URZĄD OCHRONY DANYCH OSOBOWYCH

SPOŁECZNY ZESPÓŁ EKSPERTÓW PRZY PUODO

LISTY PYTAŃ INICJALNYCH

Podejście funkcjonalne: pytania projektowe + pytania o zgodność z RODO

Wersja 0 (RODO) | Wersja 0+ (RODO + AI Act) | Wersja MŚP | Wersja sektor publiczny

5 sierpnia 2026 r.

JAK KORZYSTAĆ Z OPRACOWANIA?

Opracowanie ma dwa poziomy. Poziom wejściowy tworzą trzy niezależne listy, wybierane według profilu adresata i przedmiotu wdrożenia: Wersja 0 – dla organizacji, które nie mieszczą się w dwóch pozostałych profilach, w tym dla podmiotów budujących lub dotrenowujących własne rozwiązania; Wersja dla MŚP – dla firm korzystających z gotowych narzędzi AI, bez fazy trenowania; Wersja dla sektora publicznego – dla jednostek realizujących zadania publiczne.

Poziom pogłębiony stanowi Wersja Rozszerzona. Sięgnąć po nią należy, niezależnie od tego, która z list z poziomu wejściowego została wypełniona, gdy zachodzi co najmniej jedna z sytuacji: organizacja buduje albo dotrenowuje model; wynik systemu wpływa na sytuację prawną osób; przetwarzane są dane szczególnych kategorii, dane dzieci lub dane o wyrokach; dane są przekazywane poza EOG; system może być systemem wysokiego ryzyka w rozumieniu aktu w sprawie sztucznej inteligencji (AI Act). Wersja Rozszerzona obejmuje także sygnalizację odnoszącą się do AI Act.

O wyborze wersji rozstrzyga przedmiot oceny, nie schemat organizacyjny. Wyznaczenie inspektora ochrony danych nie decyduje o tym, którą listę należy wypełnić.

WERSJA 0: CHECKLISTA ZEROWA – PODEJŚCIE FUNKCJONALNE

Poziom: wejściowy – lista samodzielna, niezależna od pozostałych

Podstawa: RODO

Dla kogo: organizacje, które nie mieszczą się w profilu listy dla MŚP ani listy dla sektora publicznego, w tym podmioty budujące lub dotrenowujące własne rozwiązania

Cel: ustalić, czy i w jakim zakresie wdrożenie dotyczy danych osobowych, jakie obowiązki się z nim wiążą i jakich informacji brakuje do podjęcia decyzji, zebrać wstępne ustalenia potrzebne do przeprowadzenia analizy ryzyka, oceny skutków dla ochrony danych i wykazania zgodności z RODO

Moment: etap koncepcji i wyboru narzędzia, przed zakupem lub rozpoczęciem prac

Kiedy stosować: przy każdym wdrożeniu lub budowie systemu AI, odrębnie dla każdego procesu, w którym system ma być wykorzystywany; także wtedy, gdy działające już narzędzie ma zostać rozszerzone na nowy proces

Kiedy ta lista nie wystarczy: gdy zachodzi co najmniej jedna z sytuacji: organizacja buduje albo dotrenowuje model na własnych danych; wynik systemu wpływa na sytuację prawną osób; przetwarzane są dane szczególnych kategorii, dane dzieci lub dane o wyrokach; dane są przekazywane poza EOG; system może być systemem wysokiego ryzyka w rozumieniu AI Act.

Wynik: decyzja, czy prace mogą być kontynuowane, oraz czy konieczne jest przejście do Wersji Rozszerzonej

Podejście funkcjonalne: pytania projektowe (P) dostarczają wiedzy o systemie, pytania o zgodność (Z) weryfikują wymogi RODO, oznaczenie P/Z łączy oba aspekty

Założenia metodologiczne

Podejście funkcjonalne

Lista łączy dwa uzupełniające się rodzaje pytań. Pytania projektowe (P) identyfikują cel, charakter i kontekst wdrożenia AI, dostawcę, dane oraz gotowość organizacyjną – dostarczają wiedzy niezbędnej do oceny zgodności. Pytania o zgodność (Z) weryfikują spełnienie konkretnych wymogów RODO, w szczególności podstawę prawną, prawa osób, obowiązki informacyjne, ocenę skutków dla ochrony danych, uwzględnianie ochrony danych w fazie projektowania i powierzenie przetwarzania. Oznaczenie P/Z wskazuje pytanie łączące oba aspekty.

Oba rodzaje pytań są ze sobą powiązane: pytanie projektowe „Jakie dane przetwarza system?” jest warunkiem wstępnym dla pytania o zgodność „Czy istnieje podstawa prawna przetwarzania tych danych?”. Struktura listy odzwierciedla ten związek.

Fazy cyklu życia systemu AI

Każde pytanie oznaczono symbolem fazy, w której ma ono znaczenie:

Symbol	Faza	Opis
[T]	**Trenowanie / Rozwój**	Opracowywanie i trenowanie modelu AI: dane treningowe, budowa modelu, testowanie.
[W]	**Wdrożenie / Użycie**	Wdrażanie gotowego systemu AI bez trenowania: konfiguracja, integracja, codzienne użycie.
[T+W]	**Obie fazy**	Kwestie wspólne: role RODO, rejestr czynności przetwarzania, IOD, data protection by design/default, DPIA, bezpieczeństwo.

Pytania wstępne o zasadność wdrożenia

Lista rozpoczyna się od pytań o zasadność wdrożenia systemu AI. Pozwalają one ustalić, czy korzyści z budowy lub wdrożenia systemu przewyższają związane z nim ryzyka. Dotyczą w szczególności: adekwatności AI do natury rozwiązywanego problemu, zdolności systemu do spełnienia potrzeb organizacji, sprawiedliwości wpływu systemu na różne grupy osób, jakości i reprezentatywności dostępnych danych, wystarczalności zasobów ludzkich i materialnych oraz ryzyka użycia systemu poza jego przeznaczeniem.

Pytania te pełnią funkcję komplementarną wobec pytań o zgodność - ustalają kontekst decyzyjny, z którego wynikają konsekwencje zarówno projektowe, jak i regulacyjne.

Przeznaczenie listy i sposób jej wypełnienia

Lista służy wstępnej identyfikacji zagadnień ochrony danych osobowych związanych z opracowywaniem lub wykorzystywaniem systemu sztucznej inteligencji. Jest to narzędzie poziomu zerowego: pozwala ustalić, czy i w jakim zakresie planowane lub prowadzone działanie dotyczy danych osobowych, jakie obowiązki wynikające z RODO mogą się z nim wiązać oraz jakich informacji brakuje, by ocenę zgodności przeprowadzić rzetelnie. Wynik jej wypełnienia rozstrzyga również, czy konieczne jest przejście do Wersji Rozszerzonej.

Lista nie zastępuje analizy ryzyka ani oceny skutków dla ochrony danych (DPIA). Jej wypełnienie stanowi natomiast materiał wejściowy do obu tych analiz. Wypełnienie listy nie jest równoznaczne z potwierdzeniem zgodności wdrożenia z RODO.

Instrukcja wypełniania

1. Listę wypełnia się odrębnie dla każdego procesu, w którym system AI ma być tworzony lub wykorzystywany. Jedno narzędzie może być wykorzystywane w wielu procesach o różnym profilu ryzyka – ogólna ocena narzędzia nie jest wystarczająca.
2. Listę wypełnia właściciel biznesowy procesu przy udziale inspektora ochrony danych, jeżeli został wyznaczony, albo osoby odpowiedzialnej za ochronę danych. Pytania techniczne wymagają udziału osoby odpowiedzialnej za system informatyczny.
3. Odpowiedź „WYJAŚNIJ” wybiera się, gdy pytanie wymaga opisu, a nie rozstrzygnięcia tak/nie, albo gdy odpowiedź nie jest jednoznaczna. Krótkie uzasadnienie wpisuje się w kolumnie „Działanie” lub w załączniku do listy. Tę samą odpowiedź wybiera się, gdy pytanie nie dotyczy danego przypadku, wskazując powód. Odpowiedź „WYJAŚNIJ” bez wpisanego wyjaśnienia traktuje się jak brak odpowiedzi.
4. Pole odpowiedzi pozostawione puste oznacza, że organizacja nie zna odpowiedzi. Na etapie wypełniania nie jest to błąd, ale każdy taki brak odnotowuje się w kolumnie „Działanie” wraz z osobą odpowiedzialną i terminem. Kolumna „Wyjaśnienie / Źródło” wskazuje, gdzie szukać odpowiedzi.
5. Organizacje wdrażające gotowy system bez jego trenowania mogą pominąć pytania oznaczone [T]. Pytania [W] i [T+W] dotyczą wszystkich.
6. Wypełnioną listę należy zachować. Stanowi ona element dokumentacji rozliczalności (art. 5 ust. 2 RODO) i punkt odniesienia przy późniejszej weryfikacji wdrożenia.
7. Wypełnianie listy kończy się, gdy przy każdym pytaniu jest odpowiedź, a tam, gdzie odpowiedź ujawnia potrzebę działania, w kolumnie „Działanie” wpisano zadanie, osobę odpowiedzialną i termin.
8. Zadania nie są równorzędne. Zadania dotyczące warunków legalności przetwarzania, tj. w szczególności ustalenia podstawy prawnej, przesłanki przetwarzania danych szczególnych kategorii, powierzenia przetwarzania, podstawy przekazania danych poza EOG, obowiązku informacyjnego, nadzoru człowieka nad decyzjami wywołującymi skutki prawne oraz oceny skutków dla ochrony danych, jeżeli jest wymagana, wykonuje się przed rozpoczęciem

przetwarzania. Decyzji o wdrożeniu nie podejmuje się, dopóki nie zostaną wykonane.

9. Zadania dotyczące środków organizacyjnych, np. szkoleń, polityki AI, procedur reagowania na incydenty, procedur zarządzania danymi, dokumentacji technicznej, mogą być realizowane równolegle z wdrożeniem, w terminach wskazanych w kolumnie „Działanie”, o ile ryzyko w tym czasie pozostaje kontrolowane.
10. Odrębną kategorię stanowią sytuacje, w których wdrożenie w zaplanowanym kształcie jest niedopuszczalne np. w pełni zautomatyzowana decyzja wywołująca skutki prawne podejmowana automatycznie bez mechanizmu interwencji człowieka, czynność zastrzeżona przepisami dla człowieka, praktyka zakazana w zakresie AI.. Nie planuje się tu zadania z terminem konieczna jest zmiana konstrukcji procesu albo odstąpienie od wdrożenia.

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
1. CEL I ZASADNOŚĆ WDROŻENIA AI (WHY?)					
1	**P [T+W]**	Jaki konkretny problem lub potrzebę organizacyjną lub publiczną ma rozwiązać AI?	Zdefiniowanie celu jest warunkiem oceny zgodności celów przetwarzania danych (art. 5 ust. 1 lit. b RODO). Źródło: dokumentacja projektowa, biznesplan.		
2	**P [T+W]**	Czy ten cel da się osiągnąć bez AI lub istniejącymi technologiami? Jeśli tak uzasadnij swoją odpowiedź w jaki sposób osiągnięcie celu za pomocą AI będzie lepsze od osiągania go innymi / tradycyjnymi środkami?	Należy ocenić, na ile istniejące technologie i procesy rozwiązują problem lepiej, biorąc pod uwagę profil ryzyka AI i potencjalne negatywne skutki. Istotne dla testu proporcjonalności i minimalizacji przetwarzania.		
3	**P [T+W]**	Jakie korzyści mierzalne (czas,	Określenie oczekiwanych		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		koszty, zyski, jakość usług) są oczekiwane?	korzyści pozwala ocenić proporcjonalność wdrożenia i adekwatność przetwarzania danych osobowych.		
4	**P [T+W]**	Jakie ryzyka reputacyjne, prawne, społeczne lub ryzyka dla człowieka, jego praw i wolności, mogą się pojawić?	Wstępna identyfikacja ryzyk pozwala określić, czy wymagana będzie DPIA (art. 35 RODO). Źródło: analiza wstępna, konsultacja z IOD.		
5	**P [W]**	Czy na podstawie obecnych założeń istnieją przesłanki, że system spełni potrzeby i oczekiwania organizacji?	Należy ocenić, na ile planowany system spełni potrzeby i oczekiwania podmiotu wdrażającego. Niedopasowanie systemu zwiększa ryzyko przetwarzania nadmiarowych danych.		
6	**P [W]**	Czy system podejmuje autonomiczne decyzje wobec osób fizycznych?	Kluczowe dla art. 22 RODO (decyzje zautomatyzowane). Określa zakres wymaganych gwarancji i nadzoru ludzkiego.		
2. CHARAKTER SYSTEMU AI I ZAKRES AUTONOMII (WHAT?)					
7	**P [T+W]**	Co robi system AI: generuje treści, klasyfikuje osoby/dane, przewiduje zachowania, rekomenduje działania, wspiera decyzje?	Określenie funkcji systemu jest niezbędne do oceny: profilowania (art. 4 pkt 4 RODO), zautomatyzowanego podejmowania decyzji (art. 22), zakresu DPIA.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
8	**P [W]**	Czy wynik działania AI jest wiążący, rekomendacyjny, czy jedynie informacyjny?	Decyduje o zastosowaniu art. 22 RODO (decyzje automatyczne). Jeśli wiążący lub wywiera istotny wpływ – wymagane gwarancje z art. 22 ust. 3.		
9	**P [W]**	Czy system będzie wykorzystywany wobec osób fizycznych (np. klientów, obywateli, pracowników, dzieci)?	Kluczowe dla identyfikacji osób, których dane dotyczą, i zakresu obowiązków informacyjnych (art. 13–14 RODO).		
10	**P [W]**	Czy organizacja kupuje / wdraża gotowy system AI, czy buduje własny? (build vs. deploy)	Rozróżnienie determinuje zakres odpowiedzialności RODO: budujący odpowiada za dane treningowe, wdrażający za dane wejściowe i użycie.		
11	**P [W]**	Czy organizacja posiada wiedzę o architekturze systemu i instrukcjach dostawcy?	Znajomość architektury i konfiguracji warunkuje skuteczność data protection by design (art. 25) oraz ocenę ryzyka.		
12	**P [W]**	Określ w jakim stopniu Twoja organizacja będzie miała wpływ na rozwój systemu AI?	Odpowiedź na to pytanie weryfikuje poprawność kwalifikacji z pytania 10.		
13	**P [T+W]**	Czy są ryzyka użycia systemu poza jego przeznaczeniem?	Należy zidentyfikować potencjalne konteksty użycia systemu i ryzyka nadużycia, w tym wdrożenia wykraczającego		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			poza pierwotne przeznaczenie. Relewantne dla data protection by design (art. 25).		
3. DANE – IDENTYFIKACJA I ŹRÓDŁA (DATA?)					
14	**P/Z [T+W]**	Czy system AI przetwarza dane osobowe (bezpośrednio, pseudonimizowane lub generuje inferencje o osobach)?	Art. 4 pkt 1 RODO. Pytanie fundamentalne – 41–58,5% organizacji nie identyfikuje tego związku (Raport Strategiczny). Źródło: dokumentacja systemu.		
15	**P [T+W]**	Jakie kategorie danych przetwarza AI: zwykłe, szczególne (art. 9), dane dzieci (art. 8), dane dot. wyroków (art. 10)?	Kategoria danych determinuje podstawę prawną, zakres DPIA i poziom ochrony. Źródło: dokumentacja techniczna, instrukcja dostawcy.		
16	**P [T]**	Skąd pochodzą dane treningowe, testowe, walidacyjne: np. z własnych zasobów, dane publiczne, dane od dostawcy, od innych podmiotów trzecich dane syntetyczne, inne?	Źródło danych wpływa na: zgodność celów (art. 6 ust. 4), podstawę prawną, obowiązki informacyjne. Źródło: dokumentacja dostawcy, model card.		
17	**P [T+W]**	Jaki jest zakres danych przetwarzanych na etapie trenowania, danych wejściowych i danych wyjściowych?	Rozróżnienie zakresu danych w poszczególnych fazach jest niezbędne do prawidłowej oceny podstaw prawnych, retencji i minimalizacji.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
18	**P [T+W]**	Czy jakość i reprezentatywność danych jest wystarczająca, by system był skuteczny i bezpieczny?	Należy ocenić, na ile jakość i reprezentatywność danych jest wystarczająca, by racjonalnie uniknąć potencjalnych szkodliwych uprzedzeń. Relewantne dla prawidłowości danych (art. 5 ust. 1 lit. d) i niedyskryminacji.		
19	**P/Z [T+W]**	Czy organizacja ma wdrożone procedury zarządzania danymi (data governance): klasyfikację danych, kontrolę ich jakości, zarządzanie dostępem i wersjonowanie zbiorów?	Wyznaczenie roli odpowiedzialnej za dane (pytanie 29) nie jest tożsame z wdrożeniem procedur. Bez procedur organizacja nie sprawuje faktycznej kontroli nad danymi zasilającymi system AI, co uniemożliwia wykazanie zgodności z zasadami prawidłowości (art. 5 ust. 1 lit. d RODO), minimalizacji (lit. c) oraz rozliczalności (art. 5 ust. 2 RODO). Źródło: polityka zarządzania danymi, procedury wewnętrzne.		
20	**Z [T+W]**	Czy organizacja zna podstawę prawną przetwarzania danych w AI (art. 6 ust. 1 RODO)?	Jedna z sześciu przesłanek art. 6 ust. 1. Dla danych szczególnych – odrębna przesłanka z art. 9 ust. 2. Należy uwzględnić m.in.:		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			- dane treningowe, walidacyjne i testowe; - dane wejściowe; - dane wyjściowe (generowane przez system); - wszelkie dane budujące kontekst. Źródło: analiza prawna, opinia IOD.		
21	**Z [T]**	Czy cel przetwarzania danych w systemie AI jest zgodny z celem pierwotnego zbierania danych (art. 5 ust. 1 lit. b, art. 6 ust. 4 RODO)?	Kluczowe przy wykorzystaniu istniejących zbiorów danych do trenowania lub zasilania systemu AI. Jeśli cel przetwarzania w AI różni się od celu pierwotnego zbierania danych, wymagana jest ocena zgodności celów (test kompatybilności – art. 6 ust. 4 RODO) lub uzyskanie nowej, odrębnej podstawy prawnej przetwarzania.		
22	**Z [T+W]**	Czy określono okresy przechowywania danych treningowych, danych wejściowych i wyników działania systemu, w tym historii interakcji i logów (art. 5 ust. 1 lit. e RODO)?	Zasada ograniczenia przechowywania wymaga określenia okresu dla każdej kategorii danych i ich usunięcia po ustaniu celu. W systemach AI dotyczy to również historii zapytań, danych w pamięci kontekstowej i logów. Źródło: polityka retencji, umowa z dostawcą, ustawienia systemu.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
4. ROLE, ODPOWIEDZIALNOŚĆ I DOSTAWCY (WHO? / FROM WHOM?)					
23	**P/Z [T+W]**	Kim, w odniesieniu do procesu wykorzystującego AI, jest organizacja w kontekście RODO: administratorem, współadministratorem, podmiotem przetwarzającym?	Kwalifikacja roli determinuje zakres obowiązków. "Podmiot przetwarzający" (nie "użytkownik systemu AI") – terminologia RODO. Źródło: umowa z dostawcą.		
24	**P [W]**	Czy AI jest kupowana jako usługa, rozwijana wewnętrznie, czy oparta na modelach zewnętrznych?	Model dostępu wpływa na: transfer danych, role RODO, zakres umowy powierzenia, kontrolę nad danymi. Źródło: dokumentacja zakupu/wdrożenia.		
25	**Z [W]**	Czy zawarto umowę powierzenia przetwarzania z dostawcą AI (art. 28 RODO)?	Obowiązkowa, gdy dostawca przetwarza dane w imieniu organizacji. Musi regulować: przedmiot, czas, charakter, cel, kategorie danych i osób. Należy zweryfikować czy dostawca zastrzega sobie prawo do wykorzystania danych we własnych celach ze skutkami z art. 28 ust. 10 RODO.		
26	**P [W]**	Czy dostawca ujawnia źródła danych treningowych i zapewnia dokumentację modelu?	Źródło informacji kluczowe dla DPIA, oceny ryzyka bias, zgodności celów. AI Act wymaga karty modelu i instrukcji użycia od dostawców.		
27	**P [W]**	Czy model AI jest oparty na rozwiązaniu	Typ modelu wpływa na zakres kontroli		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		open source czy zamkniętym (closed source)?	nad przetwarzaniem, możliwość audytu, transparentność i ocenę ryzyka.		
28	**P/Z [T+W]**	Czy wyznaczono: właściciela biznesowego AI, osobę odpowiedzialną za compliance, inspektora ochrony danych?	Art. 35 ust. 2, art. 38–39 RODO. IOD powinien być włączony na najwcześniejszym etapie. Jasne role = rozliczalność (art. 5 ust. 2).		
29	**P [T+W]**	Czy wyznaczono rolę odpowiedzialną za zarządzanie danymi (data governance)?	Zarządzanie danymi (data governance) zapewnia jakość, spójność i dostępność danych w całym cyklu życia systemu AI.		
30	**P [T+W]**	Czy dostępne są wystarczające zasoby (ludzkie i materialne) do zarządzania ryzykami AI?	Należy ocenić, czy dostępne są wystarczające zasoby do realizacji działań technicznych i zarządczych w celu ograniczenia zidentyfikowanych ryzyk. 75,2% organizacji nie ma ekspertów AI/RODO (Raport).		
5. TRANSFER DANYCH I BEZPIECZEŃSTWO					
31	**P/Z [T+W]**	Czy dane przetwarzane przez AI są przekazywane poza EOG (chmura, API, serwery dostawcy)?	Art. 44–49 RODO. Wymagana podstawa transferu: decyzja o adekwatności, SCC, BCR. Źródło: DPA dostawcy, lokalizacja serwerów.		
32	**Z [T+W]**	Czy uwzględniono wymogi data protection by design i by default (art. 25	Ochrona danych w fazie projektowania: minimalizacja, pseudonimizacja,		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		RODO)?, Jeśli tak wyjaśnij w jaki sposób.	kontrola dostępu przy wyborze i konfiguracji AI. Domyślna ochrona: przetwarzanie tylko danych niezbędnych.		
33	**Z [T+W]**	Czy wdrożono środki bezpieczeństwa odpowiednie do ryzyka: kontrolę dostępu, szyfrowanie, rozdzielenie środowisk, ochronę przed ujawnieniem danych w wynikach systemu (art. 32 RODO)?	Art. 32 RODO wymaga środków odpowiednich do ryzyka, przy uwzględnieniu stanu wiedzy technicznej. W systemach AI istotne są ryzyka specyficzne: ujawnienie danych w odpowiedzi modelu, wstrzyknięcie polecenia (prompt injection), nieuprawniony dostęp do historii zapytań. Źródło: analiza ryzyka, dokumentacja techniczna.		
34	**Z [T+W]**	Czy procedura postępowania z naruszeniami ochrony danych obejmuje zdarzenia związane z systemem AI i czy wiadomo, kto oraz w jakim terminie dokonuje zgłoszenia (art. 33–34 RODO)?	Naruszeniem może być ujawnienie danych w wyniku działania modelu, wprowadzenie danych do narzędzia niedopuszczonego w organizacji albo nieuprawniony dostęp do historii zapytań. Zgłoszenie organowi nadzorczemu następuje bez zbędnej zwłoki, nie później niż w 72 godziny. Źródło: procedura		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			postępowania z naruszeniami.		
6. PRAWA OSÓB I TRANSPARENTNOŚĆ (HOW?)					
35	**P/Z [W]**	Jak osoby zostaną poinformowane o użyciu AI i jakie informacje otrzymają (art. 13–14 RODO)?	Art. 13 ust. 2 lit. f / art. 14 ust. 2 lit. g: informacja o zasadach działania AI, znaczeniu i konsekwencjach. Źródło: aktualne klauzule informacyjne.		
36	**Z [W]**	Czy zapewniono realizację praw osób w kontekście AI: dostęp, sprostowanie, usunięcie, sprzeciw, niepodleganie decyzjom automatycznym (art. 15–22)?	System musi technicznie umożliwiać realizację praw. Art. 22 ust. 3: prawo do interwencji ludzkiej. Źródło: konfiguracja systemu, procedury wewnętrzne.		
37	**P [W]**	Czy organizacja potrafi wyjaśnić działanie AI w sposób zrozumiały dla osób, których dane dotyczą?	Zasada przejrzystości (art. 5 ust. 1 lit. a). Wyjaśnialność jako element data protection by design. Źródło: dokumentacja dostawcy, testy.		
38	**P [T+W]**	Czy wpływ systemu będzie sprawiedliwy wobec różnych grup osób?	Należy ocenić, na ile skutki będą sprawiedliwe wobec różnych grup, których system dotyczy. Relewantne dla niedyskryminacji i oceny skutków przy DPIA.		
7. OCENA SKUTKÓW, DOKUMENTACJA I GOTOWOŚĆ (RISK? / ARE WE READY?)					
39	**Z [T+W]**	Czy przeprowadzono lub zaplanowano DPIA (art. 35 RODO)?	Wymagana m.in. przy: systematycznej ocenie osób, przetwarzaniu na		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			dużą skalę danych szczególnych, innowacyjnej technologii. Wykaz PUODO, Wytyczne EROD.		
40	**Z [T+W]**	Czy zidentyfikowano procesy, w których narzędzie AI będzie tworzone lub wykorzystywane i zaktualizowano stosownie RCP o przetwarzanie w ramach AI (art. 30)?	Obowiązek formalny i narzędzie rozliczalności. RCP powinien obejmować: cel, kategorie danych, odbiorców, retencję, środki bezpieczeństwa, ocenione w kontekście narzędzi AI.		
41	**P [T+W]**	Czy ocena ryzyka uwzględnia specyfikę typu modelu AI, jego komponentów i zasobów?	Ocena ryzyka powinna być dopasowana do konkretnego systemu: typ modelu, źródła danych, interfejsy, zależności od dostawców, uwzględniać charakter, kontekst, cele przetwarzania, zakres danych oraz stan wiedzy technicznej i koszty wdrożenia Powinna się ona odbywać z perspektywy wpływu na prawa i wolności podmiotów danych. Ocenić należy prawdopodobieństwo i powagę ziszczenia się ryzyka.		
42	**P [T+W]**	Czy organizacja posiada: politykę AI, procedury reagowania na incydenty AI,	Gotowość organizacyjna warunkuje skuteczność		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		zasoby kadrowe i finansowe?	compliance. 95,9% organizacji nie czuje się przygotowanych (Raport). Źródło: dokumentacja wewnętrzna.		
43	**P [T+W]**	Czy planowane jest szkolenie pracowników w zakresie bezpiecznego korzystania z AI?	Szkolenie użytkowników jest elementem data protection by design i ogranicza ryzyko niewłaściwego użycia systemu.		
44	**P [T+W]**	Czy określono procedury reagowania na incydenty związane z jakością danych w systemie AI?	Procedury powinny obejmować: wykrywanie błędów danych, eskalację, korekcję i dokumentowanie incydentów jakości danych.		
45	**P/Z [T+W]**	Czy przewidziano okresowy przegląd systemu po wdrożeniu: monitorowanie jakości wyników, wykrywanie pogorszenia skuteczności (dryf modelu) oraz ponowną ocenę przy istotnej zmianie systemu, danych lub sposobu korzystania?	Wypełniona lista odnosi się do stanu na dzień oceny. Aktualizacja modelu przez dostawcę, rozszerzenie zakresu danych albo nowe zastosowanie systemu wymagają ponownej oceny; bez cyklicznego przeglądu rozliczalność (art. 5 ust. 2 RODO) nie jest utrzymywana w czasie. Źródło: plan przeglądów, raporty z monitorowania.		
46	**P/Z [T+W]**	Czy zidentyfikowano, czy system AI może podlegać AI Act (klasyfikacja ryzyka)?	Pytanie sygnalizacyjne: czy system może być klasyfikowany jako wysokiego ryzyka (art. 6, Załącznik I, III		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			AI Act)? Jeśli tak – przejdź do Wersji Rozszerzonej.		
47	**P/Z [W]**	Czy wykorzystanie systemu sztucznej inteligencji nie będzie praktyką zakazaną w rozumieniu art. 5 AI Act?	Art. 5 AI Act zawiera listę zakazanych praktyk w zakresie AI.		
48	**Z [W]**	Czy zapewniono wymogi transparentności AI Act (art. 50 – systemy GPAI, chatboty, deepfakes)?	Art. 50 AI Act ustanawia wymogi transparentności: oznaczanie treści generowanych przez AI, informowanie o interakcji z chatbotem, oznaczanie deepfakes.		

Legenda typów: P = pytanie projektowe (dostarcza wiedzę), Z = pytanie o zgodność z RODO (weryfikuje wymóg), P/Z = pytanie łączące oba aspekty. Organizacje wdrażające gotowe systemy (bez trenowania) mogą pominąć pytania [T].

WERSJA DLA SEKTORA PUBLICZNEGO: CHECKLISTA RODO DLA AI

Poziom: wejściowy – lista samodzielna, niezależna od pozostałych

Podstawa: RODO

Dla kogo: jednostki samorządu terytorialnego, urzędy administracji publicznej i inne podmioty realizujące zadania publiczne

Cel: ustalić dopuszczalność wykorzystania AI w danym procesie oraz zakres obowiązków wobec obywateli

Moment: etap koncepcji i wyboru narzędzia, przed zakupem lub rozpoczęciem prac

Kiedy stosować: przy każdym wdrożeniu systemu AI w jednostce, odrębnie dla każdego rodzaju spraw. Przejście do Wersji Rozszerzonej jest konieczne, gdy jednostka buduje lub dotrenowuje model, gdy system wpływa na sytuację prawną obywateli, gdy przetwarzane są dane szczególnych kategorii lub dane dzieci, gdy dane są przekazywane poza EOG albo gdy system może być systemem wysokiego ryzyka; w sektorze publicznym przesłanki te spełnia znaczna część wdrożeń, ponieważ wiele zastosowań publicznych mieści się w załączniku III do AI Act

Wynik: decyzja o dopuszczalności wdrożenia, materiał do dokumentacji postępowania o wdrożenie systemu oraz decyzja czy konieczne jest przejście do Wersji Rozszerzonej

Podejście funkcjonalne: pytania projektowe (P) dostarczają wiedzy o systemie, pytania o zgodność (Z) weryfikują wymogi RODO, oznaczenie P/Z łączy oba aspekty, z uwzględnieniem specyfiki sektora publicznego

Założenia metodologiczne

Podejście funkcjonalne

Lista łączy dwa uzupełniające się rodzaje pytań. Pytania projektowe (P) identyfikują cel, charakter i kontekst wdrożenia AI, dostawcę, dane oraz gotowość organizacyjną – dostarczają wiedzy niezbędnej do oceny zgodności. Pytania o zgodność (Z) weryfikują spełnienie konkretnych wymogów RODO, w szczególności podstawę prawną, prawa osób, obowiązki informacyjne, ocenę skutków dla ochrony danych, uwzględnianie ochrony danych w fazie projektowania i powierzenie przetwarzania. Oznaczenie P/Z wskazuje pytanie łączące oba aspekty.

Oba rodzaje pytań są ze sobą powiązane: pytanie projektowe „Jakie dane przetwarza system?” jest warunkiem wstępnym dla pytania o zgodność „Czy istnieje podstawa prawna przetwarzania tych danych?”. Struktura listy odzwierciedla ten związek.

Fazy cyklu życia systemu AI

Każde pytanie oznaczono symbolem fazy, w której ma ono znaczenie:

Symbol	Faza	Opis
[T]	**Trenowanie / Rozwój**	Opracowywanie i trenowanie modelu AI: dane treningowe, budowa modelu, testowanie.
[W]	**Wdrożenie / Użycie**	Wdrażanie gotowego systemu AI bez trenowania: konfiguracja, integracja, codzienne użycie.
[T+W]	**Obie fazy**	Kwestie wspólne: role RODO, rejestr czynności przetwarzania, IOD, data protection by design/default, DPIA, bezpieczeństwo.

Pytania wstępne o zasadność wdrożenia

Lista rozpoczyna się od pytań o zasadność wdrożenia systemu AI. Pozwalają one ustalić, czy korzyści z budowy lub wdrożenia systemu przewyższają związane z nim ryzyka. Dotyczą w szczególności adekwatności AI do natury rozwiązywanego problemu, zdolności systemu do spełnienia potrzeb organizacji, sprawiedliwości wpływu systemu na różne grupy osób, jakości i reprezentatywności dostępnych danych, wystarczalności zasobów ludzkich i materialnych oraz ryzyka użycia systemu poza jego przeznaczeniem.

Pytania te pełnią funkcję komplementarną wobec pytań o zgodność - ustalają kontekst decyzyjny, z którego wynikają konsekwencje zarówno projektowe, jak i regulacyjne.

Przeznaczenie listy i sposób jej wypełnienia

Lista jest przeznaczona dla jednostek samorządu terytorialnego, urzędów administracji publicznej i innych podmiotów realizujących zadania publiczne. Uwzględnia zasadę legalizmuoraz szczególną odpowiedzialność podmiotów publicznych wobec obywateli, w tym osób w szczególnie wrażliwej sytuacji.

Lista nie zastępuje oceny skutków dla ochrony danych (DPIA) ani oceny wpływu na prawa podstawowe (FRIA), które w sektorze publicznym przy systemach AI są wymagane w większości przypadków. Stanowi materiał wejściowy do obu ocen. Nie zastępuje również analizy ryzyka, a wypełnienie listy nie jest równoznaczne z potwierdzeniem zgodności wdrożenia z RODO.

Instrukcja wypełniania

1. Listę wypełnia kierownik komórki merytorycznej odpowiedzialnej za proces, w którym system ma być wykorzystywany, przy udziale inspektora ochrony danych.
2. Włączenie inspektora ochrony danych jest obligatoryjne, jego wyznaczenie w podmiotach publicznych wynika z art. 37 ust. 1 lit. a RODO, a udział w ocenie wdrożenia z art. 38 ust. 1 i art. 39 RODO.
3. Jeżeli system ma wspierać wydawanie rozstrzygnięć w sprawach indywidualnych lub załatwianie spraw, listę należy skonsultować również z radcą prawnym obsługującym jednostkę.
4. Listę wypełnia się odrębnie dla każdego rodzaju spraw lub procesu, w którym system ma być wykorzystywany.
5. Pole odpowiedzi pozostawione puste oznacza lukę informacyjną, którą odnotowuje się w kolumnie „Działanie” wraz z osobą odpowiedzialną i terminem. Brak ustalonej podstawy prawnej wyklucza wdrożenie – zasada legalizmu nie dopuszcza działania w warunkach niepewności co do umocowania. Jeżeli pytanie nie dotyczy danego przypadku, wybiera się „WYJAŚNIJ” i wskazuje powód; „WYJAŚNIJ” bez wyjaśnienia traktuje się jak brak odpowiedzi.
6. Wypełnioną listę załącza się do dokumentacji postępowania o wdrożenie systemu, w tym postępowania o udzielenie zamówienia publicznego, i zachowuje jako element dokumentacji rozliczalności (art. 5 ust. 2 RODO).
7. Wypełnianie listy kończy się, gdy przy każdym pytaniu jest odpowiedź, a tam, gdzie odpowiedź ujawnia potrzebę działania, w kolumnie „Działanie” wpisano zadanie, osobę odpowiedzialną i termin.
8. Zadania nie są równorzędne. Zadania dotyczące warunków legalności tj. ustalenia podstawy prawnej i przepisu pozwalającego na wykorzystanie AI w danym procesie, nadzoru człowieka nad rozstrzygnięciami, obowiązku informacyjnego, podstawy przekazania danych poza EOG oraz oceny skutków dla ochrony danych – wykonuje się przed uruchomieniem systemu. Zasada legalizmu nie dopuszcza działania w warunkach niepewności co do umocowania.
9. Zadania dotyczące środków organizacyjnych, np. szkoleń, polityk, procedur reagowania na incydenty, procedur zarządzania danymi, dokumentacji

technicznej, mogą być realizowane równolegle z korzystaniem z systemu, w terminach wskazanych w kolumnie „Działanie”.

10. Jeżeli brak jest przepisu pozwalającego na wykorzystanie AI w danym procesie albo czynność jest zastrzeżona przepisami dla człowieka, nie planuje się zadania z terminem, konieczna jest zmiana konstrukcji procesu albo odstąpienie od wdrożenia.

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
1. CEL I ZASADNOŚĆ (WHY?)					
1	**P [T+W]**	Jaki problem / potrzebę publiczny ma rozwiązać AI i czy jest to adekwatne do natury problemu?	Należy ocenić, czy istniejące rozwiązania nie są wystarczające. Uzasadnienie wdrożenia warunkuje dalszą ocenę RODO.		
2	**P [T+W]**	Jakie korzyści mierzalne (czas, koszty, zyski, jakość usług) są oczekiwane?	Określenie korzyści pozwala ocenić proporcjonalność przetwarzania danych i zasadność wydatkowania środków publicznych.		
3	**P [T+W]**	Jakie ryzyka dla praw obywateli lub ryzyka dla człowieka mogą się pojawić? Czy wpływ będzie sprawiedliwy wobec różnych grup?	Należy ocenić, na ile skutki będą sprawiedliwe wobec grup, których dotyczą. Sektor publiczny: szczególna odpowiedzialność wobec wszystkich obywateli, w tym grup wrażliwych.		
2. CHARAKTER SYSTEMU (WHAT?)					
4	**P [W]**	Czy AI wspiera lub podejmuje decyzje	Art. 22 RODO + zasada prawdy		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		administracyjne wobec osób fizycznych albo wspiera lub załatwia sprawy niekończące się decyzjami administracyjnymi a wpływające na sferę praw obywateli?	obiektywnej KPA. Decyzja administracyjna musi być wydana przez urzędnika.		
5	**P [W]**	Czy system podejmuje autonomiczne decyzje wobec osób fizycznych?	Kluczowe dla art. 22 RODO. Autonomiczność decyzji determinuje zakres wymaganych gwarancji i nadzoru ludzkiego.		
6	**P [W]**	Czy wynik AI wpływa na prawa, wolności lub obowiązki obywateli?	Determinuje zakres: DPIA, obowiązki informacyjne, prawo do interwencji ludzkiej, FRIA.		
7	**P [T+W]**	Czy organizacja wdrażając gotowy system lub budując własny zna architekturę i konfigurację?	Rozróżnienie build/deploy determinuje zakres odpowiedzialności. Znajomość architektury warunkuje data protection by design.		
8	**P [T+W]**	Czy są ryzyka użycia systemu poza jego przeznaczeniem?	Należy zidentyfikować potencjalne konteksty użycia i ryzyka nadużycia. W sektorze publicznym: ryzyko rozszerzenia nadzoru,		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			profilowania obywateli.		
3. DANE OSOBOWE OBYWATELI (DATA?)					
9	**P/Z [T+W]**	Czy system przetwarza dane osobowe obywateli, petentów, beneficjentów świadczeń?	Art. 4 pkt 1 RODO. Obejmuje dane mieszkańców, stron postępowań. Źródło: dokumentacja systemu.		
10	**P [T+W]**	Czy wśród danych są dane szczególnych kategorii (zdrowie, orzeczenia) i grupy wrażliwe (dzieci, osoby z niepełnosprawnościami)?	Art. 9, art. 8 RODO. Sektor publiczny: pomoc społeczna, edukacja, zdrowie. Szczególną uwagę należy zwrócić na grupy w szczególnie wrażliwej sytuacji.		
11	**P [T+W]**	Czy jakość i reprezentatywność danych jest wystarczająca?	Istotne jest zidentyfikowanie ryzyka stronniczości systemu oraz określenie i wdrożenie środków mających zapobiegać generowaniu wyników niesprawiedliwych lub dyskryminujących określone grupy osób (bias). Ryzyko to występuje również w danych publicznych. Źródło: dokumentacja		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			systemu, analiza danych.		
12	**P/Z [T+W]**	Czy wdrożono procedury zarządzania danymi (data governance) obejmujące dane obywateli wykorzystywane w systemie AI: klasyfikację informacji, kontrolę jakości danych, zarządzanie dostępem i dokumentowanie pochodzenia danych?	Wdrożone procedury warunkują faktyczną kontrolę nad danymi i możliwość wykazania rozliczalności (art. 5 ust. 2 RODO). W sektorze publicznym istotne również dla zasady prawdy obiektywnej i możliwości weryfikacji podstaw rozstrzygnięcia. Pytanie uzupełnia pytanie 26 dotyczące roli odpowiedzialnej za data governance. Źródło: polityka zarządzania danymi, instrukcja kancelaryjna, regulaminy wewnętrzne.		
13	**Z [T+W]**	Czy określono okresy przechowywania danych obywateli przetwarzanych w systemie, w tym danych wejściowych, wyników i logów, spójnie z instrukcją kancelaryjną i jednolitym rzeczowym wykazem akt (art. 5 ust. 1 lit. e RODO)?	Okresy przechowywania w jednostce publicznej wynikają z przepisów o narodowym zasobie archiwalnym oraz z instrukcji kancelaryjnej i JRWA. Dane w systemie AI, w tym historia zapytań i		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			logi, nie mogą być przechowywane bezterminowo ani krócej, niż wymagają tego przepisy o archiwizacji. Źródło: instrukcja kancelaryjna, JRWA, polityka retencji.		
4. PODSTAWA PRAWNA					
14	**Z [T+W]**	Czy określono podstawę prawną: obowiązek prawny (art. 6 ust. 1 lit. c) lub zadanie w interesie publicznym (lit. e)?	W sektorze publicznym lit. f (uzasadniony interes) co do zasady nie ma zastosowania.		
15	**P/Z [W]**	Czy istnieje przepis prawa umożliwiający wykorzystanie AI w danym procesie decyzyjnym?	Zasada legalizmu. AI Act + przepisy sektorowe. Czy KPA dopuszcza wspomaganie algorytmem?		
5. NADZÓR CZŁOWIEKA I TRANSPARENTNOŚĆ (HOW?)					
16	**Z [W]**	Czy zapewniono nadzór człowieka nad wynikami AI, szczególnie przy decyzjach / załatwianych sprawach wpływających na prawa obywateli?	Art. 22 ust. 3 RODO + art. 14 AI Act. Prawo do rozpatrzenia sprawy przez człowieka, prawo do odwołania.		
17	**Z [W]**	Czy obywatele są informowani o wykorzystaniu AI (art. 13–14 RODO)?	Klauzule informacyjne: informacja o AI, zasady działania, znaczenie, konsekwencje. Art. 50 AI Act.		
18	**P [W]**	Czy organizacja jest w stanie wyjaśnić obywatelowi, jak AI	Przejrzystość (art. 5 ust. 1 lit. a). Data protection by design (art. 25) –		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		wpłynęło na decyzję / załatwioną sprawę?	wyjaśnialność systemowa. Informowanie o wykorzystaniu systemu wysokiego ryzyka (art. 26 ust. 11 AI Act). Prawo osoby, której dotyczy decyzja oparta na systemie wysokiego ryzyka, do wyjaśnienia roli tego systemu w procesie decyzyjnym oraz głównych elementów decyzji (art. 86 ust. 1 AI Act)		
6. DOSTAWCA, TRANSFER, BEZPIECZEŃSTWO					
19	**Z [W]**	Czy zawarto umowę powierzenia z dostawcą AI (art. 28)?	Obowiązkowa. Sektor publiczny: szczególne wymogi dot. kontroli i audytu.		
20	**P [W]**	Czy model AI jest oparty na rozwiązaniu open source czy zamkniętym (closed source)?	Typ modelu wpływa na zakres kontroli, możliwość audytu i transparentność. W sektorze publicznym – istotne dla rozliczalności.		
21	**P/Z [T+W]**	Czy dane są przetwarzane wyłącznie na terenie EOG?	Sektor publiczny: szczególna ostrożność. Dane obywateli nie powinny co do zasady opuszczać EOG.		
22	**Z [T+W]**	Czy wdrożono środki bezpieczeństwa	Kontrola dostępu, szyfrowanie,		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		odpowiednie do ryzyka (art. 32)?	monitoring, klasyfikacja informacji (dane zastrzeżone, poufne).		
23	**Z [T+W]**	Czy procedura postępowania z naruszeniami ochrony danych obejmuje zdarzenia związane z systemem AI (art. 33–34 RODO)?	Naruszeniem może być ujawnienie danych obywatela w wyniku działania modelu, nieuprawniony dostęp do historii zapytań albo wprowadzenie danych z akt sprawy do narzędzia zewnętrznego. Zgłoszenie organowi nadzorczemu następuje bez zbędnej zwłoki, nie później niż w 72 godziny. Źródło: procedura postępowania z naruszeniami.		
7. OCENA SKUTKÓW I DOKUMENTACJA					
24	**Z [T+W]**	Czy przeprowadzono DPIA (art. 35 RODO)?	Prawie zawsze wymagana w sektorze publicznym przy AI. Wykaz PUODO. Wytyczne EROD.		
25	**Z [T+W]**	Czy IOD został włączony w ocenę wdrożenia i czy zaktualizowano RCP?	IOD obligatoryjny w sektorze publicznym (art. 37 ust. 1 lit. a). RCP: art. 30.		
26	**P [T+W]**	Czy wyznaczono rolę odpowiedzialną za	Zarządzanie danymi zapewnia		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		zarządzanie danymi (data governance)?	jakość, spójność i dostępność danych. W sektorze publicznym – kluczowe dla rozliczalności.		
27	**Z [T+W]**	Czy zastosowano data protection by design i by default (art. 25)?	Ochrona danych w fazie projektowania. Minimalizacja, pseudonimizacja, domyślne ustawienia chroniące dane.		
8. GOTOWOŚĆ ORGANIZACYJNA (ARE WE READY?)					
28	**P [T+W]**	Czy organizacja posiada politykę AI, procedury reagowania na incydenty, zasoby kadrowe?	75,2% organizacji nie ma ekspertów. Należy ocenić, czy zasoby organizacji są wystarczające. Źródło: dokumentacja wewnętrzna.		
29	**P [T+W]**	Czy przeszkolono pracowników w zakresie bezpiecznego korzystania z AI?	Szkolenie użytkowników ogranicza ryzyko niewłaściwego użycia i jest elementem data protection by design.		
30	**P [T+W]**	Czy określono procedury reagowania na incydenty związane z jakością danych?	Procedury: wykrywanie błędów danych, eskalacja, korekcja i dokumentowanie. Istotne dla prawidłowości (art. 5 ust. 1 lit. d).		
31	**P/Z [T+W]**	Czy przewidziano okresowy przegląd	Ocena skutków podlega		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		systemu po wdrożeniu: monitorowanie jakości wyników, wykrywanie dryfu modelu oraz ponowną ocenę przy istotnej zmianie systemu, danych lub rodzaju spraw, w których jest wykorzystywany?	przeglądowi, gdy zmienia się ryzyko (art. 35 ust. 11 RODO). W jednostce publicznej zmianą taką jest również rozszerzenie systemu na nowy rodzaj spraw. Źródło: plan przeglądów, rejestr zmian, raporty monitorowania.		
32	**P [W]**	Czy dysponujemy dokumentacją techniczną systemu AI od dostawcy?	Źródło informacji do analizy ryzyka, DPIA, FRIA i bieżącej oceny. AI Act: karta modelu, instrukcja użycia.		
9. AI Act – SEKTOR PUBLICZNY					
33	**P/Z [T+W]**	Czy system może podlegać klasyfikacji jako system wysokiego ryzyka (art. 6, Załącznik III AI Act)?	Wiele zastosowań publicznych AI = wysokie ryzyko: administracja, pomoc społeczna, migracja, porządek publiczny. Jeśli tak – przejdź do Wersji Rozszerzonej		
34	**P/Z [W]**	Czy wykorzystanie systemu sztucznej inteligencji nie będzie praktyką zakazaną w rozumieniu art. 5 AI Act?	Art. 5 AI Act zawiera listę zakazanych praktyk w zakresie AI.		
35	**Z [W]**	Czy zapewniono wymogi przejrzystości z art. 50 AI Act: informowanie o interakcji z systemem AI oraz oznaczanie treści wygenerowanych lub	Art. 50 AI Act wiąże niezależnie od klasyfikacji systemu jako systemu wysokiego ryzyka.		

Nr	Typ	Pytanie (z oznaczeniem fazy)	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		zmodyfikowanych przez AI?	W jednostce publicznej dotyczy w szczególności chatbotów obsługujących mieszkańców oraz pism i materiałów przygotowanych z użyciem AI. Uzupełnia obowiązek informacyjny z art. 26 ust. 11 AI Act. Źródło: konfiguracja systemu, zasady redagowania pism.		

Legenda typów: P = pytanie projektowe (dostarcza wiedzę), Z = pytanie o zgodność z RODO (weryfikuje wymóg), P/Z = pytanie łączące oba aspekty. Organizacje wdrażające gotowe systemy (bez trenowania) mogą pominąć pytania [T].

WERSJA DLA MŚP: PRAKTYCZNA CHECKLISTA RODO DLA WDRAŻANIA AI

Poziom: wejściowy – lista samodzielna, niezależna od pozostałych

Podstawa: RODO

Dla kogo: małe i średnie przedsiębiorstwa korzystające z gotowych narzędzi AI, bez fazy trenowania

Cel: sprawdzić, czy korzystanie z narzędzia nie narusza przepisów o ochronie danych osobowych i co trzeba zrobić, żeby było zgodne z prawem

Moment: etap koncepcji i wyboru narzędzia, przed zakupem lub rozpoczęciem prac

Kiedy stosować: przy każdym zastosowaniu gotowego narzędzia AI, odrębnie dla każdego zastosowania. Lista nie wystarczy, gdy firma trenuje albo dotrenowuje model na własnych danych, gdy narzędzie ma wpływać na sytuację prawną ludzi (rekrutacja, ocena pracowników, scoring klientów), gdy w grę wchodzą dane wrażliwe lub dane dzieci albo gdy dane trafiają poza EOG – wtedy należy wypełnić Wersję Rozszerzoną albo skorzystać ze wsparcia specjalisty

Wynik: wiedza, czy z narzędzia można korzystać, oraz lista spraw do załatwienia przed użyciem go na danych klientów lub pracowników oraz decyzja czy konieczne jest przejście do Wersji Rozszerzonej

Podejście funkcjonalne: pytania oznaczone P ustalają, co robi narzędzie i na jakich danych działa, pytania oznaczone Z sprawdzają wymogi RODO, oznaczenie P/Z łączy jedno z drugim

Jak zbudowana jest ta lista

Lista zawiera dwa rodzaje pytań. Pytania oznaczone P służą ustaleniu, co robi narzędzie AI, na jakich danych działa i kto je dostarcza. Pytania oznaczone Z sprawdzają, czy spełnione są wymogi przepisów o ochronie danych osobowych. Oznaczenie P/Z to pytanie, które łączy jedno z drugim.

Kolejność nie jest przypadkowa. Bez ustalenia, jakie dane trafiają do narzędzia, nie da się ocenić, czy wolno je tam wprowadzać.

Lista zaczyna się od pytań o sens wdrożenia, tj. czy narzędzie rzeczywiście rozwiązuje problem firmy i czy korzyści przewyższają ryzyko. To pytania, które warto zadać przed podpisaniem umowy z dostawcą.

Do czego służy ta lista i jak ją wypełnić

Lista jest przeznaczona dla firmy, która chce korzystać z gotowego narzędzia AI np.asystenta tekstowego, narzędzia do obsługi klienta, wsparcia rekrutacji czy analizy dokumentów, i sprawdzić, czy nie narusza przy tym przepisów o ochronie danych osobowych. Nie wymaga wiedzy prawniczej, a jej wypełnienie zajmuje około 30 minut.

Lista nie zastępuje porady prawnej, analizy ryzyka ani oceny skutków dla ochrony danych. Pokazuje, co jest w porządku, a co wymaga sprawdzenia lub konsultacji przed dalszym korzystaniem z narzędzia. Wypełnienie listy nie jest równoznaczne z potwierdzeniem zgodności wdrożenia z RODO.

Jak wypełnić listę

1. Listę wypełnia właściciel firmy lub osoba odpowiedzialna za wdrożenie narzędzia AI, w razie potrzeby przy wsparciu osoby zajmującej się w firmie ochroną danych.
2. Listę wypełnia się osobno dla każdego zastosowania narzędzia. To samo narzędzie użyte do obsługi klientów i do rekrutacji wiąże się z innym ryzykiem.
3. Jeśli nie znasz odpowiedzi, sprawdź najpierw umowę z dostawcą narzędzia, jego regulamin i politykę prywatności. Tam znajduje się większość informacji o danych.
4. Puste pole w kolumnie odpowiedzi oznacza, że czegoś nie wiemy. To nie jest błąd, ale trzeba to zamknąć - wpisz w kolumnie „Działanie”, co trzeba sprawdzić, kto to zrobi i do kiedy. Jeśli pytanie nas nie dotyczy, zaznacz „WYJAŚNIJ” i napisz dlaczego; samo „WYJAŚNIJ” bez wyjaśnienia liczy się jak brak odpowiedzi.
5. Więcej niż trzy odpowiedzi „NIE” oznaczają, że przed dalszym korzystaniem z narzędzia należy skonsultować się ze specjalistą.
6. Wypełnioną listę należy zachować. W razie kontroli lub skargi jest ona dowodem, że firma sprawdziła te kwestie przed wdrożeniem narzędzia.
7. Lista jest wypełniona, gdy przy każdym pytaniu jest odpowiedź, a tam, gdzie trzeba coś zrobić, w kolumnie „Działanie” wpisano: co, kto i do kiedy.
8. Nie wszystko można zostawić na potem. Zanim narzędzie zostanie użyte na danych klientów lub pracowników, trzeba mieć umowę z dostawcą, ustaloną podstawę przetwarzania danych, informację dla osób, których dane trafiają do narzędzia, oraz wiedzę, gdzie te dane są przechowywane. Jeśli narzędzie wpływa na sytuację ludzi także weryfikację wyniku przez pracownika.

9. Pozostałe zadania np. szkolenie zespołu, zasady wprowadzania danych, postępowanie w razie błędu, możesz wykonywać równolegle, w terminach wpisanych w kolumnie „Działanie”.
10. Jeżeli narzędzie ma samo podejmować decyzje wobec ludzi, bez udziału pracownika, nie chodzi o zadanie do zaplanowania, trzeba zmienić sposób korzystania z narzędzia albo z niego zrezygnować.

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
1. CEL I SYSTEM AI					
1	**P**	Jaki problem / potrzebę ma rozwiązać AI, czy ten cel da się osiągnąć bez AI i jakie korzyści mierzalne są oczekiwane?	Uzasadnienie wdrożenia. Warunkuje ocenę proporcjonalności przetwarzania danych (RODO) i adekwatności rozwiązania.		
2	**P**	Co robi system AI i czy jego wyniki wpływają na sytuację osób fizycznych (klientów, pracowników)?	Jeśli tak – art. 22 RODO (decyzje automatyczne), obowiązki informacyjne, możliwa DPIA.		
3	**P**	Czy organizacja kupując gotowy system AI lub budując własny zna architekturę i konfigurację systemu?	Rozróżnienie build/deploy determinuje zakres odpowiedzialności. Znajomość architektury warunkuje data protection by design.		
2. DANE OSOBOWE					
4	**P/Z**	Czy system przetwarza dane osobowe np. klientów, pracowników lub kontrahentów?	Dane osobowe to wszelkie informacje o osobie. Dotyczy też inferencji AI o osobach. Źródło: instrukcja dostawcy.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
5	**P**	Czy wśród danych są dane wrażliwe (zdrowie, biometria) lub dane dzieci/osób wrażliwych?	Art. 9 i 8 RODO. Wymagają szczególnej podstawy prawnej i zwiększonej ochrony.		
6	**P**	Czy jakość i reprezentatywność danych jest wystarczająca, by uniknąć błędnych lub dyskryminujących wyników?	Jakość danych wpływa na prawidłowość przetwarzania (art. 5 ust. 1 lit. d) i ryzyko szkody dla osób.		
7	**P/Z**	Czy wiemy, kto w firmie odpowiada za dane wprowadzane do AI i czy mamy zasady określające, jakie dane wolno tam wprowadzać?	Podstawowe zasady zarządzania danymi (kto odpowiada, co wolno wprowadzać, gdzie dane trafiają) chronią przed przypadkowym ujawnieniem danych klientów lub pracowników w narzędziu AI. Źródło: regulamin wewnętrzny, instrukcja dla pracowników.		
3. PODSTAWA PRAWNA					
8	**Z**	Czy wiemy, na jakiej podstawie prawnej przetwarzamy dane w AI (art. 6 ust. 1)?	Zgoda, umowa, obowiązek prawny, uzasadniony interes. Jeśli nie wiemy – konsultacja z IOD/prawnikiem.		
4. DOSTAWCA AI					
9	**Z**	Czy mamy umowę powierzenia przetwarzania danych z dostawcą AI (art. 28)?	Obowiązkowa, gdy dostawca przetwarza dane w naszym imieniu. Dotyczy większości usług AI w chmurze.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
10	**P/Z**	Czy wiemy, gdzie dostawca przechowuje dane (kraj) i czy są przekazywane poza UE?	Art. 44–49 RODO. Źródło: DPA dostawcy, polityka prywatności, lokalizacja serwerów.		
11	**P**	Czy model AI jest open source czy zamknięty (closed source)? Czy dostawca udostępnia instrukcję użycia systemu?	Typ modelu wpływa na kontrolę nad danymi. AI Act wymaga dokumentacji od dostawców. Źródło: DPA, karta modelu.		
12	**P/Z**	Czy dane, które wprowadzamy do narzędzia, mogą być wykorzystywane przez dostawcę do trenowania jego modeli i czy można to wyłączyć?	Jeśli dostawca wykorzystuje wprowadzone dane do własnych celów, przestaje działać wyłącznie na nasze polecenie i w tym zakresie sam staje się administratorem (art. 28 ust. 10 RODO). Wiele narzędzi pozwala wyłączyć uczenie na danych klienta w ustawieniach konta lub w planie płatnym. Źródło: regulamin, umowa powierzenia, ustawienia konta.		
13	**Z**	Czy wiemy, jak długo dostawca przechowuje wprowadzone dane i historię rozmów oraz czy możemy je usunąć?	Art. 5 ust. 1 lit. e RODO: dane wolno przechowywać tylko tak długo, jak są potrzebne. W narzędziach AI dotyczy to także historii zapytań, załączonych plików i kopii w pamięci		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			kontekstowej. Źródło: regulamin, polityka prywatności, ustawienia konta.		
5. BEZPIECZEŃSTWO I NARUSZENIA					
14	**Z**	Czy wiemy, kto ma dostęp do konta i do danych wprowadzanych do narzędzia oraz co zrobić, jeśli dane wycieką albo trafią do niewłaściwej osoby?	Art. 32 RODO wymaga ograniczenia dostępu do osób, które go potrzebują (konta imienne, uwierzytelnianie dwuskładnikowe). Art. 33–34 RODO: naruszenie zgłasza się organowi nadzorczemu bez zbędnej zwłoki, nie później niż w 72 godziny – trzeba wiedzieć, kto w firmie za to odpowiada. Źródło: instrukcja dla pracowników, procedura postępowania z naruszeniami.		
6. OCHRONA OSÓB					
15	**Z**	Czy poinformowaliśmy osoby, że ich dane są przetwarzane z użyciem AI (art. 13–14)?	Klauzule informacyjne muszą zawierać wzmiankę o AI i zasadach działania systemu.		
16	**Z**	Czy osoby mogą zrealizować prawa RODO wobec wyników AI (dostęp, sprostowanie, usunięcie, sprzeciw)?	Art. 15–22. Jeśli AI podejmuje decyzje automatyczne – prawo do interwencji ludzkiej (art. 22).		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
17	**P/Z**	Czy wynik działania AI jest sprawdzany przez pracownika, zanim zostanie wykorzystany wobec osoby (np. przy rekrutacji, ocenie pracownika, odmowie usługi)?	Jeśli decyzja wobec człowieka zapada wyłącznie automatycznie i wywołuje skutki prawne albo w podobny sposób istotnie na niego wpływa, stosuje się art. 22 RODO. Sprawdzenie musi być rzeczywiste: pracownik powinien móc zmienić wynik na podstawie własnej oceny, a nie tylko go zatwierdzić. Źródło: opis procesu, instrukcja dla pracowników.		
7. DOKUMENTACJA I DATA PROTECTION BY DESIGN					
18	**Z**	Czy zaktualizowaliśmy RCP w związku z wdrażaniem AI (art. 30)?	Art. 30: aktualizacja rejestru.		
19	**Z**	Czy zastosowaliśmy data protection by design (art. 25) a jeśli tak to wyjaśnij jak?	Art. 25: minimalizacja, pseudonimizacja, kontrola dostępu przy wyborze AI.		
8. OCENA RYZYKA I GOTOWOŚĆ					
20	**Z**	Czy oceniliśmy, czy wymagana jest DPIA (art. 35)?	Wymagana przy: profilowaniu, dużej skali danych szczególnych, innowacyjnej technologii. Wykaz PUODO.		
21	**P/Z**	Czy włączyliśmy IOD i czy mamy wystarczające zasoby do	IOD konsultuje DPIA (art. 35 ust. 2 RODO). Należy ocenić, czy organizacja		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		zarządzania ryzykami AI?	dysponuje wystarczającymi zasobami ludzkimi i materialnymi. 75,2% organizacji nie ma ekspertów.		
22	**P**	Czy przeszkolono pracowników w zakresie bezpiecznego korzystania z AI i procedur jakości danych?	Szkolenie użytkowników ogranicza ryzyko niewłaściwego użycia. Procedury jakości danych zapewniają prawidłowość przetwarzania.		
23	**P**	Czy ktoś w firmie sprawdza okresowo, czy narzędzie nadal działa poprawnie i czy nie zmienił się sposób jego używania?	Odpowiedzi z tej listy dotyczą stanu na dziś. Dostawca może zmienić model, a pracownicy sposób korzystania z narzędzia. Warto ustalić, kto i jak często to sprawdza. Źródło: notatka z przeglądu, ustalenia wewnętrzne.		
9. AI Act					
24	**P**	Czy sprawdziliśmy, czy nasz system może być wysokiego ryzyka wg AI Act?	Jeśli dotyczy: rekrutacji, scoringu, edukacji, zdrowia – może być wysokiego ryzyka. Konsultacja ze specjalistą i jeśli odpowiedź jest pozytywna – przejdź do Wersji Rozszerzonej .		
25	**P/Z**	Czy wykorzystanie systemu sztucznej inteligencji nie będzie praktyką zakazaną w	Art. 5 AI Act zawiera listę zakazanych praktyk w zakresie AI.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		rozumieniu art. 5 AI Act?			
26	**P/Z**	Czy zapewniono wymogi transparentności AI Act (art. 50 – systemy GPAI, chatboty, deepfakes)?	Art. 50 AI Act ustanawia wymogi transparentności: oznaczanie treści generowanych przez AI, informowanie o interakcji z chatbotem, oznaczanie deepfakes.		

Legenda typów: P = pytanie projektowe (dostarcza wiedzę), Z = pytanie o zgodność z RODO (weryfikuje wymóg), P/Z = pytanie łączące oba aspekty. Organizacje wdrażające gotowe systemy (bez trenowania) mogą pominąć pytania [T].

WERSJA ROZSZERZONA: ROZBUDOWANA LISTA PYTAŃ – RODO + sygnalizacyjnie AI Act

Poziom: pogłębiony – drugi poziom dla każdej z trzech list wejściowych

Podstawa: RODO + sygnalizacyjnie AI Act

Dla kogo: organizacje każdej wielkości i z każdego sektora, po wypełnieniu listy wejściowej;

Cel: zebrać ustalenia potrzebne do przeprowadzenia analizy ryzyka, oceny skutków dla ochrony danych oraz potrzebne do wykazania zgodności z RODO i sygnalizacji w zakresie obowiązków wynikających z aktu w sprawie sztucznej inteligencji

Moment: etap koncepcji i wyboru narzędzia, przed zakupem lub rozpoczęciem prac

Kiedy stosować: niezależnie od tego, która lista z poziomu wejściowego została wypełniona, gdy zachodzi co najmniej jedna z sytuacji: organizacja buduje albo dotrenowuje model na własnych danych; wynik systemu wpływa na sytuację prawną osób; przetwarzane są dane szczególnych kategorii, dane dzieci lub dane o wyrokach; dane są przekazywane poza EOG; system może być systemem wysokiego ryzyka w rozumieniu AI Act.

Wynik: materiał wejściowy do analizy ryzyka i oceny skutków dla ochrony danych, w odpowiednich przypadkach także do oceny wpływu na prawa podstawowe (FRIA), oraz lista zadań warunkujących wdrożenie

Podejście funkcjonalne: pytania projektowe (P) dostarczają wiedzy o systemie, pytania o zgodność (Z) weryfikują wymogi RODO i AI Act, oznaczenie P/Z łączy oba aspekty

Założenia metodologiczne

Podejście funkcjonalne

Lista łączy dwa uzupełniające się rodzaje pytań. Pytania projektowe (P) identyfikują cel, charakter i kontekst wdrożenia AI, dostawcę, dane oraz gotowość organizacyjną – dostarczają wiedzy niezbędnej do oceny zgodności. Pytania o zgodność (Z) weryfikują spełnienie konkretnych wymogów RODO, w szczególności podstawę prawną, prawa osób, obowiązki informacyjne, ocenę skutków skutków dla ochrony danych, uwzględnianie ochrony danych w fazie projektowania i powierzenie przetwarzania. Oznaczenie P/Z wskazuje pytanie łączące oba aspekty.

Oba rodzaje pytań są ze sobą powiązane: pytanie projektowe „Jakie dane przetwarza system?” jest warunkiem wstępnym dla pytania o zgodność „Czy istnieje podstawa prawna przetwarzania tych danych?”. Struktura listy odzwierciedla ten związek.

Fazy cyklu życia systemu AI

Każde pytanie oznaczono symbolem fazy, w której ma ono znaczenie:

Symbol	Faza	Opis
[T]	**Trenowanie / Rozwój**	Opracowywanie i trenowanie modelu AI: dane treningowe, budowa modelu, testowanie.
[W]	**Wdrożenie / Użycie**	Wdrażanie gotowego systemu AI bez trenowania: konfiguracja, integracja, codzienne użycie.
[T+W]	**Obie fazy**	Kwestie wspólne: role RODO, rejestr czynności przetwarzania, IOD, data protection by design/default, DPIA, bezpieczeństwo.

Pytania wstępne o zasadność wdrożenia

Lista rozpoczyna się od pytań o zasadność wdrożenia systemu AI. Pozwalają one ustalić, czy korzyści z budowy lub wdrożenia systemu przewyższają związane z nim ryzyka. Dotyczą w szczególności: adekwatności AI do natury rozwiązywanego problemu, zdolności systemu do spełnienia potrzeb organizacji, sprawiedliwości wpływu systemu na różne grupy osób, jakości i reprezentatywności dostępnych danych, wystarczalności zasobów ludzkich i materialnych oraz ryzyka użycia systemu poza jego przeznaczeniem.

Pytania te pełnią funkcję komplementarną wobec pytań o zgodność – ustalają kontekst decyzyjny, z którego wynikają konsekwencje zarówno projektowe, jak i regulacyjne.

Przeznaczenie listy i sposób jej wypełnienia

Lista rozbudowana stanowi drugi krok po listach z poziomu wejściowego . Obejmuje wymogi RODO oraz sygnalizacyjnie wymogi AI Act. Jej celem jest zebranie materiału niezbędnego do przeprowadzenia analizy ryzyka, oceny skutków dla ochrony danych (DPIA), a w odpowiednich przypadkach również oceny wpływu na prawa podstawowe (FRIA). Od list z poziomu wejściowego różni się nie adresatem, lecz głębokością: te same zagadnienia rozstrzyga odrębnie dla fazy trenowania i fazy wdrożenia, osobno dla każdej podstawy prawnej, okresu retencji i kategorii danych.

Lista nie jest formularzem DPIA ani FRIA i ich nie zastępuje. Stanowi warstwę je poprzedzającą: porządkuje stan wiedzy organizacji o systemie, danych, dostawcy i rolach, bez którego obie oceny opierałyby się na założeniach. Lista nie zastępuje też analizy ryzyka. Jej wypełnienie stanowi natomiast materiał wejściowy do tych analiz. Wypełnienie listy nie

jest równoznaczne z potwierdzeniem zgodności wdrożenia z RODO. Organizacja, która wie już, że wdrożenie dotyczy danych osobowych, i dysponuje funkcją compliance, może rozpocząć od Wersji Rozszerzonej; wypełnianie Wersji 0 jest wtedy zbędne.

Instrukcja wypełniania

1. Listę wypełnia się odrębnie dla każdego procesu, w którym system AI ma być tworzony lub wykorzystywany, a przy systemach wielofunkcyjnych, odrębnie dla każdej funkcji o odmiennym profilu ryzyka.
2. Wypełnienie koordynuje właściciel biznesowy procesu przy udziale inspektor ochrony danych lub osoby odpowiedzialnej za compliance oraz osoby odpowiedzialnej za system informatyczny.
3. Przy systemach dotrenowywanych na danych organizacji pytania oznaczone [T] i [W] wypełnia się rozdzielnie dla każdej fazy. Podstawa prawna, zakres danych i okresy retencji mogą się w obu fazach różnić.
4. Jeżeli pytanie nie dotyczy danego przypadku, wybiera się „WYJAŚNIJ” i wpisuje powód w kolumnie „Działanie”. Odpowiedź „WYJAŚNIJ” bez wpisanego wyjaśnienia traktuje się jak brak odpowiedzi.
5. Pole odpowiedzi pozostawione puste oznacza lukę informacyjną, którą odnotowuje się w kolumnie „Działanie” wraz z osobą odpowiedzialną i terminem. Kolumna „Wyjaśnienie / Źródło” wskazuje, gdzie szukać odpowiedzi.
6. Sekcję 10 (sygnalizacja AI Act) należy skonsultować z osobą znającą przepisy AI Act. Pytania w tej sekcji mają charakter sygnalizacyjny i nie zastępują pełnej klasyfikacji systemu.
7. Wypełnioną listę zachowuje się jako element dokumentacji rozliczalności (art. 5 ust. 2 RODO) i punkt odniesienia przy weryfikacji wdrożenia oraz przy każdej istotnej zmianie systemu lub sposobu jego wykorzystania.
8. Wypełnianie listy kończy się, gdy przy każdym pytaniu jest odpowiedź, a tam, gdzie odpowiedź ujawnia potrzebę działania, w kolumnie „Działanie” wpisano zadanie, osobę odpowiedzialną i termin.
9. Zadania nie są równorzędne. Zadania dotyczące warunków legalności przetwarzania tj. w szczególności ustalenia podstawy prawnej odrębnie dla fazy trenowania i wdrożenia, przesłanki przetwarzania danych szczególnych kategorii, powierzenia przetwarzania, podstawy przekazania danych poza EOG, obowiązku informacyjnego, nadzoru człowieka nad decyzjami wywołującymi skutki prawne, oceny skutków dla

ochrony danych oraz przy systemie wysokiego ryzyka oceny wpływu na prawa podstawowe, wykonuje się przed rozpoczęciem przetwarzania. Decyzji o wdrożeniu nie podejmuje się, dopóki nie zostaną wykonane.

10. Zadania dotyczące środków organizacyjnych np. szkoleń i kompetencji w zakresie AI (art. 4 AI Act), polityki AI, procedur reagowania na incydenty, procedur zarządzania danymi, dokumentacji technicznej, mogą być realizowane równolegle z wdrożeniem, w terminach wskazanych w kolumnie „Działanie”, o ile ryzyko w tym czasie pozostaje kontrolowane.
11. Odrębną kategorię stanowią sytuacje, w których wdrożenie w zaplanowanym kształcie jest niedopuszczalne np. w pełni zautomatyzowana decyzja wywołująca skutki prawne podejmowana automatycznie bez mechanizmu interwencji człowieka, czynność zastrzeżona przepisami dla człowieka, praktyka zakazana w zakresie AI. Nie planuje się tu zadania z terminem. Konieczna jest zmiana konstrukcji procesu albo odstąpienie od wdrożenia.

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
1. CEL, ZASADNOŚĆ I KONTEKST WDROŻENIA					
1	**P [T+W]**	Jaki konkretny problem / potrzebę ma rozwiązać AI? Jaki jest cel biznesowy lub publiczny?	Zdefiniowanie celu jest warunkiem oceny zgodności celów przetwarzania (art. 5 ust. 1 lit. b RODO) i proporcjonalności wdrożenia. Źródło: dokumentacja projektowa.		
2	**P [T+W]**	Czy cel da się osiągnąć bez AI lub istniejącymi technologiami?	Należy ocenić, na ile istniejące technologie i procesy rozwiązują problem lepiej, biorąc pod uwagę profil ryzyka AI i potencjalne negatywne skutki. Istotne dla testu proporcjonalności (art. 5 ust. 1 lit. c RODO).		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
3	**P [T+W]**	Jakie korzyści mierzalne (czas, koszty, zyski, jakość usług) są oczekiwane?	Określenie oczekiwanych korzyści pozwala ocenić proporcjonalność wdrożenia i adekwatność zakresu przetwarzania danych osobowych (art. 5 ust. 1 lit. c RODO).		
4	**P [T+W]**	Jakie ryzyka reputacyjne, prawne, społeczne lub ryzyka dla człowieka mogą się pojawić?	Wstępna identyfikacja ryzyk pozwala określić potencjalny poziom ryzyka oraz np. czy wymagana będzie DPIA (art. 35 RODO). Bilans korzyści i ryzyk stanowi próg wejścia dla decyzji o wdrożeniu. Źródło: analiza wstępna, konsultacja z IOD.		
5	**P [W]**	Czy system spełni potrzeby i oczekiwania organizacji?	Należy ocenić, na ile planowany system spełni potrzeby i oczekiwania podmiotu wdrażającego. Niedopasowanie systemu zwiększa ryzyko przetwarzania nadmiarowego.		
6	**P [T+W]**	Jakie są konteksty użycia i ryzyka nadużycia systemu poza jego przeznaczeniem?	Należy zidentyfikować potencjalne konteksty użycia systemu i ryzyka jego nadużycia, w tym wdrożenia wykraczającego poza pierwotne przeznaczenie. Relewantne dla		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			oceny ryzyka (art. 35 RODO).		
2. CHARAKTER SYSTEMU AI I AUTONOMIA					
7	**P [T+W]**	Co robi system: generuje treści, klasyfikuje, przewiduje, rekomenduje, wspiera/podejmuje decyzje?	Określenie funkcji systemu jest niezbędne do oceny: profilowania (art. 4 pkt 4 RODO), zautomatyzowanego podejmowania decyzji (art. 22 RODO), zakresu DPIA i obowiązków informacyjnych.		
8	**P [W]**	Czy wynik AI jest wiążący, rekomendacyjny, czy informacyjny?	Charakter wyniku decyduje o zastosowaniu art. 22 RODO (decyzje automatyczne). Jeśli wynik jest wiążący lub wywiera istotny wpływ na osobę – wymagane są gwarancje z art. 22 ust. 3.		
9	**P [W]**	Czy system działa wyłącznie jako wsparcie człowieka, czy może prowadzić do decyzji o skutkach prawnych?	Kluczowe dla identyfikacji, czy dochodzi do decyzji zautomatyzowanej w rozumieniu art. 22 ust. 1 RODO i czy wymagany jest nadzór ludzki z art. 22 ust. 3.		
10	**P [W]**	Czy system podejmuje autonomiczne decyzje wobec osób fizycznych? Czy człowiek dokonuje rzeczywistej, merytorycznej weryfikacji wyniku AI – z realną możliwością jego zmiany w oparciu o własną ocenę – czy w praktyce	Odpowiedź determinuje zastosowanie art. 22 RODO i wymóg zapewnienia interwencji ludzkiej. Źródło: specyfikacja procesu, opis workflow.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		wynik AI przesądza o rozstrzygnięciu?			
11	**Z [W]**	Czy istnieją regulacje prawne wskazujące, że dana czynność powinna być prowadzona przez człowieka (np. wydawanie decyzji administracyjnych, diagnoza lekarska)?	Przy analizie zgodności może być wymagana ocena z uwzględnieniem regulacji sektorowych		
12	**P [W]**	Czy system będzie wykorzystywany wobec osób fizycznych (np. klientów, obywateli, pracowników, dzieci)?	Kluczowe dla identyfikacji osób, których dane dotyczą, i zakresu obowiązków informacyjnych (art. 13–14 RODO), a także zakresu analizy ryzykaŹródło: opis projektu, analiza interesariuszy.		
13	**P [T+W]**	Czy organizacja buduje własny system AI, czy wdraża gotowy? (build vs. deploy)	Rozróżnienie build vs. deploy determinuje zakres odpowiedzialności RODO: zasadniczo budujący odpowiada za dane treningowe, wdrażający – za dane wejściowe i sposób użycia.		
14	**P [T+W]**	Czy AI jest kupowana jako usługa, rozwijana wewnętrznie, czy oparta na modelach zewnętrznych? Jeżeli dostawca pełni rolę podmiotu przetwarzającego, należy zweryfikować, czy mimo to wskazuje jakieś własne cele przetwarzania danych (np. reuse data).	Forma pozyskania systemu determinuje zakres obowiązków: umowa powierzenia (art. 28 RODO), umowa licencyjna, współadministrowanie (art. 26 RODO), skutki z art. 28 ust. 10 RODO. Źródło: umowa z dostawcą.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
15	**P [W]**	Czy organizacja posiada wiedzę o architekturze systemu i instrukcjach dostawcy? Czy organizacja zapoznała się z instrukcją użycia i celami działania systemu, jeżeli dostawca przekazał taką instrukcję ?	Znajomość architektury i instrukcji dostawcy warunkuje skuteczność data protection by design (art. 25 RODO) oraz ocenę ryzyka (art. 32 RODO). Źródło: dokumentacja dostawcy.		
16	**P [W]**	Czy organizacja posiada wiedzę o prawidłowej konfiguracji systemu?	Poprawna konfiguracja systemu wpływa na zakres przetwarzania danych i poziom bezpieczeństwa (art. 25 i 32 RODO). Źródło: dokumentacja techniczna, instrukcja dostawcy.		
3. DANE OSOBOWE – IDENTYFIKACJA I ŹRÓDŁA					
17	**P/Z [T+W]**	Czy system AI przetwarza dane osobowe bezpośrednio (np. imiona, PESEL, dane kontaktowe, wizerunek)?	Należy uwzględnić m.in.: dane treningowe, dane wejściowe (input), dane wyjściowe (output) oraz wszelkie dane budujące kontekst (np. RAG). Art. 4 pkt 1 RODO definiuje dane osobowe szeroko. Pytanie fundamentalne – 41–58,5% organizacji nie identyfikuje tego związku (Raport Strategiczny). Źródło: dokumentacja systemu, analiza przepływu danych.		
18	**P/Z [W]**	Czy system generuje nowe dane o osobach	Dane wygenerowane przez AI o osobach (inferencje, profile,		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		(np. inferencje, profile, scoring, klasyfikacje)?	scoring) mogą stanowić dane osobowe w rozumieniu art. 4 pkt 1 RODO i profilowanie w rozumieniu art. 4 pkt 4.		
19	**P [T+W]**	Jakie kategorie danych: zwykłe, szczególne (art. 9), dane dzieci (art. 8), dane dot. wyroków (art. 10)?	Kategoria danych determinuje podstawę prawną, zakres DPIA i poziom wymaganej ochrony: art. 9 RODO (dane szczególne), art. 8 (dane dzieci), art. 10 (dane o wyrokach). Źródło: dokumentacja techniczna.		
20	**P [T+W]**	Czy wśród osób, których dane dotyczą, są osoby w szczególnie wrażliwej sytuacji (dzieci, pracownicy, osoby z niepełnosprawnościami)?	Przetwarzanie takich danych ma wpływ na ocenę podstaw prawnych, zwłaszcza podstawy z art. 6 ust. 1 lit. f tj. prawnie uzasadnionego interesu administratora, zasad przetwarzania, zwłaszcza zasady minimalizacji i ograniczenia celu, oraz na analizę ryzyka		
21	**P [T]**	Jakie są źródła danych treningowych: własne, zewnętrzne, publiczne, od dostawcy, syntetyczne, od podmiotów danych?	Źródło danych wpływa na: zgodność celów (art. 6 ust. 4 RODO), podstawę prawną, obowiązki informacyjne (art. 14 RODO – dane pozyskane pośrednio). Źródło: dokumentacja		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			dostawcy, model card.		
22	**P [W]**	Jakie są źródła danych wejściowych w fazie użycia: dane dostarczone do systemu AI przez użytkownika czy system AI sam pozyskuje z innego źródła?	Źródłem danych wejściowych może być bezpośrednio użytkownik lub system pobierający dane z zewnątrz – konieczne jest rozróżnienie dla oceny obowiązków informacyjnych i podstawy prawnej.		
23	**P [T+W]**	Jaki jest zakres danych na etapie trenowania, danych wejściowych i danych wyjściowych?	Zakres danych na każdym etapie musi odpowiadać zasadzie minimalizacji (art. 5 ust. 1 lit. c RODO). Dotyczy danych treningowych, wejściowych i wyjściowych.		
24	**P [T+W]**	Czy jakość i reprezentatywność danych jest wystarczająca?	Jakość i reprezentatywność danych warunkuje skuteczność i bezpieczeństwo systemu. Zasada prawidłowości danych (art. 5 ust. 1 lit. d RODO) wymaga unikania szkodliwych uprzedzeń.		
25	**P/Z [T+W]**	Czy organizacja ma wdrożone procedury data governance obejmujące dane wykorzystywane w systemie AI: klasyfikację danych, kontrolę jakości, zarządzanie dostępem, wersjonowanie zbiorów i dokumentowanie pochodzenia danych (data lineage)?	Wdrożone procedury zarządzania danymi warunkują faktyczną kontrolę nad danymi, a tym samym nad efektami działania systemu AI. Bez nich nie jest możliwe wykazanie zgodności z zasadami prawidłowości (art. 5		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			ust. 1 lit. d RODO), minimalizacji (lit. c), ograniczenia przechowywania (lit. e) ani rozliczalności (art. 5 ust. 2 RODO). Pytanie uzupełnia pytanie 45 dotyczące roli odpowiedzialnej za data governance. Źródło: polityka zarządzania danymi, procedury wewnętrzne, dokumentacja IT.		
4. PODSTAWA PRAWNA I CEL PRZETWARZANIA					
26	**Z [T]**	Jaka jest podstawa prawna przetwarzania danych treningowych (art. 6 ust. 1 RODO)?	Należy wskazać konkretną przesłankę z art. 6 ust. 1 RODO legalizującą przetwarzanie danych treningowych. Przesłanka może się różnić od tej dla fazy wdrożenia.		
27	**Z [W]**	Jaka jest podstawa prawna przetwarzania danych w fazie wdrożenia/użycia (art. 6 ust. 1)?	Faza wdrożenia i użycia może wymagać odrębnej podstawy prawnej z art. 6 ust. 1 RODO niż faza trenowania. Źródło: rejestr czynności przetwarzania, opinia IOD.		
28	**Z [T+W]**	Czy w przypadku zgody (lit. a) – może być ona dobrowolna przy obowiązkowym użyciu AI?	Motyw 42–43 RODO: zgoda musi być dobrowolna. W relacjach władczych (pracodawca–pracownik, organ–obywatel) dobrowolność zgody może być wątpliwa.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
29	**Z [T+W]**	Czy w przypadku prawnie uzasadnionego interesu (lit. f) – przeprowadzono test równowagi?	Art. 6 ust. 1 lit. f RODO wymaga przeprowadzenia testu równowagi pomiędzy prawnie uzasadnionym interesem administratora a interesem, prawami i wolnościami osób, których dane dotyczą.		
30	**Z [T]**	Czy przeprowadzono ocenę zgodności celów - jeśli pierwotne cele zbierania danych były inne niż rozwój systemu AI (compatibility test, art. 6 ust. 4)?	Art. 6 ust. 4 RODO: jeśli dane zebrano w innym celu niż AI, należy przeprowadzić test kompatybilności celów z uwzględnieniem kryteriów wskazanych w tym przepisie.		
31	**Z [T+W]**	Czy dla danych szczególnych kategorii istnieje odrębna przesłanka (art. 9 ust. 2)?	Przetwarzanie danych szczególnych kategorii wymaga odrębnej przesłanki z art. 9 ust. 2 RODO, niezależnie od podstawy z art. 6 ust. 1.		
5. ZASADY PRZETWARZANIA (art. 5 RODO)					
32	**Z [T]**	Czy zakres danych treningowych jest ograniczony do minimum niezbędnego (minimalizacja art. 5. ust. 1 lit. c))?	Zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO) wymaga, aby zakres danych treningowych był ograniczony do minimum niezbędnego do osiągnięcia celu.		
33	**Z [W]**	Czy dane wejściowe/wyjściowe w fazie użycia są ograniczone do niezbędnego minimum?	Zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO) dotyczy również danych wejściowych i		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			wyjściowych w fazie użycia systemu AI.		
34	**Z [T+W]**	Czy dane zarówno dane treningowe, walidacyjne i testowe, jak i wejściowe, są prawidłowe, aktualne i wolne od systemowych błędów (art. 5 ust. 1 lit. d)?	Zasada prawidłowości (art. 5 ust. 1 lit. d RODO) dotyczy wszystkich kategorii danych: treningowych, walidacyjnych, testowych i wejściowych. Nieprawidłowe dane mogą prowadzić do dyskryminacji.		
35	**Z [T]**	Czy określono okresy retencji danych treningowych?	Zasada ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO) wymaga określenia okresów retencji danych treningowych i ich usunięcia po ustaniu celu.		
36	**Z [W]**	Czy określono okresy retencji danych wejściowych i wyjściowych AI?	Zasada ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO) dotyczy również danych wejściowych i wyjściowych, w tym historii interakcji z systemem.		
37	**Z [T+W]**	Czy zastosowano data protection by design i by default (art. 25 RODO)? Jeśli tak wyjaśnij w jaki sposób.	Ochrona danych w fazie projektowania i domyślna ochrona danych (art. 25 RODO) wymagają wdrożenia odpowiednich środków technicznych i organizacyjnych już na etapie projektowania systemu.		
6. ROLE RODO, UMOWY I DOSTAWCY					

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
38	**P/Z [T+W]**	Kim jest organizacja: administratorem, współadministratorem, podmiotem przetwarzającym?	Prawidłowe ustalenie roli w rozumieniu RODO (art. 4 pkt 7–8, art. 26, art. 28) jest kluczowe dla określenia zakresu obowiązków i odpowiedzialności.		
39	**Z [W]**	Czy zawarto umowę powierzenia przetwarzania (art. 28 RODO) z dostawcą AI?	Obowiązkowa, gdy dostawca przetwarza dane w imieniu organizacji. Musi regulować: przedmiot, czas, charakter, cel, kategorie danych i osób. Należy zweryfikować czy dostawca zastrzega sobie prawo do wykorzystania danych we własnych celach ze skutkami z art. 28 ust. 10 RODO.		
40	**Z [W]**	Czy umowa powierzenia reguluje wszystkie elementy z art. 28 ust. 3 RODO: przedmiot, czas, charakter i cel przetwarzania, kategorie danych i osób, przetwarzanie wyłącznie na udokumentowane polecenie, poufność, bezpieczeństwo, warunki dalszego powierzenia, pomoc w realizacji praw osób i przy zgłaszaniu naruszeń, usunięcie lub zwrot danych po zakończeniu świadczenia usług oraz audyt i udostępnianie informacji niezbędnych do wykazania zgodności?	Art. 28 ust. 3 lit. a–h RODO określa obowiązkową treść umowy powierzenia. W praktyce najczęściej pomijane są: warunki dalszego powierzenia (lit. d w zw. z art. 28 ust. 2 i 4), pomoc w realizacji praw osób (lit. e), wsparcie przy naruszeniach (lit. f) oraz los danych po zakończeniu współpracy (lit. g) – istotny przy AI, gdzie dane mogą pozostać w modelu, w pamięci kontekstowej lub w kopiach zapasowych. Źródło: umowa		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			powierzenia, DPA dostawcy.		
41	**P [W]**	Czy dostawca ujawnia źródła danych treningowych i zapewnia dokumentację modelu?	Transparentność łańcucha dostawczego AI jest warunkiem rzetelnej oceny ryzyka i zapewnienia zgodności z RODO. Źródło: dokumentacja dostawcy, model card.		
42	**P [W]**	Czy model AI jest oparty na rozwiązaniu open source czy zamkniętym (closed source)?	Model open source vs. closed source wpływa na możliwość audytu, kontroli i oceny ryzyka przez organizację. Źródło: dokumentacja techniczna, licencja.		
43	**P [T+W]**	Czy w przypadku rozwoju wewnętrznego korzysta się z zasobów zewnętrznych (konsultanci, dane, infrastruktura)?	Korzystanie z zasobów zewnętrznych (konsultanci, podwykonawcy) przy budowie AI wymaga weryfikacji pod kątem art. 28 ust. 2 i 4 RODO (dalsze powierzenie).		
44	**P/Z [T+W]**	Czy wyznaczono właściciela biznesowego AI, osobę odpowiedzialną za compliance, inspektora ochrony danych?	Art. 24 RODO nakłada odpowiedzialność na administratora za zapewnienie zgodności. Art. 37–39 RODO określają wymogi dotyczące IOD. Źródło: struktura organizacyjna.		
45	**P [T+W]**	Czy wyznaczono rolę odpowiedzialną za zarządzanie danymi (data governance)?	Wyznaczenie roli odpowiedzialnej za zarządzanie danymi (data governance)		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			może wzmocnić zapewnienie zgodności i realizację i zasad z art. 5 RODO, w tym rozliczalności (art. 5 ust. 2).		
46	**P [T+W]**	Czy dostępne są wystarczające zasoby do zarządzania ryzykami AI?	Należy ocenić, czy dostępne zasoby ludzkie i materialne są wystarczające do spełnienia wymogów technicznych i zarządzania zidentyfikowanymi ryzykami.		
7. TRANSFER DANYCH I BEZPIECZEŃSTWO					
47	**P/Z [T+W]**	Czy dane są przekazywane poza EOG (serwery, chmura, API dostawcy)?	Art. 44 RODO ustanawia ogólną zasadę: przekazywanie danych do państw trzecich jest dopuszczalne wyłącznie przy zapewnieniu odpowiedniego poziomu ochrony.		
48	**Z [T+W]**	Jaka jest podstawa transferu: decyzja o adekwatności, SCC, BCR (art. 44–49)?	Należy wskazać konkretny mechanizm legalizacji transferu: decyzja o adekwatności (art. 45), standardowe klauzule umowne (art. 46 ust. 2 lit. c), wiążące reguły korporacyjne (art. 47).		
49	**Z [T+W]**	Czy przeprowadzono Transfer Impact Assessment (TIA)?	W następstwie wyroku Schrems II wymagane jest przeprowadzenie oceny skutków transferu (TIA) dla		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			transferów opartych na mechanizmach z art. 46 RODO w tym na standardowych klauzulach umownych. Źródło: dokumentacja dostawcy, TIA.		
50	**Z [T+W]**	Czy wdrożono środki bezpieczeństwa specyficzne dla AI (art. 32): kontrola dostępu, szyfrowanie, monitoring, ochrona przed atakami?	Art. 32 RODO wymaga wdrożenia środków bezpieczeństwa odpowiednich do zidentyfikowanych ryzyk. Należy uwzględnić aktualny stan wiedzy technicznej (state of the art).		
51	**Z [T+W]**	Czy określono procedury zgłaszania naruszeń związanych z AI (art. 33–34)?	Art. 33–34 RODO wymagają określenia procedur zgłaszania naruszeń ochrony danych organowi nadzorczemu (72 h) i osobom, których dane dotyczą.		
8. PRAWA OSÓB I TRANSPARENTNOŚĆ					
52	**Z [W]**	Czy zaktualizowano klauzule informacyjne o informację o AI (art. 13 ust. 2 lit. f / art. 14 ust. 2 lit. g)? Informacja powinna dotyczyć również użytkowników systemu, w interakcjach z którym mogą pojawić się wrażliwe treści (np. dane szczególnych kategorii w konwersacji z modelem).	Art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g RODO wymagają poinformowania o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, i istotnych informacjach o logice przetwarzania.		
53	**Z [W]**	Czy zapewniono realizację: prawa dostępu (art. 15),	Organizacja musi zapewnić techniczną i organizacyjną		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		sprostowania (art. 16), usunięcia (art. 17)?	możliwość realizacji praw: dostępu (art. 15), sprostowania (art. 16), usunięcia (art. 17) w kontekście systemu AI.		
54	**Z [W]**	Czy zapewniono: prawo do ograniczenia przetwarzania (art. 18) i przenoszenia danych (art. 20)?	Prawo do ograniczenia przetwarzania (art. 18 RODO) i przenoszenia danych (art. 20 RODO) mogą wymagać szczególnych rozwiązań technicznych w systemach AI.		
55	**Z [W]**	Czy zapewniono prawo do sprzeciwu (art. 21) wobec przetwarzania przez AI?	Prawo do sprzeciwu (art. 21 RODO) może dotyczyć przetwarzania opartego na prawnie uzasadnionym interesie (art. 6 ust. 1 lit. f) lub przetwarzania do celów marketingowych.		
56	**Z [T+W]**	Czy zapewniono prawo do niepodlegania decyzjom automatycznym (art. 22) i interwencji ludzkiej (art. 22 ust. 3)?	Art. 22 RODO wymaga zapewnienia: prawa do uzyskania interwencji ludzkiej, wyrażenia stanowiska i zakwestionowania decyzji. Wymaga to realnych, a nie formalnych mechanizmów.		
57	**P [W]**	Czy organizacja potrafi wyjaśnić działanie AI w sposób zrozumiały?	Art. 12 ust. 1 RODO wymaga, by informacje o przetwarzaniu były przekazywane		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			jasnym i prostym językiem. Dotyczy to również wyjaśniania działania AI.		
58	**P [T+W]**	Czy wpływ systemu będzie sprawiedliwy wobec różnych grup?	Należy ocenić, na ile skutki systemu będą sprawiedliwe wobec różnych grup osób, których dotyczą. Relewantne dla motywu 71 RODO (niedyskryminacja).		
9. OCENA SKUTKÓW I DOKUMENTACJA					
59	**Z [T+W]**	Czy spełnione są przesłanki z art. 35 ust. 1 lub 3 lub Wykazu PUODO? A jeśli tak to czy przeprowadzono DPIA (art. 35)?	Niezbędna jest analiza konieczności przeprowadzenia DPIA (analiza z perpektywy art. 35 RODO), W tym **kontekście** istotne będzie również ustalenie czy zidentyfikowano konkretne procesy, w których narzędzie będzie wykorzystywane? Nie wystarczy ogólna ocena narzędzia – konieczna jest ocena na poziomie poszczególnych procesów.		
60	**Z [T+W]**	Czy oceniono ryzyka specyficzne dla AI: błędne decyzje, dyskryminacja, uprzedzenia, naruszenie prywatności, ryzyka dla człowieka?	Ocena ryzyka powinna uwzględniać ryzyka specyficzne dla AI: błędne decyzje, dyskryminacja algorytmiczna, uprzedzenia w danych, brak wyjaśnialności, model drift.		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
61	**P [T+W]**	Czy ocena ryzyka uwzględnia specyfikę typu modelu AI, jego komponentów i zasobów?	Ocena ryzyka powinna uwzględniać specyfikę typu modelu AI, jego komponentów i zasobów zewnętrznych. Źródło: dokumentacja techniczna, audyt bezpieczeństwa.		
62	**Z [T+W]**	Czy zidentyfikowano procesy, w których system AI będzie tworzony lub wykorzystywany, i czy zaktualizowano rejestr czynności przetwarzania (art. 30 RODO)?	Inwentaryzacja procesów, w których AI jest tworzona lub wykorzystywana, jest warunkiem prawidłowej aktualizacji RCP. Rejestr powinien obejmować: cel przetwarzania w kontekście AI, kategorie danych i osób, odbiorców, okresy retencji oraz środki bezpieczeństwa. Źródło: dokumentacja projektowa, rejestr czynności przetwarzania.		
63	**P/Z [T+W]**	Czy przewidziano monitorowanie systemu po wdrożeniu: kontrolę jakości wyników, wykrywanie dryfu modelu, rejestrowanie zdarzeń oraz ponowną ocenę ryzyka i oceny skutków przy istotnej zmianie systemu, danych lub kontekstu użycia?	Ocena skutków podlega przeglądowi, gdy zmienia się ryzyko związane z przetwarzaniem (art. 35 ust. 11 RODO). W systemach AI zmianę taką powoduje aktualizacja modelu po stronie dostawcy, zmiana zakresu danych wejściowych albo nowe zastosowanie		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			systemu. Źródło: plan przeglądów, rejestr zmian, raporty monitorowania.		
10. SYGNALIZACJA DOTYCZĄCA AI ACT					
64	**P/Z [T+W]**	Czy system może być klasyfikowany jako system wysokiego ryzyka (art. 6, Załącznik I i III AI Act)?	Pytanie sygnalizacyjne: należy ocenić, czy system może być klasyfikowany jako system wysokiego ryzyka w rozumieniu art. 6 i Załącznika III AI Act.		
65	**P/Z [W]**	Czy wykorzystanie systemu sztucznej inteligencji nie będzie praktyką zakazaną w rozumieniu art. 5 AI Act?	Art. 5 AI Act zawiera listę zakazanych praktyk w zakresie AI.		
66	**P [T+W]**	Czy zidentyfikowana została rola organizacji z perspektywy AI Act w szczególności jako dostawcy lub podmiotu stosującego oraz obowiązki z takiej kwalifikacji wynikające?	Art. 3 pkt 4 i 8 AI Act definiują pojęcia dostawcy i podmiotu stosującego. Prawidłowa identyfikacja roli determinuje zakres obowiązków np. odnoszących się do dostawcy, w szczególności obowiązku zapewnienia zgodności systemów AI z wymogami dotyczącymi systemów wysokiego ryzyka, w tym w zakresie systemu zarządzania ryzykiem, odnoszących się do jakości danych i zarządzania nimi, dokumentacji i przejrzystości, czy		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
			odnoszących się do podmiotu stosującego, w tym wdrożenia środków zapewniających zgodność z instrucją obsługi, nadzoru, kompetencji, kontroli nad danymi wejściowymi, przeprowadzenia oceny skutktów systemów dla praw podstawowych (FRIA).		
67	**P/Z [W]**	Czy wymagana jest ocena wpływu na prawa podstawowe (FRIA) – art. 27 AI Act?	Art. 27 AI Act wymaga przeprowadzenia oceny wpływu na prawa podstawowe (FRIA) przez podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniki III do AI Act, z pewnymi wyjątkami,będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) i c).		
68	**P [W]**	Czy dostawca udostępnia dokumentację wymaganą przez AI Act	Art. 13 AI Act wymaga udostępnienia dokumentacji technicznej i instrukcji użycia. Dostępność		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		(karta modelu, instrukcja użycia)?	dokumentacji technicznej systemu AI od dostawcy jest warunkiem prawidłowej oceny ryzyka i zapewnienia zgodności z RODO i AI Act.		
69	**P [W]**	Czy podmiot stosujący zapoznał się z udostępnioną przez dostawcę dokumentacją wymaganą przez AI Act (karta modelu, instrukcja użycia)?	Art. 26 ust. 1 AI Act podmioty stosujące systemy AI wysokiego ryzyka wdrożyły odpowiednie środki techniczne i organizacyjne w celu zapewnienia, aby systemy takie były wykorzystywane zgodnie z dołączoną do nich instrukcją obsługi. .		
70	**Z [W]**	Czy zapewniono wymogi transparentności AI Act (art. 50 – systemy GPAI, chatboty, deepfakes)?	Art. 50 AI Act ustanawia wymogi transparentności: oznaczanie treści generowanych przez AI, informowanie o interakcji z chatbotem, oznaczanie deepfakes.		
11. GOTOWOŚĆ ORGANIZACYJNA (ARE WE READY?)					
71	**P [T+W]**	Czy organizacja posiada politykę AI i procedury reagowania na incydenty AI? Czy wdrożono mechanizmy wykrywania nieprawidłowości w działaniu systemu AI?	Organizacja powinna posiadać politykę AI oraz procedury reagowania na incydenty (art. 24 RODO). Źródło: polityka bezpieczeństwa, regulaminy wewnętrzne.		
72	**P [T+W]**	Czy planowane jest szkolenie pracowników w	Art. 4 AI Act (AI literacy) i art. 39		

Nr	Typ	Pytanie	Wyjaśnienie / Źródło	Odpowiedź: TAK / NIE / WYJAŚNIJ	Działanie: zadanie, osoba odpowiedzialna, termin
		zakresie bezpiecznego korzystania z AI? (AI LITERACY)	RODO (zadania IOD) wymagają zapewnienia odpowiedniego poziomu wiedzy pracowników korzystających z systemów AI.		
73	**P [T+W]**	Czy określono procedury reagowania na incydenty związane z jakością danych?	Należy określić procedury reagowania na incydenty związane z jakością danych (art. 5 ust. 1 lit. d RODO: zasada prawidłowości), w tym procedury korekty i ponownej walidacji.		

Legenda typów: P = pytanie projektowe (dostarcza wiedzę), Z = pytanie o zgodność z RODO (weryfikuje wymóg), P/Z = pytanie łączące oba aspekty. Organizacje wdrażające gotowe systemy (bez trenowania) mogą pominąć pytania [T].

Koordynator i redaktor opracowania:
prof. UŁ dr hab. Dominik Lubasz, członek Społecznego Zespołu Ekspertów przy Prezesie UODO

Opracowanie powstało przy wsparciu ekspertów Urzędu Ochrony Danych Osobowych
oraz pozostałych członków Społecznego Zespołu Ekspertów przy Prezesie UODO

URZĄD OCHRONY DANYCH OSOBOWYCH

SPOŁECZNY ZESPÓŁ EKSPERTÓW PRZY PUODO