

# DOBRE PRAKTYKI ANTYKORUPCYJNE W ORGANIZACJI

## OBSZAR:

### Informatyzacja (w szczególności zamówienia publiczne)

## WPROWADZENIE

Sektor informatyzacji (IT) odgrywa kluczową rolę w nowoczesnym świecie, przekształcając wiele aspektów codziennego życia, w tym także zadań administracji publicznej i sposobów prowadzenia biznesu. Jednakże wraz z dynamicznym rozwojem technologii i wzrostem inwestycji w informatyzację, sektor ten staje się coraz bardziej podatny na praktyki korupcyjne, zwłaszcza w kontekście zamówień publicznych. Zamówienia publiczne w sektorze IT często wiążą się z dużymi nakładami finansowymi, co sprawia, że są one atrakcyjnym celem dla działań korupcyjnych. Wzrost inwestycji w sektorze IT dla nieetycznych i nielegalnych praktyk.

## OBSZARY RYZYKA

1. **Nieprzejrzyste procedury przetargowe** - skomplikowane i niejasne procesy przetargowe, które mogą być manipulowane w celu faworyzowania konkretnych firm czy rozwiązań.

Skomplikowane procedury przetargowe często prowadzą do sytuacji, w której jedynie nieliczne firmy posiadają wystarczającą wiedzę i zasoby, by w pełni zrozumieć i spełnić wszystkie formalne wymogi. Może to prowadzić do ograniczenia konkurencji, gdyż małe i średnie przedsiębiorstwa są wykluczane z procesu już na samym początku.

Z drugiej strony, wielkie korporacje mogą wykorzystywać swoją dominującą pozycję i wpływy, aby wpływać na kształtowanie specyfikacji i wymagań przetargowych, tak by były one dostosowane do ich oferty.

2. **Specyfikacje techniczne** - dostosowane do konkretnego produktu czy dostawcy, zamiast opierania się na otwartych standardach.

Może to prowadzić do wielu negatywnych konsekwencji. Przede wszystkim, eliminuje to równą konkurencję, faworyzując określonego dostawcę kosztem innych. W rezultacie, instytucje publiczne mogą przepłacać za rozwiązania informatyczne, ponieważ brak konkurencji nie zachęca dostawców do oferowania bardziej konkurencyjnych cen czy innowacyjnych rozwiązań.

3. **Zawyżanie kosztów** - prezentowanie wyższych kosztów w celu uzyskania większych środków na realizację projektu.

Chodzi tutaj o sytuację, w której dostawcy technologiczni, konsultanci lub wykonawcy projektów celowo prezentują zaniżoną wartość rzeczywistej wartości usługi czy produktu w celu uzyskania wyższych marż zysku czy dodatkowych środków na realizację

projektu. Często zaczyna się od przedstawienia nieprecyzyjnych lub zawyżonych szacunków kosztów początkowych, które są następnie akceptowane przez nieświadomego klienta, w tym przypadku instytucje publiczną. W miarę postępu prac nad projektem pojawiają się dodatkowe koszty, które nie były uwzględnione w pierwotnym budżecie, co prowadzi do konieczności renowacji umowy i zwiększenia budżetu.

4. **Konflikt interesów** - udział osób lub firm mających ukryte powiązania z dostawcami w procesie podejmowania decyzji.

Konflikt interesów w obszarze informatyzacji, zwłaszcza w kontekście zamówień publicznych, może prowadzić do sytuacji, w której decyzje są podejmowane nie w oparciu o dobro publiczne, ale w celu uzyskania korzyści dla konkretnych osób lub firm. Kiedy osoby zaangażowane w proces przetargowy lub podejmowanie decyzji mają ukryte powiązania z dostawcami, ryzyko korupcyjne wzrasta, co może prowadzić do niestandardowych działań, które nie są w najlepszym interesie zamawiającego.

5. **Zmowy cenowe i nielegalne porozumienia** - w branży IT, zmowy cenowe i nielegalne porozumienia stanowią jedno z głównych zagrożeń.

Chodzi tutaj o sytuacje, gdy podmioty działające na rynku, zamiast konkurować, decydują się na współpracę w celu uzyskania nienaturalnie wysokich cen za swoje produkty lub usługi, czym poszkodowane zostaje instytucje publiczne. W praktyce takie działania mogą przyjmować różne formy. Może to być uzgodnienie między firmami cen, które zostaną zaproponowane w ofertach przetargowych, aby zapewnić wygraną określonemu dostawcy czy też przedstawianie ofert "słabszych", by dana firma miała pewność wygranej, zachowując jednocześnie pozory konkurencji.

6. **Nieodpowiednie relacje firm informatycznych z doradcami** - firmy IT mogą oferować "darmowe" konsultacje, mając nadzieję na wpływanie na decyzje urzędników.

Nieodpowiednie relacje między firmami informatycznymi a doradcami stanowią poważne ryzyko korupcyjne, zwłaszcza w kontekście zamówień publicznych w obszarze informatyzacji. W idealnym rozwiązaniu doradcy powinni działać niezależnie, dostarczając obiektywne rekomendacje bazujące na najlepszych dostępnych rozwiązaniach dla klienta. Niemniej jednak, gdy doradcy utrzymują zbyt bliskie relacje z określonymi dostawcami, ich rekomendacje mogą być nieodpowiednio kierowane przez interesy tych firm zamiast faktycznych potrzeb klienta.

7. **Manipulowanie specyfikacją zamówienia** - konstruowanie specyfikacji w porozumieniu z preferowanym dostawcą jest poważnym zagrożeniem. Zamówienia mogą być niekompletne, a późniejsze aneksy do umowy korzystne dla dostawcy.

Gdy instytucje publiczne lub firmy prywatne przygotowują specyfikację techniczną dla przyszłego projektu, oczekuje się, że będą one oparte na rzeczywistych potrzebach organizacji, a nie na możliwościach konkretnego dostawcy.

Jednak, kiedy specyfikacja jest ukierunkowana w taki sposób, że tylko jeden dostawca jest w stanie spełnić wszystkie jej wymagania, może to wskazywać na nieodpowiednie porozumienie między zamawiającym a dostawcą.

- 8. Długoterminowe konsekwencje wyborów technologicznych** - wybór określonego sprzętu czy oprogramowania może prowadzić do długoterminowych zobowiązań względem jednego dostawcy.

Decyzja o wyborze określonego sprzętu czy oprogramowania nie jest jedynie chwilowym zobowiązaniem finansowym; jest to także długofalowa inwestycja w relację z jednym dostawcą. Gdy instytucja publiczna zdecyduje się na konkretną technologię, zazwyczaj zobowiązuje się do korzystania z niej przez wiele lat. W rezultacie, jeśli początkowy wybór został dokonany na podstawie niejasnych kryteriów lub w wyniku potencjalnie korupcyjnych działań, organizacja może zostać związana z rozwiązaniem, które nie jest dla niej optymalne pod względem technicznym, finansowym czy operacyjnym.

## DOBRE PRAKTYKI (REKOMENDACJE)

- 1. Standaryzacja procedur przetargowych** - wprowadzenie jasnych, przejrzystych i standaryzowanych procedur dla wszystkich zamówień publicznych w sektorze IT.

Jasne i przejrzyste procedury przetargowe zapewniają, że wszyscy oferenci są traktowani równo, co promuje uczciwą konkurencję. Dzięki temu instytucje publiczne mogą skorzystać z najlepszych dostępnych rozwiązań technologicznych, jednocześnie osiągając korzystne warunki finansowe.

Standaryzacja procedur przetargowych pomaga unikać niejasności i luk w regulacjach, które mogą być wykorzystywane do manipulacji wynikami przetargów czy faworyzowania pewnych dostawców.

Dodatkowo, ujednoczenie procedur ułatwia kontrolę nad procesem przetargowym. Dzięki temu zewnętrzne organy nadzorcze, media czy obywatele mogą łatwiej śledzić i oceniać przebieg oraz wyniki przetargów. W środowisku, gdzie procedury są standaryzowane, każde odstępstwo od normy łatwiej dostrzec i zareagować na ewentualne nieprawidłowości.

Współczesne technologie informacyjne oferują także narzędzia, które mogą wspierać standaryzację i przejrzystość w procesach przetargowych. Elektroniczne systemy przetargowe, które umożliwiają składanie ofert online, śledzenie postępów przetargu w czasie rzeczywistym i dostęp do dokumentacji przetargowej, mogą znacząco przyczynić się do zwiększenia przejrzystości i uczciwości procesu.

Ujednoczenie procesów i zastosowanie nowoczesnych narzędzi technologicznych mogą pomóc w osiągnięciu tych celów, przynosząc korzyści zarówno instytucjom publicznym, jak i społeczeństwu jako całości.

- 2. Promowanie rozwiązań open-source** - zachęcanie do korzystania z otwartych standardów technologicznych, które umożliwiają większą konkurencję i innowacje.

Dzięki otwartym standardom technologicznym, zamawiający mają szansę skorzystać z szerokiej gamy dostępnych rozwiązań, które nie są obciążone ograniczeniami licencyjnymi czy koniecznością wiązania się z jednym dostawcą na długie lata.

Rozwiązania open-source zapewniają też pewność, że produkty i usługi, na które się decydujemy, były poddawane gruntownej ocenie przez społeczność ekspertów i programistów. Ta wieloaspektowa kontrola jakości zwiększa szanse na wysoką jakość i bezpieczeństwo oferowanych rozwiązań. Poza tym, korzystanie z technologii open-source umożliwia dostosowywanie ich do indywidualnych potrzeb i wymagań instytucji publicznych, zamiast polegania na gotowych, często niedopasowanych produktach.

Ponadto, otwarte standardy technologiczne sprzyjają innowacyjności. Dzięki temu, że wiele osób (ekspertów) pracuje nad jednym projektem, pojawia się mnóstwo kreatywnych rozwiązań, które mogą być wdrożone w praktyce. Dodatkowo, korzystając z otwartego oprogramowania, instytucje publiczne mogą znacząco obniżyć koszty związane z zakupem licencji czy długoterminowym wsparciem technicznym.

W środowisku, gdzie obawiamy się korupcji i nieprawidłowości, wykorzystanie technologii, której działanie jest jawne i dostępne do weryfikacji przez każdego, może być silnym argumentem przemawiającym za uczciwością i transparentnością działania instytucji publicznych.

**3. Wprowadzenie systemów audytu i monitoringu** - regularne przeglądy i audyty projektów w celu zapewnienia zgodności z ustalonymi standardami i przeciwdziałania nadużyciom.

Staje się także nieodłącznym elementem dbałości o transparentność i odpowiedzialność w realizacji projektów technologicznych. W świecie, gdzie technologia rozwija się w zawrotnym tempie, a skomplikowane projekty IT są na porządku dziennym, konieczność weryfikacji zgodności z ustalonymi standardami i wykrywanie potencjalnych nadużyć jest kluczowa.

Regularne przeglądy i audyty projektów nie są jedynie formalnością, ale skutecznym narzędziem do identyfikacji luk w systemie, potencjalnych zagrożeń oraz miejsc wymagających poprawy. Dzięki takim działaniom, możliwe jest nie tylko wczesne wykrywanie problemów, ale również zapobieganie powstawaniu poważniejszych kryzysów czy nadużyć w przyszłości. Wprowadzenie systematycznego audytu sprawia, że wszystkie strony zaangażowane w realizację projektu są świadome konieczności przestrzegania określonych standardów, co w naturalny sposób podnosi poziom odpowiedzialności i profesjonalizmu.

Działania stanowią nie tylko zabezpieczenie przed potencjalnymi nadużyciami, ale również sposobność do ciągłego doskonalenia się i podnoszenia jakości realizowanych projektów.

**4. Szkolenia i edukacja dla pracowników sektora publicznego** - regularne programy szkoleniowe dla pracowników odpowiedzialnych za przetargi i zamówienia publiczne w sektorze IT, koncentrujące się na etyce i rozpoznawaniu praktyk korupcyjnych.

W sektorze publicznym, gdzie odpowiedzialność za zarządzanie środkami publicznymi i zapewnienie transparentności w działaniach jest szczególnie istotna, umiejętność rozpoznawania potencjalnych praktyk korupcyjnych jest kluczowa. Regularne programy

szkoleniowe skoncentrowane na etyce oraz identyfikacji sytuacji mogących prowadzić do nadużyć, wprowadzają kulturę prewencji i świadomości ryzyka wśród pracowników.

Dzięki temu, pracownicy sektora publicznego stają się bardziej czujni i przygotowani na różnorodne sytuacje, które mogą napotkać podczas realizacji projektów IT. Szkolenia te nie tylko dostarczają wiedzy na temat aktualnych zagrożeń korupcyjnych, ale także uczą, jak w praktyce podejmować decyzje zgodne z etyką i prawem. Uczestnicy takich programów uczą się rozpoznawania sygnałów ostrzegawczych, które mogą wskazywać na nieprawidłowości, co z kolei prowadzi do wczesnego wykrywania i eliminowania potencjalnych zagrożeń.

Zaangażowanie w regularne szkolenia i edukację jest również dowodem na to, że instytucje publiczne traktują poważnie kwestie związane z korupcją i nadużyciami. Demonstruje to ich zaangażowanie w budowanie zaufania społecznego oraz w utrzymanie wysokich standardów w działalności publicznej.

- 5. Wprowadzenie klauzul Antykorupcyjnych** - klauzule antykorupcyjne w umowach to fundamentalny krok w kierunku eliminowania nieuczciwych praktyk. Powinny być one standardem we wszystkich umowach.

Klauzule antykorupcyjne stają się coraz bardziej popularne w wielu sektorach, a ich obecność w umowach w obszarze IT może odegrać kluczową rolę w tworzeniu kultury zero tolerancji dla wszelkich form korupcji.

Klauzule te stanowią jasne zobowiązanie obu stron umowy do przestrzegania najwyższych standardów etycznych oraz do działania w pełni zgodnie z prawem. Wprowadzając takie klauzule, instytucje publiczne wysyłają jednoznaczny sygnał do rynku, że oczekują od swoich partnerów biznesowych przestrzegania tych samych standardów, jakie same stosują. Klauzule antykorupcyjne mogą zawierać różnego rodzaju postanowienia, takie jak zobowiązanie do nieofiarowywania i nieprzyjmowania łapówek (także wszelkiego rodzaju upominków), przestrzeganie odpowiednich procedur wewnętrznych zapobiegających korupcji czy zobowiązanie do regularnych audytów wewnętrznych.

Jednocześnie, aby klauzule antykorupcyjne były skuteczne, niezbędne jest ich prawidłowe egzekwowanie. Zastosowanie klauzuli bez środków nadzoru i kontroli miałyby niewielką wartość. Dlatego też instytucje publiczne, zawierając takie klauzule w umowach, powinny również inwestować w mechanizmy monitorowania oraz egzekwowania ich przestrzegania. Obejmuje to regularne audyty, które pomagają zapewnić, że dostawcy rzeczywiście przestrzegają postanowień klauzul.

- 6. Wzmacnianie mechanizmów zgłaszania nieprawidłowości** - stworzenie systemów, które umożliwiają pracownikom, firmom oraz zainteresowanym stroną zgłaszanie podejrzeń o korupcję w sposób anonimowy.

Jednym z kluczowych wyzwań w walce z korupcją jest to, że wiele osób, które dostrzegają nieprawidłowości, obawia się represji czy konsekwencji związanych z ich zgłoszeniem. Dlatego stworzenie systemów, które gwarantują anonimowość i ochronę zgłaszających, jest tak ważne. Jeśli pracownicy, partnerzy biznesowi czy inne zainteresowane

strony mają pewność, że ich tożsamość pozostanie chroniona, znacznie chętniej zdecydują się podzielić swoimi obawami.

Stworzenie takiego systemu wymaga jednak więcej niż tylko zapewnienia anonimowości. Konieczne jest zapewnienie, że zgłoszone informacje są odpowiednio analizowane, a podejrzenia badane przez odpowiednie jednostki. Wprowadzenie systemu zgłaszania nieprawidłowości, który nie gwarantuje odpowiedniego działania w odpowiedzi na zgłoszenia, miałyby ograniczoną skuteczność. Dlatego kluczowe jest zapewnienie, że cały proces – od zgłoszenia, przez analizę, aż po podjęcie odpowiednich działań następczych – jest dobrze zorganizowany i efektywny.

Wprowadzając takie mechanizmy, instytucje publiczne nie tylko zwiększają swoją zdolność do wykrywania przypadków korupcji, ale także budują zaufanie wśród pracowników i partnerów biznesowych.