zgody na publikację, przekazanie materiału poza Firmę albo wypowiadanie się w imieniu Firmy.

§7. Incydenty

1. Incydent związany z korzystaniem z Narzędzia AI zgłasza się niezwłocznie do Działu IT za pomocą zgłoszenia serwisowego w systemie Statlook oraz jednocześnie informuje się Opiekuna Polityki. Jeżeli Incydent dotyczy danych osobowych, postępuje się również zgodnie z obowiązującą procedurą naruszeń ochrony danych osobowych.

2. Użytkownik nie usuwa samodzielnie skutków Incydentu, historii interakcji, plików, logów ani innych dowodów, chyba że otrzyma takie polecenie od osoby prowadzącej obsługę Incydentu.

3. Zgłoszenie Incydentu w dobrej wierze nie stanowi samodzielnej podstawy odpowiedzialności zgłaszającego.

4. W przypadku gdy Incydent dotyczy systemu wysokiego ryzyka lub może stanowić poważny Incydent w rozumieniu AI Act, Opiekun Polityki ocenia obowiązki zgłoszeniowe Firmy wobec dostawcy systemu oraz właściwych organów nadzoru; w przypadku Incydentu dotyczącego danych osobowych informuje Inspektora Ochrony Danych.

5. Do czasu decyzji Opiekuna Polityki dotyczącej Narzędzia, którego dotyczy incydent wstrzymuje się korzystanie z Narzędzia AI w zakresie objętym Incydentem; zabezpiecza się historię komunikacji z narzędziem i inne dowody oraz nie usuwa się śladów Incydentu.

6. Logi bezpieczeństwa oraz dowody dotyczące Incydentów AI przechowuje się zgodnie z Polityką Bezpieczeństwa Informatycznego i obowiązującymi procedurami retencji, nie krócej niż przez 12 miesięcy, chyba że przepisy prawa, umowa, procedura incydentowa albo wymagania klienta przewidują okres dłuższy. Logi i dowody zabezpiecza się przed nieuprawnioną zmianą i udostępnia wyłącznie osobom upoważnionym.

§8. Opiekun Polityki

1. Opiekunem Polityki jest Dział Transformacji Cyfrowej i Procesów.
2. Opiekun Polityki jest właścicielem Polityki, prowadzi Rejestr narzędzi i zastosowań AI, koordynuje ocenę i zatwierdzanie Narzędzi AI oraz ich zastosowań biznesowych, organizuje szkolenia, monitoruje stosowanie Polityki oraz dokonuje jej okresowego przeglądu i aktualizacji.
3. Ocena i zatwierdzanie zastosowań AI odbywa się z udziałem właściwych komórek organizacyjnych, odpowiednio do charakteru zastosowania, w szczególności:
   a. Działu IT, w tym Kierownika Działu IT albo osoby przez niego upoważnionej – w zakresie technicznego dopuszczenia Narzędzia AI, bezpieczeństwa, kont, licencji, integracji, uprawnień, logowania zdarzeń, retencji, DLP, kopii zapasowych, ciągłości działania oraz konfiguracji;
   b. Inspektora Ochrony Danych – w zakresie danych osobowych, DPIA, umów powierzenia oraz Incydentów dotyczących danych osobowych;
   c. obsługi prawnej – w zakresie umów, praw autorskich, AI Act oraz wymagań klientów;
   d. właściwego właściciela biznesowego – w zakresie celu, uzasadnienia oraz kontroli wyników danego zastosowania.
4. Użytkownik odpowiada za przestrzeganie Polityki, ocenę dopuszczalności danych, zachowanie nadanych uprawnień, weryfikację wyniku pracy Narzędzia AI oraz zgłaszanie Incydentów.
5. Dział IT odpowiada, w granicach swoich kompetencji, za ocenę, zatwierdzenie i utrzymanie technicznych środków bezpieczeństwa dotyczących Narzędzi AI, w szczególności uwierzytelniania, uprawnień, logowania, retencji, DLP, integracji, kopii zapasowych i ciągłości działania, zgodnie z Polityką Bezpieczeństwa Informatycznego.
6. Zastosowania AI o podwyższonym poziomie ryzyka oraz odstępstwa od zasad określonych w Polityce wymagają akceptacji Zarządu EPK.

§9. Instruktaż i rozwój kompetencji w zakresie AI

1. Przed rozpoczęciem korzystania z Narzędzi AI do Celów służbowych Użytkownik odbywa Instruktaż AI odpowiedni do jego roli, wiedzy technicznej, doświadczenia, wykorzystywanych Narzędzi AI, kategorii danych oraz kontekstu zastosowania. Instruktaż AI jest ponawiany okresowo oraz w przypadku istotnej zmiany zasad korzystania z Narzędzi AI, zakresu dopuszczonych zastosowań, kategorii danych albo funkcjonalności Narzędzia AI.
2. Instruktaż AI obejmuje co najmniej:
   a. podstawowe informacje dotyczące działania, możliwości i ograniczeń Narzędzi AI;
   b. zasady wynikające z Polityki, Rejestru narzędzi i zastosowań AI oraz Macierzy dopuszczalności danych;
   c. zasady korzystania z kont firmowych i kont prywatnych;
   d. zasady ochrony danych chronionych, danych osobowych, informacji objętych NDA oraz dokumentacji klientów i projektów;
   e. obowiązek weryfikacji wyników Narzędzi AI, w tym ryzyko występowania błędów, nieaktualnych informacji i tzw. halucynacji;
   f. zasady dotyczące praw autorskich, licencji, norm technicznych, publikacji i materiałów pochodzących od osób trzecich;
   g. ryzyko prompt injection oraz zasady bezpiecznej pracy z dokumentami, wiadomościami, stronami internetowymi i innymi treściami zewnętrznymi;
   h. praktyki zakazane, ograniczenia dotyczące podejmowania decyzji wobec osób oraz zasady kontroli działań Agentów AI, integracji i automatyzacji;
   i. zasady zgłaszania Incydentów.

3. Program, treść, formę, częstotliwość oraz sposób dokumentowania Instruktażu AI określa Opiekun Polityki, z udziałem właściwych komórek organizacyjnych odpowiednio do zakresu instruktażu, w szczególności Działu IT, Inspektora Ochrony Danych, obsługi prawnej oraz właścicieli biznesowych zastosowań.

4. Instruktaż AI może być prowadzony w szczególności w formie szkolenia stacjonarnego, spotkania zdalnego, szkolenia elektronicznego, prezentacji, nagrania, materiału do samodzielnego zapoznania się albo połączenia tych form. Jeżeli wymaga tego zakres instruktażu, jego ukończenie może obejmować sprawdzenie wiedzy.

5. Opiekun Polityki prowadzi lub zapewnia prowadzenie aktualnych materiałów Instruktażu AI, zawierających co najmniej oznaczenie wersji i datę obowiązywania. Materiały instruktażowe mają charakter wykonawczy i nie stanowią załącznika do Polityki.

6. Zapoznanie się z Polityką Użytkownik potwierdza oświadczeniem według Załącznika nr 2 albo w postaci elektronicznego potwierdzenia zarejestrowanego w systemie wskazanym przez Firmę. Firma prowadzi ewidencję ukończenia Instruktażu AI, obejmującą co najmniej Użytkownika, datę ukończenia oraz wersję lub zakres instruktażu.

7. Dostęp do wskazanych Narzędzi AI, Agentów firmowych, integracji, konektorów lub zastosowań może zostać uzależniony od wcześniejszego ukończenia dodatkowego Instruktażu AI właściwego dla danego Narzędzia AI albo zastosowania.

§10. Postanowienia końcowe

1. Naruszenie Polityki może stanowić naruszenie obowiązków pracowniczych lub kontraktowych.

2. Zmiany treści Polityki oraz Załącznika nr 2 wprowadza się w trybie właściwym dla przyjęcia Polityki. Zmiany Załączników nr 1 i 3 wprowadza się w trybie określonym w ust. 4.

3. Polityka wchodzi w życie z dniem 23 października 2026 r.

4. Rejestr narzędzi i zastosowań AI stanowiący Załącznik nr 1 oraz Macierz dopuszczalności danych stanowiąca Załącznik nr 3 są dokumentami wykonawczymi prowadzonymi przez Opiekuna Polityki. Mogą być aktualizowane przez Opiekuna Polityki po uzyskaniu wymaganych akceptacji, w tym akceptacji Działu IT, a w odpowiednich przypadkach także IOD, obsługi prawnej i właściciela biznesowego. Każda zmiana podlega wersjonowaniu oraz udokumentowaniu wraz z datą, autorem i wykazem akceptacji. Aktualizacja nie może zmieniać ani osłabiać zasad wynikających z niniejszej Polityki lub Polityki Bezpieczeństwa Informatycznego.

5. Firma może monitorować i audytować korzystanie z Narzędzi AI w zakresie dopuszczonym przez prawo, dokumentację RODO i regulacje wewnętrzne. Monitoring prowadzi się na zasadach określonych w Polityce Bezpieczeństwa Informatycznego i ogranicza do informacji niezbędnych dla bezpieczeństwa, zgodności, jakości, obsługi Incydentów oraz właściwego wykorzystania licencji i zasobów. Dostęp do wyników monitoringu mają wyłącznie osoby upoważnione, a okresy retencji wynikają z obowiązujących procedur.

6. Załączniki stanowią integralną część Polityki, przy czym dla Załączników nr 1 i 3 stosuje się szczególny tryb aktualizacji określony w ust. 4. Szczegółowy zakres dopuszczenia konkretnego Narzędzia AI lub zastosowania wynika z aktualnej wersji Rejestru narzędzi i zastosowań AI.

Tytuł	Polityka korzystania z Narzędzi sztucznej inteligencji
Autor / zespół	Dział Transformacji Cyfrowej i Procesów
Data publikacji	23 października 2026
Wersja	1.0

REJESTR NARZĘDZI I ZASTOSOWAŃ AI

Rejestr zawiera wyłącznie Narzędzia AI i zastosowania, które uzyskały status „Zatwierdzone” zgodnie z §3 ust. 12 Polityki. Narzędzi i zastosowań będących w trakcie oceny nie zamieszcza się w Rejestrze. Jedna pozycja Rejestru odpowiada jednemu Narzędziu AI i jednemu zatwierdzonemu zastosowaniu. Jeżeli to samo Narzędzie AI ma kilka zastosowań różniących się celem, grupą Użytkowników, kategoriami danych, sposobem dostępu albo klasyfikacją według AI Act, każde zastosowanie ujmuje się jako odrębną pozycję.

Lp.	Narzędzie i wariant usługi	Zatwierdzony cel użycia	Dopuszczony sposób dostępu i rodzaj konta	Dopuszczeni Użytkownicy	Dopuszczone kategorie danych	Zastosowania i dane zabronione	Klasyfikacja zastosowania według AI Act	Właściciel zastosowania	Warunki dodatkowe
1	Microsoft 365 Copilot / Copilot Chat – środowisko EPK	Przygotowywanie, redagowanie, porządkowanie, podsumowywanie, tłumaczenie i analizowanie informacji w zatwierdzonym środowisku Microsoft 365. Wsparcie pracy z pocztą, dokumentami, prezentacjami, arkuszami, spotkaniami oraz innymi zasobami, do których Użytkownik posiada uprawnienia.	Wyłącznie Konto firmowe EPK, firmowy tenant Microsoft 365 oraz konfiguracja zatwierdzona przez Dział IT. Zakres dostępnych funkcji zależy od licencji przypisanej Użytkownikowi oraz konfiguracji środowiska EPK. Korzystanie za pośrednictwem Kont prywatnych jest niedozwolone. Wpis obejmuje zarówno Copilot Chat dostępny w środowisku EPK, jak i Microsoft 365 Copilot dla Użytkowników posiadających przypisaną licencję rozszerzoną.	Pracownicy i współpracownicy posiadający Konto firmowe EPK oraz odpowiednią licencję lub dostęp nadany zgodnie z zasadami obowiązującymi w Firmie, którzy ukończyli wymagany Instruktaż AI. Dostęp do rozszerzonych funkcji, Agentów AI, konektorów, integracji i dodatkowych źródeł danych może wymagać ukończenia dodatkowego Instruktażu AI oraz zostać ograniczony do wskazanych osób lub grup.	Dane publicznie dostępne. Informacje wewnętrzne, dane osobowe, dokumentacja projektowa i inne dane chronione – wyłącznie w zakresie dopuszczonym w Macierzy, zgodnym z uprawnieniami Użytkownika, celem użycia, wymaganiami projektu, umową i NDA.	Hasła, klucze, tokeny, dane logowania i nieujawnione podatności. Dane, których wykorzystania zabrania prawo, umowa, NDA, klient lub regulacja wewnętrzna. Samodzielne podejmowanie decyzji kadrowych, prawnych, finansowych, technicznych lub projektowych. Wykorzystywanie wyników bez wymaganej weryfikacji.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku zastosowania Narzędzia AI do podejmowania lub istotnego wspierania decyzji dotyczących osób, uruchomienia Agentów AI, podłączenia dodatkowych źródeł danych, konektorów lub integracji albo wdrożenia automatyzacji wykonującej działania w systemach Firmy.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów**. Właściciel techniczny: **Dział IT**. W sprawach danych osobowych: **IOD**.	Narzędzie korzysta wyłącznie z uprawnień posiadanych przez Użytkownika. Podłączenie nowego Agenta AI, konektora, wtyczki, źródła danych, API lub automatyzacji wymaga odrębnego zatwierdzenia. Sam fakt posiadania dostępu do dokumentu nie przesądza o możliwości wykorzystania go w AI.
2	ChatGPT Business – firmowa przestrzeń robocza EPK	Przygotowywanie, redagowanie, tłumaczenie, porządkowanie i analizowanie treści. Wsparcie researchu, przygotowywanie zestawień, materiałów roboczych, kodu, skryptów, zapytań i analiz. Praca z plikami wyłącznie w zakresie dopuszczonym w Macierzy. Wsparcie analizy, redagowania i porządkowania dokumentacji formalnej związanej z realizowanymi inwestycjami, w tym pism, umów, dokumentacji kontraktowej, projektowej, technicznej, ofertowej i handlowej. Wsparcie pracy z dokumentacją klientów i kontrahentów, w tym przygotowywania analiz, porównań, zestawień, projektów treści i materiałów roboczych, z zachowaniem obowiązku weryfikacji wyniku przez Użytkownika.	Wyłącznie konto służbowe w firmowej przestrzeni roboczej EPK oraz konfiguracji zatwierdzonej przez Firmę. Korzystanie z prywatnych kont ChatGPT do Celów służbowych jest niedozwolone, chyba że odrębny wpis w Rejestrze narzędzi i zastosowań AI wyraźnie dopuszcza konkretny sposób korzystania wyłącznie na Danych publicznie dostępnych.	Pracownicy i współpracownicy, którym przydzielono Konto firmowe lub dostęp do firmowej przestrzeni roboczej EPK i którzy ukończyli wymagany Instruktaż AI. Dostęp do Agentów AI, projektów współdzielonych, konektorów, integracji i innych funkcji rozszerzonych przysługuje wyłącznie wskazanym osobom lub grupom i może wymagać ukończenia dodatkowego Instruktażu AI właściwego dla danego zastosowania.	Dane publicznie dostępne. Informacje wewnętrzne, dane osobowe, dokumentacja projektowa, treści umów, dokumentów stanowiących zapytania Ofertowe, Ogólne Warunki Zamówień itp. oraz inne Dane chronione wyłącznie po wyraźnym dopuszczeniu danego zastosowania i kategorii danych w Rejestrze i Macierzy. Dopuszcza się przetwarzanie informacji wewnętrznych EPK, dokumentacji projektowej, technicznej, kontraktowej, handlowej i ofertowej, treści umów i korespondencji projektowej oraz innych Danych chronionych, w tym danych osobowych, w zakresie niezbędnym do zatwierdzonego celu, o ile nie zabrania tego prawo, umowa, NDA, wymaganie klienta, instrukcja projektu lub inna wiążąca regulacja.	Hasła, klucze, tokeny, dane logowania, nieujawnione podatności i szczegółowe konfiguracje zabezpieczeń. Dane niedopuszczone w Macierzy. Wprowadzanie dokumentów klientów lub dokumentacji objętej NDA bez sprawdzenia warunków umownych. Samodzielne podejmowanie decyzji wywołujących skutki prawne, finansowe, kadrowe, projektowe lub techniczne. Udostępnianie agentów lub podłączanie konektorów bez zatwierdzenia. Dane zakwalifikowane przez EPK, klienta, kontrahenta lub właściwy projekt do przetwarzania wyłącznie w środowisku lokalnym lub offline lub całkowicie niedopuszczone do przetwarzania.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku zastosowań dotyczących osób, podejmowania lub istotnego wspierania decyzji, Agentów AI, integracji, automatyzacji, przetwarzania danych osobowych albo rozszerzenia zakresu przetwarzanych danych.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów**. Właściciel techniczny: **Dział IT**. W sprawach danych osobowych: **IOD**.	Do korzystania dopuszcza się wyłącznie wariant usługi, zasady zarządzania kontami, retencję danych, zakres dostępu administratorów oraz integracje zatwierdzone zgodnie z procedurą określoną w §3 ust. 10–12 Polityki, z udziałem Opiekuna Polityki i Działu IT, a w przypadkach określonych w Polityce także Inspektora Ochrony Danych, obsługi prawnej i właściwego właściciela biznesowego. Agenci osobiści nie mogą być udostępniani innym osobom bez zatwierdzenia jako Agenci firmowi. Firmowa przestrzeń robocza ChatGPT Business jest skonfigurowana w sposób wyłączający wykorzystywanie danych EPK do trenowania lub ulepszania modeli dostawcy w zakresie przewidzianym dla tej usługi.
3	NotebookLM – konto prywatne Użytkownika	Analiza, porównywanie, organizowanie, streszczanie i wyszukiwanie informacji w publicznie dostępnych aktach prawnych, materiałach urzędowych, artykułach, publikacjach i innych materiałach, których warunki wykorzystania pozwalają na przesłanie ich do zewnętrznego Narzędzia AI.	Konto prywatne Użytkownika dopuszczone wyjątkowo i wyłącznie dla celu oraz danych wskazanych w niniejszym wpisie. Dopuszczenie konta prywatnego nie obejmuje żadnych innych zastosowań służbowych.	Pracownicy i współpracownicy, którzy zapoznali się z Polityką i ukończyli wymagany Instruktaż AI obejmujący w szczególności zasady korzystania z Kont prywatnych, rozpoznawania Danych publicznie dostępnych oraz wykorzystywania norm, publikacji i innych materiałów licencjonowanych. Firma może ograniczyć dopuszczenie do wskazanych komórek organizacyjnych, ról, projektów lub grup Użytkowników poprzez odpowiednią zmianę wpisu w Rejestrze.	Dane publicznie dostępne. Akty prawne, orzeczenia, komunikaty i materiały urzędowe publicznie udostępnione. Publiczne publikacje i inne materiały, które stanowią Dane publicznie dostępne w rozumieniu Polityki i których warunki wykorzystania pozwalają na przesłanie ich do zewnętrznego Narzędzia AI. Normy, specyfikacje techniczne i inne materiały licencjonowane wyłącznie wtedy, gdy stanowią Dane publicznie dostępne w rozumieniu Polityki, a warunki ich licencji pozwalają na przesłanie ich do zewnętrznego Narzędzia AI.	Wszystkie informacje wewnętrzne EPK. Dane osobowe i dane spseudonimizowane. Dokumentacja klientów, dokumentacja projektowa, techniczna, kontraktowa, ofertowa, handlowa oraz dokumentacja objęta NDA. Tajemnica przedsiębiorstwa, know-how i dane finansowe nieujawnione publicznie. Kod źródłowy, skrypty, konfiguracje i dokumentacja systemowa Firmy lub klientów. Hasła, klucze dostępowe, tokeny, kody uwierzytelniające, dane logowania, nieujawnione podatności i konfiguracje zabezpieczeń. Łączenie Danych publicznie dostępnych z informacjami niepublicznymi. Przesyłanie norm, publikacji, raportów, baz wiedzy lub innych materiałów, które nie stanowią Danych publicznie dostępnych albo których warunki licencji nie pozwalają na przesłanie do zewnętrznego Narzędzia AI.	**Pozostałe zastosowanie dla opisanego celu pracy na Danych publicznie dostępnych.** Każde rozszerzenie celu, grupy Użytkowników, kategorii danych lub sposobu korzystania wymaga ponownej oceny i aktualizacji wpisu.	**Dział Transformacji Cyfrowej i Procesów**.	Sam fakt posiadania dostępu do dokumentu nie oznacza, że dokument jest publicznie dostępny ani że może zostać przesłany do NotebookLM. W przypadku wątpliwości materiału nie wolno przesyłać. Dopuszczalne jest wykorzystywanie własnych notatek lub opisów wymagań sporządzonych własnymi słowami wyłącznie wtedy, gdy powstały na podstawie Danych publicznie dostępnych, nie zawierają Danych chronionych ani informacji dotyczących niepublicznych spraw Firmy, jej klientów, kontrahentów lub projektów oraz nie naruszają warunków licencji ani praw osób trzecich.

Lp.	Narzędzie i wariant usługi	Zatwierdzony cel użycia	Dopuszczony sposób dostępu i rodzaj konta	Dopuszczeni Użytkownicy	Dopuszczone kategorie danych	Zastosowania i dane zabronione	Klasyfikacja zastosowania według AI Act	Właściciel zastosowania	Warunki dodatkowe
4	OpenAI Codex – w ramach ChatGPT Business	Tworzenie, analiza, refaktoryzacja, objaśnianie i weryfikacja kodu, skryptów, makr, zapytań, konfiguracji i narzędzi wewnętrznych. Wsparcie tworzenia prototypów, aplikacji, automatyzacji, pipeline'ów przetwarzania dokumentów, narzędzi RAG oraz innych rozwiązań rozwijanych przez EPK. Analiza plików i repozytoriów wyłącznie w zakresie dopuszczonym niniejszym wpisem i Macierzą.	Wyłącznie Konto firmowe w firmowej przestrzeni roboczej ChatGPT Business EPK oraz urządzenie i jego konfiguracja. Dostęp do funkcji terminala, repozytoriów, integracji i wykonywania działań może zostać ograniczony do wskazanych Użytkowników i środowisk.	Pracownicy i współpracownicy, którym przydzielono dostęp do ChatGPT Business i Codex oraz którzy ukończyli wymagany Instruktaż AI. Dostęp do repozytoriów, systemów i funkcji wykonawczych wyłącznie w granicach faktycznych uprawnień Użytkownika.	Dane publicznie dostępne. Informacje wewnętrzne, dane osobowe, dokumentacja projektowa, treści umów, dokumentów stanowiących zapytania Ofertowe, Ogólne Warunki Zamówień itp. oraz inne Dane chronione wyłącznie po wyraźnym dopuszczeniu danego zastosowania i kategorii danych w Rejestrze i Macierzy. Kod źródłowy, skrypty, makra, zapytania, konfiguracje i dokumentacja systemowa EPK oraz dokumentacja projektowa i techniczna w zakresie dopuszczonym w Rejestrze i Macierzy. Dla niniejszego wpisu dopuszcza się przetwarzanie informacji wewnętrznych EPK, dokumentacji projektowej, technicznej, kontraktowej, handlowej i ofertowej, treści umów i korespondencji projektowej oraz innych Danych chronionych, w tym danych osobowych, w zakresie niezbędnym do zatwierdzonego celu, o ile nie zabrania tego prawo, umowa, NDA, wymaganie klienta, instrukcja projektu lub inna wiążąca regulacja.	Hasła, klucze dostępowe, tokeny, certyfikaty prywatne, dane logowania, kody uwierzytelniające, nieujawnione podatności i szczegółowe konfiguracje zabezpieczeń. Uruchamianie kodu lub poleceń bez wymaganej weryfikacji, testów i kontroli zgodnie z zasadami bezpieczeństwa oraz zarządzania zmianą. Samodzielne wykonywanie działań powodujących skutki prawne, finansowe, kadrowe, projektowe lub techniczne bez wymaganej kontroli człowieka.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku rozszerzenia uprawnień wykonawczych, automatycznego wykonywania działań, podłączenia nowych repozytoriów, systemów, konektorów lub danych albo zastosowania do istotnego wspierania decyzji dotyczących osób.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów.** Właściciel techniczny: **Dział IT.** W sprawach danych osobowych: **IOD.**	Każdy kod, skrypt, konfiguracja lub polecenie wygenerowane przez Codex wymaga przeglądu i przetestowania przed użyciem w środowisku Firmy. Codex nie może otrzymywać dostępu do danych ani systemów szerszego niż uprawnienia nadane Użytkownikowi. Zastosowania wykorzystujące terminal, wykonywanie poleceń, integracje lub automatyczne modyfikacje zasobów wymagają odpowiedniego ograniczenia uprawnień i kontroli.
5	ChatGPT Pro – firmowe konto indywidualne poza przestrzenią roboczą EPK	Przygotowywanie, redagowanie, tłumaczenie, porządkowanie i analizowanie treści oraz wsparcie researchu i przygotowywania materiałów roboczych. Zastosowanie uzupełniające względem ChatGPT Business, wykonywane w bardziej restrykcyjnym zakresie danych.	Wyłącznie indywidualne konto ChatGPT Pro, którego licencja jest finansowana lub przypisana przez Firmę, lecz które nie jest częścią firmowej przestrzeni roboczej ChatGPT Business EPK. Ustawienia wykorzystywania treści do trenowania lub ulepszania modeli muszą pozostawać wyłączone. Korzystanie z prywatnych, niezatwierdzonych kont do Celów służbowych jest niedozwolone.	Wyłącznie wskazani pracownicy i współpracownicy, którym Firma przydzieliła licencję ChatGPT Pro i którzy ukończyli wymagany Instruktaż AI.	Dane publicznie dostępne. Kod źródłowy, skrypty, makra, zapytania, konfiguracje i dokumentacja systemowa EPK oraz dokumentacja projektowa i techniczna w zakresie dopuszczonym w Rejestrze i Macierzy. Dokumentacja klientów i kontrahentów wyłącznie, gdy pozwalają na to umowa, NDA, wymagania klienta i zasady projektu.	Hasła, klucze dostępowe, tokeny, certyfikaty prywatne, dane logowania, kody uwierzytelniające, nieujawnione podatności i szczegółowe konfiguracje zabezpieczeń. Uruchamianie kodu lub poleceń bez wymaganej weryfikacji, testów i kontroli zgodnie z zasadami bezpieczeństwa oraz zarządzania zmianą. Samodzielne wykonywanie działań powodujących skutki prawne, finansowe, kadrowe, projektowe lub techniczne bez wymaganej kontroli człowieka.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Każde rozszerzenie kategorii danych, celu lub sposobu dostępu wymaga ponownej oceny i aktualizacji wpisu.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów.** Właściciel techniczny: **Dział IT.** W sprawach danych osobowych: **IOD.**	Konto musi pozostawać pod kontrolą organizacyjną Firmy w zakresie licencji i zatwierdzonej konfiguracji. Przed użyciem Użytkownik weryfikuje, że ustawienia prywatności i wykorzystywania treści do ulepszania modeli pozostają zgodne z konfiguracją zatwierdzoną przez Firmę. Codex nie może otrzymywać dostępu do danych ani systemów szerszego niż uprawnienia nadane Użytkownikowi. Zastosowania wykorzystujące terminal, wykonywanie poleceń, integracje lub automatyczne modyfikacje zasobów wymagają odpowiedniego ograniczenia uprawnień i kontroli.
6	Lokalne środowisko AI – Ollama / modele lokalne	Lokalne uruchamianie zatwierdzonych modeli AI na infrastrukturze EPK do analizy dokumentów, ekstrakcji danych, RAG, wyszukiwania semantycznego, generowania i analizy treści, klasyfikacji, embeddingów oraz prac badawczo-rozwojowych. Przetwarzanie danych o wysokiej poufności w trybie odizolowanym od Internetu, zgodnie z warunkami niniejszego wpisu.	Wyłącznie lokalna infrastruktura EPK, zatwierdzone stacje robocze lub serwery oraz modele uruchamiane lokalnie, bez przekazywania danych do zewnętrznych usług AI. Dla danych o najwyższym poziomie poufności: wyłącznie stacja robocza odłączona od Internetu i innych niezaufanych sieci przez cały okres obecności danych na urządzeniu.	Wyłącznie wskazani pracownicy i współpracownicy posiadający uprawnienia do danego środowiska i danych oraz wymagany Instruktaż AI. Dostęp do środowisk przetwarzających dane o najwyższej poufności może być dodatkowo ograniczony do imiennie wskazanych osób.	Dane publicznie dostępne oraz Dane chronione w zakresie dopuszczonym przez prawo, umowę, NDA, wymagania klienta, instrukcję projektu i uprawnienia Użytkownika. Dokumentacja klienta, projektowa, techniczna, kontraktowa, handlowa, ofertowa, dane osobowe, tajemnica przedsiębiorstwa i know-how – warunkowo, zgodnie z Macierzą i warunkami danego projektu. Dane zakwalifikowane do przetwarzania wyłącznie offline – wyłącznie w odizolowanym trybie pracy określonym w niniejszym wpisie.	Hasła, klucze dostępowe, tokeny, kody uwierzytelniające, certyfikaty prywatne i dane logowania. Nieujawnione podatności, szczegółowe konfiguracje zabezpieczeń i informacje umożliwiające nieuprawniony dostęp. Dane, których wykorzystania w AI zabrania prawo, umowa, NDA, klient, właściciel informacji, warunki licencji lub regulacja wewnętrzna.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku podłączenia zewnętrznego API, funkcji sieciowej, narzędzia wykonującego działania w systemach Firmy, nowej kategorii danych albo zastosowania dotyczącego decyzji wobec osób.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów.** Właściciel techniczny: **Dział IT.** W sprawach danych osobowych: **IOD.**	Zatwierdzone rodziny i komponenty modelowe obejmują w szczególności: Meta Llama, OpenAI gpt-oss, modele embeddingowe rodziny mxbai oraz IBM Granite/Granite-Docling, a także inne modele lokalne zatwierdzone przez Dział Transformacji Cyfrowej i Procesów oraz Dział IT. Zmiana wersji modelu w ramach zatwierdzonej rodziny może być prowadzona jako zmiana techniczna, o ile nie zmienia zakresu danych, sposobu działania, funkcji sieciowych, warunków licencyjnych ani profilu ryzyka. Dodanie nowej rodziny modelu lub istotnie odmiennej funkcji wymaga ponownej oceny. Przed ponownym podłączeniem odizolowanej stacji roboczej do Internetu dane o najwyższej poufności oraz ich kopie robocze muszą zostać usunięte zgodnie z procedurą zatwierdzoną przez Dział IT.
7	Langflow – lokalna platforma budowy workflow AI/RAG	Budowanie, testowanie i uruchamianie lokalnych pipeline'ów AI, w szczególności do analizy i ekstrakcji dokumentów, RAG, wyszukiwania semantycznego, klasyfikacji, generowania treści oraz orkiestracji zatwierdzonych modeli lokalnych.	Wyłącznie lokalna instalacja lub środowisko EPK zatwierdzone przez Dział IT. Dla Danych chronionych wykorzystywane mogą być wyłącznie zatwierdzone lokalne modele, endpointy i komponenty. Podłączenie zewnętrznego API, modelu chmurowego, konektora lub zewnętrznego źródła danych wymaga odrębnego zatwierdzenia.	Wyłącznie wskazani pracownicy i współpracownicy posiadający uprawnienia do środowiska oraz wymagany Instruktaż AI.	Dane publicznie dostępne oraz Dane chronione w zakresie dopuszczonym dla lokalnego środowiska AI i konkretnego workflow. Dane o najwyższym poziomie poufności wyłącznie wtedy, gdy cały pipeline, modele, magazyny danych i komponenty działają lokalnie na odizolowanej stacji roboczej bez dostępu do Internetu.	Przesyłanie Danych chronionych do niezatwierdzonych zewnętrznych API, modeli, konektorów, telemetryki lub usług. Hasła, klucze, tokeny, dane logowania, nieujawnione podatności i informacje umożliwiające nieuprawniony dostęp. Workflow wykonujące działania w innych systemach bez wymaganej kontroli i zatwierdzenia.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku dodania zewnętrznych integracji, funkcji wykonawczych, nowych kategorii danych albo udostępnienia workflow szerszej grupie Użytkowników.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów.** Właściciel techniczny: **Dział IT.** W sprawach danych osobowych: **IOD.**	Konfiguracja workflow musi zapewniać, że dane są kierowane wyłącznie do zatwierdzonych modeli, komponentów i magazynów danych. Dla danych o najwyższej poufności obowiązują warunki izolacji i usuwania danych określone dla lokalnego środowiska modeli AI. Każdy workflow przed użyciem produkcyjnym podlega przeglądowi i testom.

Lp.	Narzędzie i wariant usługi	Zatwierdzony cel użycia	Dopuszczony sposób dostępu i rodzaj konta	Dopuszczeni Użytkownicy	Dopuszczone kategorie danych	Zastosowania i dane zabronione	Klasyfikacja zastosowania według AI Act	Właściciel zastosowania	Warunki dodatkowe
8	n8n – lokalna platforma automatyzacji i orkiestracji workflow AI	Budowanie, testowanie i uruchamianie lokalnych pipeline'ów AI, w szczególności do analizy i ekstrakcji dokumentów, RAG, wyszukiwania semantycznego, klasyfikacji, generowania treści oraz orkiestracji zatwierdzonych modeli lokalnych.	Wyłącznie lokalna instalacja lub środowisko EPK zatwierdzone przez Dział IT. Dla Danych chronionych wykorzystywane mogą być wyłącznie zatwierdzone lokalne modele, endpointy i komponenty. Podłączenie zewnętrznego API, modelu chmurowego, konektora lub zewnętrznego źródła danych wymaga odrębnego zatwierdzenia.	Wyłącznie wskazani pracownicy i współpracownicy posiadający uprawnienia do środowiska oraz wymagany Instruktaż AI.	Dane publicznie dostępne oraz Dane chronione w zakresie dopuszczonym dla lokalnego środowiska AI i konkretnego workflow. Dane o najwyższym poziomie poufności wyłącznie wtedy, gdy cały pipeline, modele, magazyny danych i komponenty działają lokalnie na odizolowanej stacji roboczej bez dostępu do Internetu.	Przesyłanie Danych chronionych do niezatwierdzonych zewnętrznych API, modeli, konektorów, telemetryki lub usług. Hasła, klucze, tokeny, dane logowania, nieujawnione podatności i informacje umożliwiające nieuprawniony dostęp. Workflow wykonujące działania w innych systemach bez wymaganej kontroli i zatwierdzenia.	**Pozostałe zastosowanie dla opisanego sposobu użycia.** Ponowna ocena jest wymagana w przypadku dodania zewnętrznych integracji, funkcji wykonawczych, nowych kategorii danych albo udostępnienia workflow szerszej grupie Użytkowników.	Właściciel biznesowy: **Dział Transformacji Cyfrowej i Procesów.** Właściciel techniczny: **Dział IT.** W sprawach danych osobowych: **IOD.**	Konfiguracja workflow musi zapewniać, że dane są kierowane wyłącznie do zatwierdzonych modeli, komponentów i magazynów danych. Dla danych o najwyższej poufności obowiązują warunki izolacji i usuwania danych określone dla lokalnego środowiska modeli AI. Każdy workflow przed użyciem produkcyjnym podlega przeglądowi i testom.

Załącznik nr 2

OŚWIADCZENIE O ZAPOZNANIU SIĘ Z POLITYKĄ I ODBYCIU INSTRUKTAŻU AI

Katowice, dnia .....

OŚWIADCZENIE PRACOWNIKA

Imię i nazwisko: .....

Komórka organizacyjna / podmiot: .....

Oświadczam, że:

1. zapoznałem/zapoznałam się z „Polityką korzystania z Narzędzi sztucznej inteligencji” obowiązującą w ENERGOPROJEKT-KATOWICE SA;

2. zobowiązuję się do przestrzegania Polityki oraz zasad określonych dla dopuszczonych Narzędzi AI i ich zastosowań.

[podpis]

MACIERZ DOPUSZCZALNOŚCI DANYCH W NARZĘDZIACH AI

Ogólne zasady określające, jakie kategorie danych mogą być przetwarzane w poszczególnych klasach Narzędzi AI

Brak wyraźnego dopuszczenia Narzędzia AI, zastosowania, rodzaju konta, grupy Użytkowników lub kategorii danych w Rejestrze oznacza zakaz ich użycia.

Kategoria danych	Microsoft 365 Copilot / Copilot Chat – Konto firmowe EPK	Inne Narzędzie AI ujęte w Rejestrze – Konto firmowe lub firmowa przestrzeń robocza	Narzędzie AI ujęte w Rejestrze i wyraźnie dopuszczone do użycia za pośrednictwem Konta prywatnego
Dane publicznie dostępne	**Dopuszczalne**, jeżeli wykorzystanie jest zgodne z prawem, zatwierdzonym celem, warunkami licencji i prawami osób trzecich.	**Dopuszczalne**, jeżeli wpis w Rejestrze nie stanowi inaczej.	**Dopuszczalne,** wyłącznie w Narzędziu AI, dla zastosowania, sposobu dostępu i grupy Użytkowników wyraźnie wskazanych w Rejestrze, bez łączenia z informacjami niepublicznymi. Użytkownik sprawdza, czy wykorzystanie materiału jest zgodne z prawem, warunkami licencji, prawami autorskimi i regulaminem źródła.
Akty prawne, orzeczenia, komunikaty i materiały urzędowe publicznie udostępnione	**Dopuszczalne.**	**Dopuszczalne**, jeżeli wpis w Rejestrze nie wprowadza dodatkowych ograniczeń.	**Dopuszczalne**, jeżeli materiał został zgodnie z prawem udostępniony nieograniczonemu kręgowi odbiorców i nie jest łączony z informacjami niepublicznymi.
Dane prawidłowo zanonimizowane, których nie można przypisać do osoby fizycznej	**Dopuszczalne**, jeżeli nie zawierają innych Danych chronionych.	**Dopuszczalne**, jeżeli wpis w Rejestrze nie stanowi inaczej i anonimizacja jest rzeczywista.	**Zabronione**, chyba że dane zostały zgodnie z prawem udostępnione nieograniczonemu kręgowi odbiorców, stanowią Dane publicznie dostępne w rozumieniu Polityki i ich użycie zostało wyraźnie dopuszczone w Rejestrze.
Informacje wewnętrzne Firmy, które nie zawierają danych osobowych, tajemnicy przedsiębiorstwa ani informacji objętych NDA	**Warunkowo dopuszczalne**, jeżeli pozwalają na to wpis w Rejestrze, cel użycia, uprawnienia Użytkownika oraz wymagania projektu.	**Warunkowo dopuszczalne**, wyłącznie gdy wpis w Rejestrze wyraźnie dopuszcza daną kategorię i zastosowanie.	Zabronione.
Dane osobowe pracowników, współpracowników, klientów lub innych osób	**Warunkowo dopuszczalne**, po spełnieniu wymagań §4 Polityki, w zakresie niezbędnym, zgodnym z RODO, podstawą prawną, uprawnieniami i wpisem w Rejestrze.	**Warunkowo dopuszczalne**, po spełnieniu wymagań §4 Polityki oraz wyraźnym dopuszczeniu Narzędzia, celu, Użytkowników i kategorii danych w Rejestrze.	Zabronione.
Dane spseudonimizowane	Traktowane jak dane osobowe. **Warunkowo dopuszczalne** na zasadach dotyczących danych osobowych.	Traktowane jak dane osobowe. **Warunkowo dopuszczalne** na zasadach dotyczących danych osobowych.	Zabronione.
Dane szczególnych kategorii, dane dotyczące zdrowia, niepełnosprawności, poglądów, przynależności związkowej, biometrii lub inne dane wymagające podwyższonej ochrony	**Warunkowo dopuszczalne wyłącznie wyjątkowo**, po odrębnej ocenie z udziałem IOD i wyraźnym dopuszczeniu danego zastosowania.	**Warunkowo dopuszczalne wyłącznie wyjątkowo**, po odrębnej ocenie z udziałem IOD i wyraźnym wpisie w Rejestrze.	Zabronione.
Tajemnica przedsiębiorstwa, know-how i informacje stanowiące o przewadze konkurencyjnej Firmy lub kontrahenta	**Warunkowo dopuszczalne**, wyłącznie w zakresie wskazanym w Rejestrze, przy zachowaniu minimalizacji, uprawnień i wymaganych środków bezpieczeństwa.	**Warunkowo dopuszczalne**, po wyraźnym dopuszczeniu Narzędzia, zastosowania, grupy Użytkowników i kategorii danych.	Zabronione.
Dane finansowe nieujawnione publicznie	**Warunkowo dopuszczalne**, jeżeli wpis w Rejestrze, cel użycia oraz zakres uprawnień wyraźnie na to pozwalają.	**Warunkowo dopuszczalne**, po wyraźnym zatwierdzeniu danego zastosowania i kategorii danych.	Zabronione.
Dokumentacja klienta, projektowa, techniczna, kontraktowa, handlowa, ofertowa lub objęta NDA	**Warunkowo dopuszczalne**, gdy pozwalają na to umowa, NDA, wymagania klienta, instrukcja projektu, wpis w Rejestrze oraz uprawnienia Użytkownika. Obowiązuje minimalizacja danych.	**Warunkowo dopuszczalne**, wyłącznie po zatwierdzeniu Narzędzia dla konkretnego projektu, zastosowania, grupy Użytkowników i kategorii dokumentacji.	Zabronione.
Normy techniczne, płatne publikacje, komentarze, raporty, bazy wiedzy i inne materiały licencjonowane	**Warunkowo dopuszczalne**, jeżeli pozwalają na to warunki licencji, umowa z dostawcą materiału oraz wpis w Rejestrze.	**Warunkowo dopuszczalne**, po sprawdzeniu warunków licencji i wyraźnym dopuszczeniu w Rejestrze.	**Zabronione,** chyba że materiał stanowi Dane publicznie dostępne w rozumieniu Polityki, został wyraźnie dopuszczony w Rejestrze, a warunki jego licencji pozwalają na przesłanie go do zewnętrznego Narzędzia AI. Sam fakt posiadania legalnego dostępu do materiału nie oznacza zgody na przesłanie go do Narzędzia AI.
Własne notatki Użytkownika dotyczące norm, publikacji lub materiałów licencjonowanych	**Dopuszczalne**, jeżeli nie zawierają Danych chronionych ani fragmentów wykorzystanych z naruszeniem licencji.	**Dopuszczalne**, jeżeli wpis w Rejestrze nie stanowi inaczej, a notatki nie zawierają danych niedopuszczonych ani treści wykorzystanych z naruszeniem licencji.	**Dopuszczalne**, wyłącznie, jeżeli notatki stanowią opracowanie Danych publicznie dostępnych, zostały sporządzone własnymi słowami, nie zawierają Danych chronionych ani informacji dotyczących niepublicznych spraw Firmy, jej klientów, kontrahentów lub projektów, a ich wykorzystanie nie narusza warunków licencji ani praw osób trzecich.
Kod źródłowy, skrypty, makra, zapytania, konfiguracje i dokumentacja systemowa Firmy	**Warunkowo dopuszczalne**, jeżeli nie zawierają danych dostępowych, podatności ani innych niedopuszczonych informacji i dane zastosowanie zostało zatwierdzone.	**Warunkowo dopuszczalne**, po wyraźnym dopuszczeniu Narzędzia i zastosowania, z zachowaniem wymagań bezpieczeństwa, praw autorskich i licencji.	**Zabronione.**
Kod źródłowy, dokumentacja lub rozwiązania należące do klienta albo osoby trzeciej	**Warunkowo dopuszczalne**, wyłącznie, jeżeli pozwalają na to umowa, licencja, NDA, wymagania klienta oraz wpis w Rejestrze.	**Warunkowo dopuszczalne**, po odrębnym zatwierdzeniu konkretnego zastosowania.	**Zabronione.**
Hasła, klucze dostępowe, tokeny, kody uwierzytelniające, certyfikaty prywatne i dane logowania	**Zabronione.**	**Zabronione.**	**Zabronione.**
Nieujawnione podatności, informacje o lukach bezpieczeństwa, szczegółowe konfiguracje zabezpieczeń i informacje umożliwiające nieuprawniony dostęp	**Zabronione.**	**Zabronione.**	**Zabronione.**
Dane publiczne połączone z informacjami wewnętrznymi lub niepublicznymi	Stosuje się zasady właściwe dla kategorii danych o **najwyższym poziomie ochrony** występującej w materiale.	Stosuje się zasady właściwe dla kategorii danych o **najwyższym poziomie ochrony** występującej w materiale.	**Zabronione.**
Dane przeznaczone do podejmowania lub istotnego wspierania decyzji dotyczących rekrutacji, zatrudnienia, oceny, awansu, wynagrodzenia, rozwiązania współpracy lub innych istotnych decyzji wobec osób	**Zabronione**, chyba że zastosowanie zostało objęte odrębną procedurą, oceną ryzyka i zatwierdzeniem przez uprawnione organy Firmy.	**Zabronione**, chyba że zastosowanie zostało objęte odrębną procedurą, oceną ryzyka i zatwierdzeniem przez uprawnione organy Firmy.	**Zabronione.**
Dane, których wykorzystania w AI zabrania prawo, umowa, NDA, klient, właściciel informacji, warunki licencji lub regulacja wewnętrzna	Zabronione.	Zabronione.	**Zabronione.**