/Komparycja Pisma: /

Kierownik Jednostki Samorządu Terytorialnego - w rozumieniu art. 33 ust. 3 Ustawy o samorządzie gminnym (t.j. Dz. U. z 2024 r. poz. 1465, 1572, 1940) Adresatem niniejszego pisma - jest Organ ujawniony w komparycji - jednoznacznie identyfikowalny za pośrednictwem adresu e-mail pozyskanego z Biuletynu Informacji Publicznej Urzędu/Adresata - pod którym odebrano niniejsze pismo.

Aby zachować pełną jawność i transparentność - wnosimy o opublikowanie - niniejszego pisma - w części dot. petycji w BIP Adresata, wyrażając jednocześnie zgodę na publikację wszystkich danych - poniżej podpisanej Osoby Prawnej. (Nadawcy niniejszego pisma) Podstawa prawna, na którą powołujemy się wnosząc o publikację - w Internecie w BIP Urzędu - kontentu dotyczącego niniejszej petycji - określona została w art. 8 ustawy z dnia z dnia 11 lipca 2014 r. o petycjach (tj. Dz.U. 2018 poz. 870) Dane nadawcy (Osoba Prawna) - znajdują się poniżej w stopce 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 2024 r. poz. 1725). Data dostarczenia pisma do Urzędu - dla potrzeb ewentualnej procedury odwoławczej i sądowo-administracyjnej - rejestrowana jest po stronie nadawcy zgodnie z dyspozycją art. 61 pkt. 2 ustawy Kodeks Cywilny (t.j. Dz. U. z 2024 r. poz. 1061, 1237)

W niniejszym piśmie znajdują się 3 sekcje, które w naszym mniemaniu powinny być dekretowane - oddzielnie - w trzech różnych trybach ustawowych. Zgodnie z art 222 KPA to na urzędnikach ciąży obowiązek podziału pisma na 3 sprawy, 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.

Prosimy o ile to możliwe aby nie drukować pisma ale procedować je w postaci elektronicznej - vide judykatura i piśmiennictwo: "J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania…, s. 668; por. także art. 12 ust. 1 komentowanej ustawy (…) Dzielenie pisma na kilka spraw i dekretacja w różnych trybach - Postanowienia WSA i piśmiennictwo - dostępne w sieci Internet.

/ Preambuła pisma (petycji/Wniosku) /
/
Tematyką niniejszego pisma jest walka z incydentami naruszającymi bezpieczeństwo danych powierzonych Urzędnikom przez Obywateli.
Duże uszczegółowienie niniejszego pisma, drobiazgowe powoływanie się na podstawy prawne oraz stosowana nomenklatura słowna wynikają ważkości tematyki, oraz z olbrzymiej skali zagrożeń jakie pojawiają się w związku z incydentami godzącymi w cyberbepieczeństwo danych powierzonych Urzędnikom oraz z katastrofalnych skutków - jakie niesie ze sobą nasilający się w ostatnim czasie - cyberterroryzm.

Każdy, kto analizuje doniesienia prasowe oraz ma dostęp do uzyskiwanych od 25 lat przez nasz podmiot informacji w trybie ustawy o dostępie do informacji publicznej - jest

zaszokowany bezczynnością gmin i marnotrawstwem środków publicznych w tym obszarze. Każdy kto analizuje te materiały - nabiera przekonania, że coraz liczniejsze skuteczne cyberwłamania i incydenty (vide: linki do doniesień prasowych zamieszczone na końcu pisma) - są oczywistym i naturalnym następstwem nieracjonalnego wydatkowania środków w tym obszarze kompetencji przez Urzędy oraz ignorowania rzeczonej problematyki przez Decydentów.
Problem staje się szczególnie istotny w obecnej - złożonej sytuacji geopolitycznej.

W mniemaniu wnioskodawcy - Ministerstwo Cyfryzacji skutecznie i efektywnie zabiega o dodatkowe środki w ramach kolejnych grantów przeznaczanych dla JST. Miarą skuteczności i zaangażowania Ministerstwa Cyfryzacji jest to, ze wg. szacunków łączne środki przekazane JST w ostatnim czasie przewyższają kwotę 2 mld pln.

Z kolei jak wynika z udzielanych nam odpowiedzi środki te są czesto nieracjonalnie wydatkowane w Gminach - i absorbowane inter alia przez Zmowy Cenowe. Ad exemplum - w niektórych gminach dochodzi do zakupu corocznego audytu, o którym mowa w §19 pkt. 14 Rozporządzenia KRI za kwotę ponad 20 tys. pln. Ten sam audyt kosztował 3 lata temu 5000 pln - i miało to miejsce do czasu uruchomienia miliardowych środków z Programu Cyberbezpieczny Samorząd - sic !
To tylko jeden z przykładów, a mamy doskonały tego obraz gdyż - jak wiadomo od 25 lat zadajemy szczegółowe pytania Gminom w trybie ustawy o dostępie do informacji publicznej i udzielając odpowiedzi pod takimi absurdalnymi zmowami cenowymi podpisują się Decydenci.
Takich patologii nie wyeliminuje samo stosowanie przepisów związanych z zamówieniami publicznymi - i wszędzie na Świecie wypracowano już skuteczne mechanizmy pozwalające walczyć ze zmowami cenowymi - w przypadku dodatkowych środków finansowych zwiększających w krótkim okresie podaż w danym obszarze usług.
Jak wykazały udzielane nam odpowiedzi część Decydentów całkowicie ignoruje tematykę - niwecząc tym samym ciężką i efektywną Pracę Ministerstwa Cyfryzacji.

W innych obszarach (np.inwestycje drogowe) wypracowano już mechanizmy weryfikujące zmowy cenowe - o czym można czytać w linkach pond koniec pisma w artykule dot. Prezydenta Tarnowa.
Miejmy nadzieję, że w obszarze cyberbepieczeństwa już niedługo dojdzie do podobnych weryfikacji - chętnie udostępnimy wtedy uzyskane kwantyfikacje.

Wyjaśnienie przedmiotu naszej petycji:
Naszą idee fixe jest działanie łączące - uzasadniony interes pro publico bono - z partykularnymi zdrowo-pojętymi gospodarczymi interesami naszej osoby prawnej.

Większość podmiotów zwracających sie do Urzędów nastawiona jest aby uzyskiwać partykularnie - jakąś osobistą wartość dodaną (zezwolenia/zapomogi/zwolnienia/dokumenty, etc)
W naszym przypadku natomiast - zgodnie z definicją artykułów 28 i 241 Ustawy Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695) - pragniemy „nie tylko brać" - jak czyni to większość zwracających się do Urzędów Podmiotów - ale w ramach zawodowego charakteru działalności staramy się osiągać synergię z urzędami oraz wnosić wartość dodaną poprzez dzielenie się wiedzą, którą w trybie ustawy o dostępie do informacji publicznej uzyskiwaliśmy w ciągu ostatnich 25 lat i dzięki której poddajemy sanacji i usprawniamy funkcjonowanie administracji publicznej.

W ramach wzmiankowanego art . 241 KPA namawia do tego Ustawodawca: “Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności.”

Usprawnianie i zwracanie uwagi na obszary związane z cyberbezpieczeństwem wydaje się szczególnie istotne z punktu widzenia uzasadnionego interesu społecznego pro publico bono. A jak wynika z udzielanych nam informacji publicznych - o czym pisaliśmy powyżej - stan faktyczny w gminach jest katastrofalny.

Biją na alarm również media (linki do niewielkiej części doniesień prasowych opisujących skuteczne cyberataki na Urzędy - zamieszczamy in fine niniejszego pisma.

Per analogiam - pomimo wydana olbrzymich pieniędzy podatników w ostanim czasie - Najwyższa Izba Kontroli opatruje wnioski pokontrolne z 2025 r. - znaczącym tytulem „Cyberbezpeiczeństwo w samorządach kuleje” dalej w protokołach pokontrolnych NIK zaznacza expressis verbis: „(…) Ponad 70 proc. skontrolowanych przez NIK urzędów samorządowych nie byłoby w stanie zapewnić ciągłości działania systemów informatycznych w przypadku wystąpienia sytuacji kryzysowej. Kontrolerzy Izby wykryli też wiele innych niedociągnięć dotyczących bezpieczeństwa cyfrowego JST. (…) „ od lat NIK zwraca uwagę Samorządowców inter alia również na ataki hybrydowe, etc.
O wszystkich tych negatywnych ocenach można czytać w protokole NIK z lutego 2025 r. - sygnatura akt: KAP.430.9.2024 Nr ewid. 123/2024/P/24/004/KAP - dostępny w pełnej postaci na stronach nik.gov.pl <http://nik.gov.pl/>

Skutek wydatkowania olbrzymich środków podatników w tym obszarze jest taki, że o ile w 2019 r. NIK ocenił negatywnie 70% ze skontrolowanych JST w tym obszarze - to w kontroli per analogiam wzmiankowanej powyżej i wykonanej w 2025 r. negatywną oceną objął już nie 70% ze skontrolowanych Urzędów, ale 71% - sic !

Analizują odpowiedzi uzyskiwane z Gmin - nie dziwimy się wcale i uważamy że Minister Cyfryzacji - ma w 100% rację - kiedy powtarza podczas udzielanych wywiadów, że **" Polska jest na cyfrowej wojnie”**

Ministerstwo Cyfryzacji wykonuje tytaniczną pracę, uruchamiając kolejne programy pomocowe podczas kiedy w w gminach chętnie bezrefleksyjnie wydatkowane są środki publiczne na ten cel, beneficjentami są powtarzające się nazwy tych samych firm … efektem tych wdrożeń mnożą się stosy kopiowanej dokumentacji - w której zmieniają się tylko nazwy gmin.
I wszystko jak mawiają Decydenci - w zgodzie z dokumentacją tylko nieliczne gminy starają się walczyć ze zmowami cenowymi i weryfikować setki stron uzyskiwanej dokumentacji - w której jak pokazują nasze analizy np. po złożeniu skargi do Rady Gminy (gdy rzeczona dokumentacja jest poddawana analizie przez Komisję Skarg i Wniosków) - nawet nazwy gmin są czesto mylone w ramach stosowanej przez Usługodawców techniki /kopiuj/wklej - sic !

Jednakże - jak pokazują uzyskiwane przez nas informacje w trybie ustawy o dostępie do informacji publicznej - skuteczne cyberataki zazwyczaj wiążą się z wyjątkowo prostymi błędami popełnianymi przez Urzędników. Co więcej gros skutecznych ataków wykorzystujących proste błędy Urzędników ma miejsce po wdrożeniu programu „Cyfrowa

Gmina" i w trakcie wdrażania programu „Cyberbepieczny Samorząd" - tak jakby hakerzy chcieli udowodnić sobie lub Urzędnikom, że oprócz sprzętu i procedur - ważny jest również aspekt psychologiczny i praca przede wszystkim nad obszarem behawioralnym w Urzędach. Jak wykazują odpowiedzi na nasze wnioski - w których Decydenci opisują genezę incydentów - pracy nad obszarem behawioralnym - nie zastąpi żaden żaden sprzęt zakupiony za pieniądze podatników i żadne procedury usprawniane i kopiowane w stosach dokumentów na papierze.

Wnioskodawca z premedytacją wydłużył niniejszy wstęp - tak aby w BIP gminy - opublikowana została powyższa analiza oparta na wnioskach instytucji kontrolnych analizujących stan faktyczny w skali makro oraz na uzyskiwanych przez nas informacjach publicznych.
W naszym mniemaniu już samo informowanie o kazusach jakie miały miejsce w gminach oraz o incydentach opisywanych nam w trybie ustawy o dostępie do informacji publicznej - działa jak swoista szczepionka, która uodparnia poprzez budzenie niepokoju i szukanie środków zaradczych.

Osnowa Petycji:
Sekcja I §1) Wnosimy rozważenie zainicjowania procedury sanacji przedmiotowego obszaru w Jednostce i pozyskania z rynku „raportu dobrych praktyk" traktującego o zaistniałych kazusach (incydentach związanych z cyberbezpieczeństwem) które pozwolą na unikanie błędów jakie występują notorycznie w większości JST.

Materiał taki w założeniach miałby być przeznaczony dla Kierownictwa Jednostki powinien służyć jako krótka informacja zwracająca percepcję - na najczęściej występujące i powtarzające się błędy w JST, jakich można łatwo uniknąć posiadając świadomość o ich metodologii okolicznościach ich zaistnienia w innych JST.

Aby zachować zasady uczciwej konkurencji oraz jawności i transparentności wnosimy o opublikowanie niniejszej petycji wraz z załącznikami w BIP.

Uzasadnienie petycji:
Ataki z 2025 r. - na Gminy i na system rejestrów państwowych (w tym system PIT) etc - świadczą o tym, że nawet najlepiej chronione systemy (zrealizowane w przetargach za miliony złotych) nie są bezpieczne i widać, że celem ataku hakerów jest utrudnianie życia obywatelom, ośmieszanie Decydentów w samorządach, i dezinformacja - jak miało to miejsce w przypadku ataku na PAP lub dezinformacji w Mieście Tychy

A ataki na takie Urzędy gmin jak Werbkowice, Tuczna czy Nowa Sarzyna - ze względu na złożone umiejętności atakujących - mnożna nazwać jedynie mianem cyberterroryzmu tylko przypadek sprawił, że dotyczyły akurat wzmiankowanych Urzędów - a nie innych.

Afery i cyberataki jakie miały miejsce na instytucje samorządowe w Estonii, na gminy w Finlandii czy w Norwegii są świadectwem, że nawet najlepsze zabezpieczenia serwerów nie wystarczą jeśli nie zadba się odpowiednio o dobre praktyki. Notabene w Finlandii jeden z głośniejszych w i brzemiennych w skutkach cyberataków zaczął się od małej gminy Vellinge (gdzie popełniono szereg prostych błędów) a jego efektem końcowym - na zasadzie kolejnych kostek domina - było ujawnienie niezwykle wrażliwych danych olbrzymiej ilości osób.

Ilość ataków jest na tyle duża i nasila się w takim tempie, że ze strony Ministerstwa Cyfryzacji padają nawet stwierdzenia typu „Samorządy są miękkim podbrzuszem bezpieczeństwa cyfrowego" a celem ataków coraz to częściej może być nawet złośliwe ośmieszanie polskich urzędników wysokiego i niskiego szczebla. Według danych Ministerstwa Cyfryzacji i w zeszłym roku mieliśmy ponad 111 tysięcy incydentów z tym związanych. Widać wyraźną falę wzrostową, vide: https://samorzad.pap.pl/kategoria/aktualnosci/samorzady-miekkim-podbrzuszem-bezpieczestwa-cyfrowego-mc-zapowiada-miliardowe

https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjskie-sluzby-atakuja-polske-nie-tylko-wojna-jest-zagrozeniem

Tymczasem jak wynika z udzielonych nam odwiedzi w trybie ustawy o dostępie do informacji publicznej - w niektórych gminach problematyka jest prawie ignorowana, a Decydenci uważają, że środki otrzymane z Ministerstwa wyczerpują problematykę związaną z zarządzaniem ryzykiem w gminach - sic !
Szerokie, skuteczne i efektywne działania Ministerstwa kontrastują z niefrasobliwością jaką

Opisane powyżej przypadki są wierzchołkiem góry lodowej - a incydenty tego typu miały miejsce w setkach innych gmin i wynika to z udzielanych odpowiedzi na nasze wnioski w trybie ustawy o dostępie do informacji publicznej i nasze skargi złożone do Rad Gmin w trybie art 229 KPA

Pomimo zalewu informacji o nieprawidłowościach w JST o jakimi zasypują nas w ostatnim czasie media (patrz: linki - zamieszczone in fine niniejszego pisma) oraz częstych niejasności wynikających z udzielanych nam informacji publicznych (świadczących często o nieracjonalności w wydatkowaniu powierzonych Decydentom środków podatników) - mamy nadzieję, że ewentualne postępowanie zainicjowane niniejszą petycją będzie prowadzone nie tylko zgodnie z przepisami prawa ale również lege artis - czyli poza bezwzględnym stosowaniem przepisów prawa również zgodnie z zasadami etyki i uczciwej konkurencji. Zawsze sugerujemy aby Decydenci - również w przypadku kwot stanowiących mały ułamek granicznej kwoty 130 tys. pln - (uwzględniając oczywiście zapisy wewnętrznych regulaminów) nawet nadmiarowo posiłkowali się dyspozycją art 275 pkt. 2 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710, 1812, 1933, 2185, z 2023 r. poz. 412)

I.§2) **Aby zachować pełną jawność i transparentność działań - wnosimy o opublikowanie treści petycji (Sekcja dot. 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 danych naszej osoby prawnej. Chcemy działać w pełni jawnie i transparentnie.**

Reasumując - biorąc pod uwagę powyższe wnosimy - jak w osnowie petycji.

Część formalna:
W niniejszym piśmie znajdują się trzy sekcje, które w mniemaniu autora podlegają różnym trybom ustawowym, a co za tym idzie powinny być dekretowane oddzielnie w zależności od aktu prawnego określającego charakter sekcji.

Powyższa część to petycja, natomiast poniżej znajduje się odrębna sekcja, która wg. autora powinna być dekretowana - trybem ustawy Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695)

Wg. piśmiennictwa i judykatury - taka forma jest jak najbardziej dopuszczalna przyczynia się do oszczędności papieru i pozwala traktować sprawy i pisma Interesantów w sposób kompleksowy.
Oczywiście - na urzędnikach ciąży obowiązek dokonania odrębnych odpowiednich dekretacji w zależności od charakteru pisma - w tym przypadku najlepiej w postaci elektronicznej. Interpretacja wg. piśmiennictwa - vide - J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania…, s. 668; por. także art. 12 ust. 1 komentowanej ustawy - dostępne w sieci Internet.