

From: "Szulc Adam - Spółka Akcyjna Szulc-Euphenics.com p SA " <adam.szulc@szulc-euphenics.com>
Sent: Monday, April 14, 2025 2:25 PM
To: halinow@halinow.pl
Cc: dwnik@nik.gov.pl
Subject: Petycja w trybie ustawy Ustawy z dnia 11 lipca 2014 r. o petycjach (tj. Dz.U. 2018 poz. 870) w związku z arty. 241 KPA

Kierownik Jednostki Samorządu Terytorialnego (dalej JST) - w rozumieniu art. 33 ust. 3 Ustawy o samorządzie gminnym (t.j. Dz. U. z 2024 r. poz. 1465, 1572.)

Aby zachować pełną jawność i transparentność - wnosimy o opublikowanie - niniejszej petycji w BIP - podstawę prawną, z której wynika obligatoryjność wzmiankowanej - podajemy in fine niniejszego pisma.

Komparycja Petycji:

Dane nadawcy (Osoba Prawna) - znajdują się poniżej oraz - w załączonym pliku sygnowanym podpisem elektronicznym, weryfikowanym kwalifikowanym certyfikatem - stosownie do dyspozycji Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2019 r. poz. 162, 1590) - Data dostarczenia - zgodna z dyspozycją art. 61 pkt. 2 Ustawy Kodeks Cywilny (t.j. Dz. U. z 2024 r. poz. 1061, 1237)

W niniejszym piśmie znajduje się kilka sekcji, które w mniemaniu autora podlegają różnym trybom ustawowym, a co za tym idzie powinny być dekretowane oddzielnie w zależności od aktu prawnego na który powołuje się autor pisma w danej sekcji.

Wg. piśmiennictwa i judykatury nie jest to łączenie trybów ale korzystanie z różnych środków prawnych. **Na urzędnikach ciąży obowiązek dokonania odrębnych dekretacji** - najlepiej w postaci elektronicznej - vide - J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania..., s. 668; por. także art. 12 ust. 1 komentowanej ustawy - dostępne w sieci Internet.

Naszą idee fixe jest poniższy akapit:

"Wszyscy mamy obowiązek patrzenia Decydentom na ręce - Wydają nasze podatki
! Składajmy Wnioski/Petycje i Skargi i zachęcajmy wszystkich do składania takich Wniosków.

W trybie art. 241 KPA - zmniejszajmy koszty publiczne i usprawniamy Administrację Publiczną"

Preambuła:

Z informacji uzyskanych przez Autora - spośród wielu kontroli NIK w innych Gminach -

w obszarze Cyberbezpieczeństwa - ani jedna kontrola nie zakończyła się opinią pozytywną/ambivalentną - a contrario - wszystkie kontrole w Gminach zakończyły się opinią negatywną.

Oczywiście wszyscy Wójtowie/Burmistrzowie - uważają, że „ich gmina jest wyjątkowa” - i często dopiero nasze wnioski/skargi i petycje - odsłaniają stan faktyczny.

Niemal zawsze - po wykonaniu rekonesansu - okazuje się, że sytuacja w danej gminie jest nawet gorsza, niż pisze o tym NIK w swoich protokołach pokontrolnych i podobna jak w przypadku Gmin, które uległy cyberatakowi o czym codziennie donoszą media relacjonując kolejne udane włamania hakerskie do Urzędów i przytaczając słowa kolejnych zdziwionych Wójtów/Burmistrzów i Prezydentów - sic!

Dochodzi to tego, że - pomimo wydatkowania olbrzymich środków podatników w obszarze cyberbezpieczeństwa, w Gminach permanentnie mają miejsce takie przypadki ad absurdum - jak w Gminie Rzęśnia - gdzie już dwukrotnie !!!! - sic! - wysłano przelewy na konto cyberoszustów

vide: 1) <https://tvn24.pl/lodz/rzasnia-gmina-stracila-5-mln-zlotych-jest-prokuratorskie-sledzwo-st5091169>

2) <https://twojepajeczno.pl/wiadomosci/powiat/gmina-oszukana-na-5-milionow-zlotych/>

Za pierwszym razem pół miliona złotych - wg. doniesień prasowych i odpowiedzi na nasze wnioski:

najpierw - „(...) Cyberprzestępcy zlecieli w systemie bankowości elektronicznej dwa duże przelewy i wyprowadzili w ten sposób 500 tysięcy złotych(...)”

Następnie - później za kadencji tego samego Wójta wysłano - 5 milionów złotych.

Z informacji udzielonych przez Prokuraturę w Wieluniu „(...) Skarbnik Urzędu Gminy w Rzęśni (...) przelał na konto oszustów zawrotną kwotę 5 milionów złotych.

Notabene skarbnik został odsunięty przez Wójta od pełnionej funkcji (...)” ... podatnikowi pieniędzy nikt nie zwróci...

Per Analogiam, a nawet gorzej w Gminie Konstancin-Jeziorna - oraz jak wynika z udzielanych na odpowiedzi na nasze wnioski - w setkach innych Gmin.

Wzmiankowany kazus Konstancina - opisany jest przez publikacje prasowe, do jednej z nich zamieszczamy link: - vide: „Z kasy gminy zniknęło 5 mln” pieniędzy Podatników Konstancin-Jeziorna. Prokuratura zajęła mieszkanie burmistrza. Wcześniej z miejskiej kasy zniknęło 5 milionów złotych <https://tvn24.pl/tvnwarszawa/najnowsze/konstancin-jeziorna-prokuratura-zajela-mieszkanie-burmistrza-wczesniej-z-miejskiej-kasy-zniknelo-5-milionow-zlotych-st6552624>

Zaistniały katastrofalny stan faktyczny wynikający z doniesień medialnych i uzyskiwanych przez nas odpowiedzi na nasze wnioski - potwierdzają również wszystkie kontrole NIK w Urzędach Gmin.

Badając w empirii stan faktyczny NIK pisze w protokołach pokontrolnych: „ (...) **Wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, nieświadomość i brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, które miało krytyczne luki – to główne nieprawidłowości wykryte w urzędach gmin (...)** . W

konsekwencji samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców.(...) „ vide Nr ewidencyjny: NIK I/23/001/LSZ - w całości z katastrofalnymi i druzgocącymi dla Decydenetów w Gminach wnioskami pokontrolnymi można zapoznać się w protokołach publikowanych na www.nik.gov.pl (data publikacji kwiecień 2024 - scilicet już po wydatkowaniu miliardów złotych w ramach programu „Cyfrowa Gmina”)

W mniemaniu Autora - Ministerstwo Cyfryzacji dokłada wszelkich starań i wyjątkowo profesjonalnie dba o dofinansowanie Gmin w obszarze Cyberbezpieczeństwa uruchamiając kolejne programy wspierające gminy.

Z kolei Gminy nie wydatkują przyznanych środków racjonalnie, wręcz przeciwnie - co wynika - expressis verbis - z odpowiedzi udzielnych nam od lat w trybie ustawy o dostępie do informacji publicznej - vide www.szulc-euphenics.com

W naszym mniemaniu środki Podatników w ramach programu „Cyfrowa Gmina” oraz „Cyberbezpieczny Samorząd” nie są wydatkowane w Gminach racjonalnie i oszczędnie - wręcz a contrario - olbrzymie środki są marnotrawione - ze względu na zmony cenowe oraz mentalność jaką prezentuje gros Decydenetów w Gminach.

Dziwi nas, że rzeczonymi kwestiami nie zainteresowali się jeszcze Radni Gmin - choć informacje publikowane na naszych stronach www.szulc-euphenics.com - powodują, że uzyskujemy coraz to więcej sygnałów o kolejnych - sytuacjach ad absurdum w Urzędach.

Do Gmin i jednostek administracji publicznej dostarczamy od 25 lat wnioski o udostępnienie informacji publicznej i staraliśmy się składać również wnioski optymalizacyjne i sanacyjne w trybie art. 241KPA*

Art. 241 KPA : “Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności.”

Osnowa Petycji:

W mniemaniu Petycjodawcy:

- naprawa skandalicznego stanu faktycznego opisanego w cytowanych protokołach NIK - **należy - bez żadnej wątpliwości - do wartości wymagających szczególnej ochrony w imię dobra wspólnego, mieszczących się w zakresie zadań i kompetencji adresata petycji** ponadto
- oszczędność w wydatkowaniu środków podatników i przeciwdziałanie nieuczciwym praktykom firm - polegającym na zmonie cenowej i zawyżaniu cen usług w ramach środków pochodzących z programów Cyfrowa Gmina i Cyberbezpieczny Samorząd - **należy - bez żadnej wątpliwości - do wartości wymagających szczególnej ochrony w imię dobra wspólnego, mieszczących się w zakresie zadań i kompetencji adresata petycji**

✓ Zatem w trybie Ustawy o petycjach (Dz.U.2018.870 tj. z dnia 2018.05.10) w związku z powołanym w argumentacji art. 241 KPA:

§1) Wnosimy rozważenie położenia większego nacisku na pozyskanie szkoleń i raportów traktujących o zaistniałych kazusach (incydentach związanych z cyberbezpieczeństwem) które pozwolą na unikanie błędów jakich należy unikać i jakie zazwyczaj kończą się defraudacją środków publicznych - ad exemplum przykład Gminy Rząśnia

vide: <https://tvn24.pl/lodz/rzasnia-gmina-stracila-5-mln-zlotych-jest-prokuratorskie-sledzwo-st5091169>

Autor niniejszego pisma zapytał w trybie ustawy o dostępie do informacji publicznej gros JST o incydenty tego typu i po otrzymaniu szczegółowych odpowiedzi opisujących jaki błąd ludzki doprowadził do cyberprzestępstwa - jest krańcowo zaniepokojony ilościami takich przypadków, krańcowym brakiem elementarnej wiedzy wśród Decydentów i olbrzymią ilością zmarnotrawionych pieniędzy Podatników.

Notabene - pieniądze - uzyskiwane w ten haniebny sposób przez cyberprzestępców najczęściej nie trafiają do obiegu polskiej gospodarki ale wędrują za granicę - często do Rosji lub do Białorusi - co jest dodatkowym argumentem na to że jest to najgorszy rodzaj defraudacji/sprzeniewieżenia i środków podatników - jakiego mogą się dopuścić urzędnicy.

Ministerstwo Cyfryzacji stara się wspomóc Gminy w obszarze cyberbezpieczeństwa uruchamiając kolejne dobrze przemyślane programy „Cyfrowa Gmina” „Cyberbezpieczny Samorząd”. Są do doskonałe, korzystne społecznie inicjatywy i dzięki temu większość Gmin ma możliwość zainwestowania w obszar cyberbezpieczeństwa kwoty od pół miliona do 1 miliona pln w interwale czasowym lat 2022-2025.

Jesteśmy pod wrażeniem doskonałej organicznej pracy jaką wykonuje Ministerstwo Cyfryzacji / MSWiA . Jednakże wysiłki te i olbrzymie kwoty grantów są najczęściej niweczone przez najprostsze ludzkie błędy Urzędników w Gminach. W trybie ustawy o dostępie do informacji publicznej uzyskujemy wiedzę o tych przypadkach o tych prostych szkolnych błędach a jest ich tyle, że doniesienia prasowe są jedynie „wierzchołkiem góry lodowej”

Taką wiedzą chcemy się podzielić z Decydentami i jesteśmy przekonani że jest to najbardziej przydatna forma szkolenia/raportu - działająca jak dobrze przetestowana szczepionka. A o dostęp do informacji publicznej pytamy już ponad 25 lat - vide www.szulc-euphenics.com

§2) W trybie Ustawy o petycjach (Dz.U.2018.870 tj. z dnia 2018.05.10) wnosimy o przeprowadzenie analizy zastosowania art 275 §2 Ustawy Prawo zamówień Publicznych

pod kątem zastosowania dyspozycji tego przepisu tak aby przeciwdziałać opisanym przez NIK i przez wnioskodawcę - deliktom prawnym, których efektem jest - w mniemaniu petycjodawcy - defraudacja i marnotrawstwo środków publicznych i stan faktyczny opisany w powyżej zacytowanym protokole NIK.

Odrębną sprawą są tzw. zminy cenowe. Mianowicie zawsze po wejściu w życie programu dofinansowania usług w JST ceny wzrastają i jest to oczywiste prawo popytu i podaży.

Natomiast w przypadku programu „Cyberb. Sam.” wzrost kwantyfikacji cenowych określanych przez firmy biorące udział w postępowaniach jest na tyle drastyczny, że wzrosty cen sięgają czasami nawet 250% (w przeciągu 4 lat) - sic! - I wynika to nie z naszej oceny - lecz z uzyskiwanych przez nas odpowiedzi.

Przypominamy, że w naszych wnioskach/petycjach i skargach podajemy konkretne przykłady w których Decydenci w Gminach:

po uzyskaniu środków z grantu:

- wydatkują zawyżone środki w postępowaniach (zmowa cenowa)
- marnotrawią środki - gdyż poziom bezpieczeństwa nie wzrasta - o dziwo skuteczne włamania najczęściej mają miejsce - w końcowej fazie konsumpcji grantu tak jakby cyberprzestępcy w ten sposób dodatkowo chcieli ośmieszyć polskie gminy (lub udowodnić w swoim przestępczym kręgu - że pokonali wyższą poprzeczkę.
- zbyt mało percepcji poświęcają na analizę błędów ludzkich - wynikających w empirii i kazuśw jakiegoż „badania naukowego oderwanego od rzeczywistości” - wynika to z udzielanych nam odpowiedzi w trybie ustawy o dostępie do informacji publicznej i tym chcemy się podzielić z Decydentami.

§3) W trybie Ustawy o petycjach (Dz.U.2018.870 tj. z dnia 2018.05.10) wnosimy o przyporządkowanie do klasy z wykazu akt załączonego schematu umowy.

Wg. petycjodawcy analiza dokumentów i raportów, o jakich piszemy w rzeczowej umowie może być skutecznym przyczynkiem do waliki z wyżej wskazanymi nieuczciwymi praktykami.

Wnosimy o archiwizację załącznika - w trybie §6 ust. 2 załącznika nr 1 do Rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z dnia 20 stycznia 2011 r.).

Uzasadnienie petycji:

Poniżej Komentarz fakultatywny wzmacniający argumentację - powtórzenia najbardziej rażących stwierdzeń dodane kilkakrotnie - dokonano w pełni świadomie aby expressis verbis uwypuklić stan faktyczny:

Autor pisma jako Osoba Prawna - jest podmiotem prawa handlowego - prowadzi działalność

gospodarczą oraz zażądał wykonania czynności (udzielenia odpowiedzi w trybie ustawy o dostępie do informacji publicznej) ze względu na uzasadniony interes publiczny pro publico bono oraz własny interes prawny - podobnie jak czyni to większość podmiotów w relacjach z każdym Organem (Urzędem)

W odróżnieniu jednak od większości innych podmiotów - zwracających się do Urzędu (Organu) i chcących zaspokoić - jedynie swój własny partykularny interes (Osób chcących jedynie załatwić swoją sprawę) - Autor - poza swoim partykularnym interesem związanym z prowadzeniem działalności gospodarczej oraz poddawaniem się zasadom uczciwej konkurencji - realizuje również uzasadniony interes społeczny pro publico bono - w ramach zawodowego charakteru działalności i know-how kompletowanego w ciągu 25 lat pracy dla Jednostek Administracji Publicznej - vide: www.szulc-euphenics.com

W mniemaniu Autora/Wnioskodawcy* - Ustawodawca - dedykował do tego celu art 241 Ustawy KPA*

Art. 241 KPA* : "Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności."

W mniemaniu Autora - Ministerstwo Cyfryzacji i MSWIA dokładają wszelkich starań i wyjątkowo profesjonalnie dbają o dofinansowanie Gmin w obszarze Cyberbezpieczeństwa uruchamiając kolejne programy wspierające gminy.

Z kolei Gminy nie wydrukują przyznanych środków racjonalnie, wręcz przeciwnie - co wynika - expressis verbis - z odpowiedzi udzielnych nam od lat w trybie ustawy o dostępie do informacji publicznej - vide www.szulc-euphenics.com

W naszym mniemaniu środki Podatników w ramach programu „Cyfrowa Gmina” oraz „Cyberbezpieczny Samorząd” nie są wydatkowane w Gminach racjonalnie i oszczędnie - wręcz a contrario - olbrzymie środki są marnotrawione - ze względu na zmywy cenowe oraz mentalność jaką prezentuje gros Decydentów w Gminach.

Urzędnicy w Gminach - w dużym uproszczeniu - wychodzą często z założenia: „...skoro otrzymaliśmy środki z Ministerstwa i niemalże 'spadły nam z nieba' - to trzeba je szybko wydać ...”

Co więcej nie dość, że ceny usług są zawyżane - i ma to w mniemaniu Autora/Wnioskodawcy - w JST wręcz powszechny charakter korupcyjny - to dodatkowo jeszcze zakupywane w ramach zawyżonych cen - usługi nie są zgodne ze stanem prawnym.

Rzeczoną niezgodność usług w tym obszarze expressis verbis sygnalizuje we wszystkich kontrolach Najwyższa Izba Kontroli.

W szczególności NIK w ramach prawie wszystkich kontroli piętnuje niezgodność usług z obowiązującą normą PN 27001.

Jak wynika z odpowiedzi uzyskiwanych w trybie ustawy o dostępie do informacji publicznej - zмова cenowa ma miejsce w wielu obszarach, ale w obszarze cyberbezpieczeństwa - par excellence - w najbardziej rażącej i beczelnej postaci.

Przed złożeniem niniejszego pisma* Wnioskodawca dokonał analizy deliktów prawnych związanych ze zmovą cenową w Jednostkach Administracji Publicznej o podobnym mechanizmie i w ramach zaistniałych okoliczności - per analogiam:

1) <https://samorząd.pap.pl/kategoria/prawo/winny-korupcji-bprezydent-tarnowa-skazany-na-3-lata-za-korupcje>

2) <https://www.radiokrakow.pl/aktualnosci/tarnow/po-pieciu-latach-procesu-zapadl-ostatni-wyrok-ws-zmowy-przetargowej-przy-budowie-lacznika-a4-w-tarnowie/>

Podobna zмова cenowa - w mniemaniu Autora - istnieje w obszarze usług cyberbezpieczeństwa. Mamy nadzieję, że w jakimś minimalnym stopniu przyczyniliśmy się do wyrzucia i zdemaskowania - tych korupcjogennych mechanizmów (zmowy cenowej), gdyż permanentnie składaliśmy zapytania w trybie ustawy o dostępie do informacji publicznej w Mieście Tarnów (tak jak i w innych gminach) już od wielu lat i udostępnialiśmy niepokojące odpowiedzi do wiadomości publicznej - in fine: (poniżej jedna z takich niepokojących odpowiedzi)

Ponownie sygnalizujemy, że mamy wrażenie iż w obszarze cyberbezpieczeństwa istnieje zмова cenowa - o charakterze bardzo zbliżonym.

W naszym mniemaniu potwierdzają to również protokoły Najwyższej Izby Kontroli - ad exemplum: Nr ewidencyjny: I/23/001/LSZ vide: <https://www.nik.gov.pl/najnowsze-informacje-o-wynikach-kontroli/zachodniopomorskie-gminy-cyberzagrozenia.html> oraz dyspozycji Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222), Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 22 maja 2024 r.) oraz prawa UE, a także odnośnych Polskich Norm w tym PN 27001.

Podsumowanie

Podkreślamy ponownie z naciskiem, że w ostatnim czasie w Gminach - z pieniędzy Podatników zostały wydatkowane olbrzymie kwoty związane z obszarem cyberbezpieczeństwa.

Planowane jest wydatkowanie w najbliższych 2 latach - w gminach (JST) - z pieniędzy Podatników kolejnych ok. 2 mld złotych - w ramach tzw. programu „Cyberbezpieczny Samorząd”

Tym samym urzędnicy w Gminach - dyskredytują i niszczą ciężką pracę wykonaną przez Ministerstwo Cyfryzacji - przepłacając za złej jakości zawyżone cenowo usługi w pseudo firmach - co stwarza obraz korupcjogenny i gwałcący wszelkie zasady uczciwej konkurencji.

To ogólnie znana i tolerowana w Urzędach Gmin - Tajemnica poliszynela - i byłoby to groteskowe i niewarte percepcji - gdyby nie to, że płacą za to Podatnicy - uderza to również w Podmioty zmuszone prowadzące uczciwą działalność gospodarczą.

Z odpowiedzi udzielonych nam w trybie ustawy o dostępie do informacji publicznej, a szczególnie w rozmowach telefonicznych - sami Decydenci permanentnie przyznają, że po wejściu w życie programów typu „Cyfrowa Gmina” oraz „Cyberbezpieczny Samorząd” ceny usług na rynku „ad hoc magicznie wzrosły” od 100% do 300 % (patrz mechanizmy powołane w obszarze usług budowlanych w przypadku Miasta Tarnowa) .

Z uzyskiwanych przez nas odpowiedzi wynika, że czasami nawet wzrosły powyżej 300% - sic !

Wszyscy w gminach wiedzą i przyznają, że status quo został zachwiany, a tworzone quasi audyty i raporty to często dokumenty, w których na setkach pozbawionych wartościowego kontentu stronach (rzekomych audytach i quasi raportach) - zmianie ulegają jedynie nazwy/nomenklatury Gmin/Jednostek Administracji Publicznej.

Potwierdzają to wszyscy urzędnicy w rozmowach telefonicznych - sic! - ceny wzrosły o kilkaset procent.

Dodatkowo - po wydatkowaniu miliardów środków publicznych w obszarze cyberbezpieczeństwa - wszystkie kontrole NIK - potwierdzają katastrofalny stan zastany w Urzędach Gmin przez Kontrolerów.

Wszystko w kontekście przepisów dot. sanacji związanej z wydatkowaniem środków podatników, ulepszeniem organizacji, wzmocnieniem praworządności, usprawnieniem pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności. - którą każdy podmiot ma prawo i obowiązek - prowadzić - w ramach zasad uczciwej konkurencji i równego traktowania - bez dyskryminacji, szykanowania i narażania na jakikolwiek uszczerbek ze strony Urzędników (art. 225KPA) Oczywiście, żaden Ustawodawca na świecie - nie stopniuje ważności Interesanta: Mieszkaniec, Bezrobotny, Przedsiębiorca, Radny, etc ... Każdy Obywatel UE i każdy Podmiot ma możliwość przekazania swoich uwag w tym trybie.

Podsumowanie końcowe:

Autor pracuje z gminami już ponad 25 lat i uważa, że w niektórych gminach, które wykonały organiczną pracę związaną z Cyberbezpieczeństwem sytuacja nie jest aż tak tragiczna jak obrazuje to NIK ale są to gminy nieliczne, którym pomogliśmy wdrożyć procedurę sanacyjną.

W mniemaniu Autora - Jeśli Gmina współpracuje z doświadczonymi podmiotami, z którymi koncentruje się w pierwszym rzędzie na właściwym określeniu stanu początkowego dostosowanego do specyfiki gminy, wtedy na zasadzie zarządzania realnym ryzykiem - wszystkie kolejne działania wykonywane są w sposób racjonalny, a pieniądze podatników są wydatkowane oszczędnie i powyżej zawarte tezy i zarzuty formułowane przez NIK - są mało prawdopodobne.

Jak pisaliśmy już wielokrotnie

W tej sprawie wysłaliśmy wniosek do Adresata w trybie Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) przywołując jednocześnie art 241 KPA*

Oczywiście ABY NASZA PETYCJA NIE BYŁA W ŻADNYM RAZIE ŁĄCZONA Z PÓŹNIEJSZYM trybem zamówienia nie musimy dodawać, że jesteśmy przekonani, iż postępowanie będzie prowadzone z uwzględnieniem zasad uczciwej konkurencji - i o wyborze oferenta będą decydować jedynie ustalone przez decydentów kryteria związane inter alia z aktualnym stanem prawnym, bezpieczeństwem oraz racjonalnym wydatkowaniem środków publicznych.

Aby zachować pełną jawność i transparentność działań - wnosimy o opublikowanie treści petycji na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go

obsługującego (Adresata) - na podstawie art. 8 ust. 1 ww. Ustawy o petycjach - co jest jednoznaczne z wyrażeniem zgody na publikację wszystkich danych. Chcemy działać w pełni jawnie i transparentnie.

Petycja odrębna - dla ułatwienia i zmniejszenia biurokracji - została dołączona do niniejszego wniosku - vide - J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania..., s. 668; por. także art. 12 ust. 1 komentowanej ustawy - dostępne w sieci Internet. - co jak wynika z cytowanego piśmiennictwa nie jest łączeniem trybów.

III. WNIOSEK odrębny - w tym samym piśmie kierowany do Organu w trybie KPA:

III.1) Na mocy art. 253 Ustawy Kodeks postępowania adm. (t.j. Dz. U. z 2024 r. poz. 572.) (dalej KPA) wnosimy o wyznaczenie terminu, o którym mowa w powołanej dyspozycji - scilicet: w dzień przyjęć interesantów w sprawach skarg i wniosków - przez Organ o którym mowa w §1 wzmiankowanego przepisu.

Poddamy się w pełni: trybowi i terminom oraz sposobom zaspokojenia tego przepisu - określonymi w regulaminie Organu - jednakże z naszej strony (jeśli to możliwe) aby nie absorbować zbytnio czasu Decydentów - pozwalamy sobie zaproponować tryb telefoniczny - określony w art. 14 §2 KPA.

Jeśli tryb telefoniczny (ze względu na konieczność przygotowania oraz sygnowania protokołu) - będzie niewygodny dla Organu - zaakceptujemy wszelkie inne rozwiązania.

- Prosimy o wyznaczenie konkretnej daty i godziny w ramach interwału określonego w art 253 §2 KPA.

PS: Tematem rozmowy w kontekście wyżej powołanych podstaw prawnych - będą sprawy określone w art 241 KPA - w przedmiocie inter alia: sugestii ewentualnego usprawnienia obszaru wypełniania zadań publicznych - zgodnie z treścią wyżej zawartego wniosku i petycji.

Duża skala nieprawidłowości i deliktów jakie dostrzega autor w JST - wynika nie tylko z udzielanych mu odpowiedzi - w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902, etc, etc) na przestrzeni ostatnich 25 lat, ale również wynika z dostępnych i przywołanych przez autora protokołów NIK oraz doniesień medialnych. Wierchołek tej „góry lodowej” staramy się również opisać na naszym portalu - vide szulc-euphenics.com

§3) Wnosimy o zwrotne potwierdzenie otrzymania niniejszego wniosku w trybie §7 Rozporządzenia Prezesa Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania s. i wniosków. (Dz. U. z dnia 22 stycznia 2002 r. Nr 5, poz. 46) -

na adres poczty elektronicznej: jawnosc-transparentnosc@szulc-euphenics.com

§4) Wnosimy o to, aby odpowiedź w przedmiocie powyższych pytań i petycji złożonych na mocy art. 63 Konstytucji RP - w związku z art. 241 KPA, została udzielona - zwrotnie na adres poczty elektronicznej jawnosc-transparentnosc@szulc-euphenics.com

§5) Wniosek został sygnowany bezpiecznym, kwalifikowanym podpisem elektronicznym - stosownie do wytycznych Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2016.1579 dnia 2016.09.29)

Sygnowano elektronicznie ipso iure ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2016.1579 dnia 2016.09.29)

Osoba Prawna:

Szulc-Euphenics.com p. Spółka Akcyjna

Prezes Zarządu - Adam Szulc

ul. Poligonowa 1

04-051 Warszawa

tel. 608-318-418

nr KRS: 0001 007 117

www.gmina.pl

Szulc-Euphenics.com p. Spółka Akcyjna z siedzibą w Warszawie 04-051, ul. Poligonowa 1, wpisaną pod numerem 000100 711 7 do Rejestru Przedsiębiorców KRS prowadzonego przez Sąd Rejonowy dla M. St. Warszawy w Warszawie, XIII Wydział Gospodarczy KRS, zarejestrowaną jako podatnik VAT, posiadającą numer identyfikacji podatkowej NIP: 113 308 02 05, tel. 608-318-418 fax: 22 673-62-12, reprezentowaną przez: Prezesa Zarządu – Adama Szulc - zwaną w treści umowy Usługodawcą lub Wykonawcą
Konto bankowe : 33 1600 1462 1730 2681 7000 0001

ZAMÓWIENIE – Niniejszy dokument – jest oświadczeniem woli zawarcia umowy i zaczyna obowiązywać strony w momencie przyjęcia go i podpisania przez Zamawiającego - ipso iure art. 66 § 1 Kodeksu Cywilnego. Do spraw nieuregulowanych w niniejszym zleceniu, stosuje się dyspozycje ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (t.j. Dz. U. z 2020 r. poz. 1740)

Usługodawca: Szulc-Euphenics.com p. Spółka Akcyjna o danych jw.

Zamawiający:
reprezentowana przez

Przedmiot Zamówienia:

§1) W ramach niniejszego zlecenia Usługodawca opracuje i **wykona raport „dobrych praktyk” dla Kierownictwa Jednostki Samorządu Terytorialnego w zakresie empirycznych aspektów związanych z zarządzaniem ryzykiem i szacowaniem ryzyka w obszarze cyberbezpieczeństwa Jednostki Administracji Publicznej.**

§1a) Tezy zawarte w przedmiotowym raporcie wynikają z 25 lat doświadczenia – jakim dysponuje Usługodawca – w ramach badania kasusów związanych ze stanem faktycznym i problematyką związaną z cyberbezpieczeństwem w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. 2022 poz. 902)

§2) Rzeczona analiza dot. cyberbezpieczeństwa zostanie dokonana w kontekście zaistniałych kasusów w Jednostkach Samorządu Terytorialnego (dalej JST) związanych z zaistniałymi incydentami (ad exemplum: Konstancin J. Rzaśnia, Nowiny, etc) w wyniku, których powstały delikty przeciwko bezpieczeństwu danych, dyspozycjom Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 22 maja 2024 r.), dyspozycjom ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222) oraz Polskiej Normy PN-ISO/IEC 27001. W ramach powołanej analizy bierze się również pod uwagę wnioski wynikające z rekonesansu dokonanego w obszarze odnośnych protokołów pokontrolnych NIK dot. kontrolowanych Jednostek o podobnym jak Zamawiający potencjale - w skali Kraju.

§2a) W założeniach – tezy zawarte w raporcie mają za zadanie wspomóc Decydentów w walce z najczęściej występującymi błędami ludzkimi oraz w warstwie formalnej - ze zmwami cenowymi w tym obszarze sięgającymi nawet 300%. Przedmiotowe zmwoty cenowe mają miejsce w obszarze postępowań związanych z cyberbezpieczeństwem i uzyskiwanych środków z grantów w tym obszarze. (Kwantyfikacje 300% przypadków „zmowy cenowej” - wynikają z realnych odpowiedzi na piśmie uzyskiwanych w trybie ustawy o dostępie do informacji publicznej z JST.) **W założeniach – już samo publicity jakim dysponuje Usługodawca w związku ze składaniem skarg/wniosków/petycji oraz nawiązanie stosunku gospodarczego z Zamawiającym – ma działać – w pewnym stopniu - odstraszająco na podmioty – stosujące nieuczciwe praktyki cenowe (zmowy cenowe)**

§3) W ramach niniejszego zlecenia – bez dodatkowych opłat - Usługodawca pozostaje dyspozycyjny w przedmiocie konsultacji telefonicznych - w kontekście Systemu Zarządzania Bezpieczeństwem Inf. (SZBI) oraz metodyki skorzystania z możliwości odmowy udzielania informacji publicznej w obszarze spraw związanych z cyberbezpieczeństwem w ramach ograniczeń określonych w art. 5 ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902)

§4) W przedmiotowym raporcie Usługodawca zamieści wnioski wynikające z analizy protokołów pokontrolnych NIK w obszarze cyberbezpieczeństwa w JST. Wzmiankowane wnioski wynikać będą również z udzielonych odpowiedzi jakie usługodawca uzyskał wnioskując permanentnie do Jednostek Administracji Publicznej w trybie Ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902, etc, etc) Takie ujęcie powoduje, że dokonana analiza zawiera wnioski optymalizacyjne i sanacyjne wynikające nie tylko z aktualnego stanu prawnego (de leg lata) ale również z uwarunkowań praktycznych wynikających de facto z metodologii rozwiązywania najczęściej występujących problemów. **(zarządzanie realnym ryzykiem)**

Wnioski wynikające z rzeczonoj analizy Usługodawca ujmuje w przedmiotowym raporcie dostarczonym do JST.

§5) W niniejszym raporcie znajduje się również **sekcja dot. metodyki odmowy udzielania informacji publicznej w obszarze spraw związanych z cyberbezpieczeństwem w ramach możliwości zastosowania ograniczeń w udzielaniu informacji publicznej - określonych w art. 5 ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902)** – scilicet – możliwość powołania się na poufność informacji.

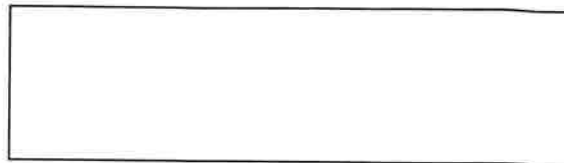
§4) Koszt łączny ww. usług, został uzgodniony pomiędzy stronami na kwotę: **pln + VAT 23%**,
(słownie: złotych) + VAT 23% - (scilicet: pln brutto)

*Uwagi o przedmiocie zamówienia:
.....

W imieniu Zamawiającego:

pieczęć imienna / podpis

**niepotrzebne skreślić*



Pieczęć