Dane Podmiotu wnoszącego wniosek/petycję* znajdują się poniżej oraz w załączonym pliku sygnowanym kwalifikowanym podpisem elektronicznym - 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) oraz przepisów art. 4 ust. 5 Ustawy o petycjach (tj. Dz.U. 2018 poz. 870)
Data dostarczenia zgodna z dyspozycją art. 61 pkt. 2 Ustawy Kodeks Cywilny (t.j. Dz. U. z 2020 r. poz. 1740)

Adresatem Wniosku/Petycji* - jest Organ ujawniony w komparycji - jednoznacznie identyfikowalny za pośrednictwem adresu e-mail pod którym odebrano niniejszy wniosek/petycję. Rzeczony adres e-mail uzyskano z Biuletynu Informacji Publicznej Urzędu.

W razie wątpliwości co do trybu jaki należy zastosować do naszego pisma - wnosimy o bezwzględne zastosowanie dyspozycji art. 222 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695)

Preambuła Wniosku/Petycji*:
Punktem wyjścia niniejszego wniosku/petycji jest zapis 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.”
Wszystko w kontekście 61 i 63 Konstytucji RP (…) "Każdy ma prawo składać petycje, wnioski i skargi w interesie publicznym, własnym, (…) etc” oraz art 225 KPA: „Nikt nie może być narażony na jakikolwiek uszczerbek lub zarzut z powodu złożenia skargi lub wniosku (…) „

Przed złożeniem niniejszego pisma Wnioskodawca dokonał analizy protokołów NIK, obowiązujących terenów w UE oraz dyspozycji Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222) , Rozporządzenie 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 protokołach pokontrolnych NIK o wspólnym numerze ewidencyjnym - I/23/001/LSZ i cząstkowych protokołach dotyczących każdej z kontrolowanych gmin inter alia wystąpienie pokontrolne: LSZ.411.3.4.2023, etc - kontrolerzy NIK opisali wnioski pokontrolne, w których czytać można m.in.:
„ (…) W każdej ze skontrolowanych jednostek negatywnie oceniono zapewnienie bezpieczeństwa teleinformatycznego. Kontrola wykazała wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, infrastruktury informatycznej, wiedzy i szkoleń pracowników, jak i wykorzystywanie nieaktualnego lub nieprawidłowo skonfigurowanego oprogramowania. W konsekwencji urzędy gmin nie były przygotowane na ataki cybernetyczne.
(…)
Ponadto ustalono, że w żadnym ze skontrolowanych urzędów pracownicy nie przeszli odpowiednich szkoleń w zakresie cyberbezpieczeństwa
(…)
„(…) 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 województwie (…) . W konsekwencji samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców. (…)”

W ostatnich latach liczba incydentów teleinformatycznych systematycznie rośnie. W raporcie za 2021 r. CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa ABW) wskazał na ponad 762 tys. zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego. Dla porównania w 2020 r. było to nieco ponad 246 tys. zgłoszeń i niecałe 227 tys. zgłoszeń w 2019 r. W samych tylko urzędach miast i gmin zarejestrowano ponad 5,5 tys. incydentów. Jak wynika z danych uzyskanych przez NIK od CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez NASK – PIB), który jest odpowiedzialny za obsługę incydentów zgłaszanych m.in. przez jednostki sektora finansów publicznych, liczba incydentów zgłaszanych w województwie zachodniopomorskim w okresie od 2018 r. do 2022 r. wzrosła aż o ponad 1000%. Co istotne, incydenty zgłaszało tylko 30 podmiotów, gdzie na terenie województwa zachodniopomorskiego samych gmin i powiatów jest 135.

Niezależnie od powyższego, od 30 listopada 2023 r. do 29 lutego 2024 r. w Polsce obowiązywał trzeci stopień alarmowy CRP (CHARLIE-CRP), wprowadzony wobec zagrożenia o charakterze terrorystycznym. Zagrożenie to dotyczy

systemów teleinformatycznych administracji publicznej lub systemów, wchodzących w skład infrastruktury krytycznej. (..)

Z całością protokołów pokontrolnych urzędnicy mogą zapoznać się na stronach: www.nik.gov.pl

W mniemaniu wnioskodawcy - taki dramatyczny obraz pracy Urzędników wydatkujących nasze podatki - wynikający z protkołów NIK może być krzywdzący dla niektórych gmin wiejskich.
Wnioskodawca ex professo zajmuje się tym obszarem już ponad 25 lat świadcząc różnego rodzaju usługi dla JST - vide szulc-euphenics.com - i wg. wnioskodawcy są Gminy - mające lege artis zabezpieczony i uregulowany ten obszar usług publicznych.

Niektóre gminy wiejskie - wg. wiedzy Wnioskodawcy - dobrze zarządzają ryzykiem związanym z cyberbepieczeństwem - racjonalnie wydatkują środki podatników w tym obszarze oraz w miarę dobrze - zgodnie z obowiązującymi przepisami - chronią dane Interesantów/Podatników.
Dodatkowo zamawiane usługi zamawiane w tych gminach - są zlecane zgodnie z zasadami uczciwej konkurencji - co wg. NIK - vide nik.gov.pl - nie zawsze ma miejsce w tym obszarze złożonych i wymagających dużego know-how usług.

W niektórych gminach - wg. powyższych danych - i doświadczenia wnioskodawcy - wydatkowane są olbrzymie środki związane z cyberbepieczeństwem a nie przekłada się to na zwiększanie poziomu cyberbepieczeństwa i w dalszym ciągu - podstawowe przepisy prawa są w tym obszarze pogwałcane.
Zagrożenie terrorystyczne oraz zagrożenie ze strony wrogich nam Państw - w związku z obszarem wojen prowadzonych w cyberprzestrzeni - jest najlepszynm dowodem na to sprawy związane z cyberbepieczenstwem są wartością wymagającą szczególnej ochrony i atencji z punktu widzenia uzasadnionego interesu społecznego pro publico bono.
Każde - nawet minimalne - podwyższenie poziomu cyberbepieczeństwa w Jednostkach Administracji Publicznej - jest krokiem milowym z punktu widzenia dobra wspólnego związanego z bepieczeństwem wszystkich Obywateli (Podatników)

W związku z powyższym - Osnowa Wniosku:

§1) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) - w dalszej części rzeczona ustawa może występować pod akronimem: uoddip) - wnosimy o udzielnie informacji publicznej - w przedmiocie:

§1.1) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) - czy wszystkie systemy operacyjne użytkowane w urzędzie posiadają wsparcie producenta
Niniejsze pytanie zostało zadane na postawie obowiązku, który powinni spełnić Urzędnicy - zgodnie z art 19 ust. 2 pkt 12 lit. a 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.)
§1.2) Czy opracowano i wdrożono SZBI - ipso iure art 19 ust. 1 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.)
§1.3) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902)
- jaką samoocenę - en bloc - w skali od 0 do 10 może wg. Kierownictwa przydzielić sobie Urząd w zakresie sensu largo w związku ze stosowaniem zasad cybebepieczeństwa w kontekście - konkretnych wymogów bezwzględnych dyspozycji zawartych §19 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 art. 22 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222)
Oczywiście aproksymacji można dokonać - circa - na podstawie wstępnej wiedzy o stanie faktycznym jaką dysponują decydenci na dzień złożenia przedmiotowego wniosku.
Wnioskodawca uznaje że 0 to najniższa ocena - stan faktyczny niezgodny z wszystkimi powyżej powołanymi dyspozycjami ustawowymi a 10 to ocena najwyższa - scilicet - stan faktyczny zgodny ze wszystkimi wyżej powołanymi przepisami.

Notabene - ze względu napiętą sytuację geopolityczną oraz na zdarzające się coraz to częściej - skuteczne ataki - o jakich pisze w wyżej powołany protokołach Najwyższa Izba Kontroli oraz donoszą media - poniżej znajduje się petycja aby Decydenci podjęli wszelkie racjonalne działania związane związane z podwyższeniem oszacowanego powyżej poziomu związanego z wypełnianiem podanych, obowiązujących podstaw prawnych.

§1.4) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) - czy w ciągu ostatniego roku wykonano okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji - nakazany §19 ust. 2 pkt. 14 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.) ?
§1.4.1) Jeśli odpowiedź na niniejsze pytanie jest twierdząca - wnosimy o podanie nazwy podmiotu/firmy, która wykonała rzeczony audyt.

§2) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) - ile incydentów zgłosiła Jednostka w przeciągu ostatniego roku do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV w rozumieniu art. 22 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222).
§2.1) W trybie wyżej wzmiankowanych przepisów - czy forma zgłoszeń była zgodna z art. 23 rzeczonej ustawy.

W razie dodatkowych pytań dotyczących kontentu wniosku prosimy o kontakt pod numerem: 608-318-418

Ciąg Dalszy Nastąpi po uzyskaniu pierwszych odpowiedzi.

Aby nie absorbować zbytnio czasu Urzędników, Wnioskodawca zaznacza, że wystarczy, iż poniższe dane zostaną podane w szacunkowej formie, z pewnym przybliżeniem tak aby możliwa była - na tym etapie - jedynie analiza ogólna i wyciągnięcie wniosków wstępnych o stanie faktycznym panującym w Jednostce utrzymywanej ze środków podatników.

Wnioskodawca będzie bardziej usatysfakcjonowany jeśli szacunkową odpowiedź uzyska - ad hoc wg. kwantyfikacji przybliżonych - „bez zbędnej zwłoki” przed upływem terminu ustawowego określonego w art 13 uoddip niż ze szczegółowej, dokładnej odpowiedzi udostępnionej pod koniec maksymalnego interwału czasowego określonego przez Ustawodawcę w rzeczonym przepisie.
Jeszcze raz zaznaczmy, celem wnioskodawcy jest oszacowanie ogólnego, przybliżonego obrazu stanu faktycznego, oraz złożenie petycji o podniesienie poziomu bezpieczeństwa cybernetycznego - a nie ocena pod kątem szczegółowych wyliczeń.

Uzasadnienie pytań:

Wg. powyżej powołanych protokołów NIK, odnośnych podstaw prawnych wynikających z dyspozycji ustawowych, oraz informacji medialnych dotyczących kazusów jakie miały miejsce w tym obszarze.

II - Dodatkowa petycja - procedowana w trybie ustawy o petycjach (tj. Dz.U. 2018 poz. 870)

Petycja odrębna - dla ułatwienia i zmniejszenia biurokracji - odrębna petycja została dołączona do niniejszego pisma. Jak wynika z poniższego piśmiennictwa nie jest to łącznie trybów - vide - J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania…, s. 668; por. także art. 12 ust. 1 komentowanej ustawy - (materiał dostępny w sieci Internet).

W trybie Ustawy o petycjach (Dz.U.2018.870 tj. z dnia 2018.05.10) - biorąc pod uwagę, wyżej przytoczone akty prawa, piśmiennictwo i powołane argumenty - można upewnić się że poruszana przez nas tematyka należy z pewnością do wartości wymagających szczególnej ochrony w imię dobra wspólnego, mieszczących się w zakresie zadań i kompetencji adresata petycji

- wnosimy o:

II.1) Szczegółowe zapoznanie się Decydentów z cytowanymi protokołami NIK oraz zaplanowanie działań zapobiegawczych pod kątem regularnego badania zasobów w zakresie zagadnień cyberbepeiczeństwa etc i spełnienia wszystkich powołanych powyżej obowiązujących przepisów prawa.
Wszystko w kontekście tez stawianych przez NIK oraz działań związanych z zaspokojeniem wyżej powołanych aktow prawa.
Przywołane przez wnioskodawcę protokoły oraz pozostałe protokoły z tego obszaru dostępne są na stronach

www.nik.gov.pl

Nakreślony przez NIK panujący w Gminach negatywny stan faktyczny związany z tym obszarem jest - w naszym mniemaniu - wręcz tragiczny, ale być może są gminy gdzie jednak rzeczywisty obraz poziomu cyberbepieczeństwa - odbiega od tego co diagnozuje NIK.
Mamy taką nadzieję.

Oczywiście ABY NASZA PETYCJA NIE BYŁA W ŻADNYM RAZIE ŁĄCZONA Z PÓŹNIEJSZYM ewentualnym trybem zamówienia nie musimy dodawać, że jesteśmy przekonani, iż ewentualne postępowanie dot wyłonienia Usługodawców będących beneficjentem - postępowań związanych z sanacją tego obszaru - 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, oraz racjonalnym wydatkowaniem środków publicznych.

II.2) 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.

Oczywiście uczulamy aby nie udzielać nam żadnych innych informacji poufnych - poza powyższymi odnoszącymi się wyżej powołanych do konkretnych przepisów prawa zawartych w przywołanych - ustawach i rozporządzeniach.

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

III. §3) 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 i kontakt pod numer celem sprecyzowania czy jest to termin dogodny dla obu stron.
§4) Przy okazji prosimy o zwrotne poinformowanie jakim dniem jest w urzędzie dzień przyjęć interesantów w sprawach skarg i wniosków i czy w ramach tego dnia przyjmowane są też wnioski w trybie art 241 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.

W oparciu o zasadę, konieczności ciągłego usprawniania każdej organizacji - w ramach zdobytej przez nas wiedzy w tym obszarze ex professo - pragniemy w trybie art 253 KPA w związku z art 241 KPA skorzystać - pro publico bono - z ewentualnej próby możliwości optymalizacji tego obszaru w uzasadnionym interesie pro publico bono.

Z góry - dziękujemy za poświęcone nam pół godziny czasu.

§5) 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 styczna 2002 r. Nr 5, poz. 46) - na adres jawnosc-transparentnosc@samorzad.pl
§5a) 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 jawnosc-transprentnosc@samorzad.pl

Wniosek został sygnowany 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)

Wnioskodawca:
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

Elektronicznie podpisany przez:
Adam Bolesław Szulc
Data:
2024-11-15 14:37:56

Zwyczajowy Komentarz do Pisma.
W naszym na każdym ciąży obywatelski obowiązek uczestnictwa w usprawnianiu Administracji Publicznej - tak aby w ramach posiadanej wiedzy - kontrolować - w jaki sposób Urzędnicy wydatkują nasze podatki.

Zgodnie z intencją Ustawodawcy do osiągnięcia tego celu np. 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.”

Pamiętajmy o przepisach zawartych inter alia: w art. 225 KPA: "§ 1. Nikt nie może być narażony na jakikolwiek uszczerbek lub zarzut z powodu złożenia skargi lub wniosku albo z powodu dostarczenia materiału do publikacji o znamionach skargi lub wniosku, jeżeli działał w granicach prawem dozwolonych. § 2. Organy państwowe, organy jednostek samorządu terytorialnego i inne organy samorządowe oraz organy organizacji społecznych są obowiązane przeciwdziałać hamowaniu krytyki i innym działaniom ograniczającym prawo do składania skarg i wniosków lub dostarczania informacji - do publikacji - o znamionach skargi lub wniosku.”

Pomimo, że zgodnie z judykaturą: I OSK 1277/08 i odnośnym piśmiennictwem - w mniemaniu wnioskodawcy - nie ma konieczności opatrywania pisma kwalifikowanym podpisem elektronicznym - w ramach wniosku o takiej formie - autor pisma - z ostrożności i chcąc działać bona fides - sygnował odnośny załącznik zgodnie z przepisami Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2019 r. poz. 162, 1590) oraz art. 4 ust. 5 Ustawy o petycjach (tj. Dz.U. 2018 poz. 870)

Eksperci NIK piszą: "Niewielka liczba składanych wniosków o udzielenie informacji publicznej, liczba skarg złożonych do WSA, jak również liczba pozwów złożonych do sądów rejonowych, świadczyć może o braku zainteresowania w egzekwowaniu powszechnego prawa do informacji publicznej. Z drugiej strony, realizację tego prawa utrudniają podmioty zobowiązane do pełnej przejrzystości swojego działania, poprzez nieudostępnianie wymaganej informacji publicznej" [Protokół pokontrolny dostępny w sieci Internet: LBY-4101- […] Mamy nadzieję, zmienić powyższą ocenę, być może nasz wniosek choć w niewielkim stopniu – przyczyni się do zwiększenia tych wskaźników.

Dobro Petenta i jawność życia publicznego powinno być nadrzędnym celem każdego podmiotu, dlatego staramy się również upowszechniać zapisy Ustawowe dotyczące Wnioskowania. Kwestie te Ustawodawca podkreślił i uregulował w art. 63 Konstytucji RP: "Każdy ma prawo składać petycje, wnioski i skargi w interesie publicznym, własnym lub innej osoby za jej zgodą do organów władzy publicznej oraz do organizacji i instytucji społecznych w związku z wykonywanymi przez nie zadaniami zleconymi z zakresu administracji publicznej." oraz w art. 54 ust. 1 Konstytucji RP "Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji.”

Ponadto publicity medialne świadczące o tym że warto i należy pytać o stan faktyczny w Jednostkach Administracji Publicznej - szczególnie w Gminach/Miastach
Zdaniem Autorów wniosku - w Jednostkach Administracji Rządowej sytuacja o wiele lepsza.
To jak wygląda sytuacja w Gminach wynika - w sposób oczywisty wynika choćby z takich kazusów opisanych przez Media inter alia:
1) „Z kasy gminy zniknęło 5 mln” pieniędzy Podatników Konstancin-Jeziorna. Prokuratura zajęła mieszkanie burmistrza. Wcześniej z miejskiej kasy zniknęło 5 milionów złotych | TVN Warszawa (tvn24.pl) - sic !
2. Ostrowice „Wójt i skarbniczka skazani na 7 lat więzienia” Z tytułu samych odsetek parabanków Podatnik poniósł szkodę na co najmniej 13 mln pln: https://tvn24.pl/trojmiasto/ostrowice-z-powodu-zadluzenia-gmina-zniknela-z-mapy-polski-wojt-i-skarbniczka-uslyszeli-wyrok-st5680605
3. Procedury ochrony danych osobowych - WSA potwierdził karę dla burmistrza (prawo.pl) „Burmistrz Aleksandrowa K. nie zawarł umowy RODO … wraz z kosztami sądowymi zapłacił ponad 50 tys. pln
4. Afera w Dolnośląskim Urzędzie Wojewódzkim - 2019 r. - https://wroclaw.wyborcza.pl/wroclaw/7,35771,30691325,dolnoslaska-afera-wizowa-proces-w-sprawie-korupcji-w-urzedzie.html
5. Sędzia Tomasz Szmydt - już od roku współpracował z obcym wywiadem - nikt tego nie podejrzewał - sic! - Czy nikt Go o nic nie pytał? przez rok czasu? … gdzie jawność i transparentność ?
vide materiał PAP: https://www.pap.pl/aktualnosci/nowe-ustalenia-sluzb-po-zdradzie-tomasza-szmydta
6. Skuteczny atak na urząd w Sokołowie Podlaskim https://cyberdefence24.pl/cyberbezpieczenstwo/atak-ransomware-

na-urzad-gminy-w-sokolowie-podlaskim-danych-nie-wykradziono
7. Wyciek Danych Osobowych w Gminie Sitkówka https://kielce.wyborcza.pl/kielce/7,47262,27912551,po-wycieku-danych-z-urzedu-gminy-w-nowinach-prace-stracil-informatyk.html

W Centralnych Jednostkach Administracji Rządowej sytuacja jest o wiele lepsza.
Pomimo powyższych informacji prasowych pozostajemy w przekonaniu, że gros Urzędników działa w dobrej wierze - zatem tym bardziej warto dbać o stan faktyczny aby poprzez jawność i transparentność wspierać usprawnianie administracji publicznej.

etc, etc - więcej na naszych stronach www.szulc-euphenics.com

W Jednostkach Administracji Rządowej sytuacja jest o wiele lepsza.

etc, etc - więcej na naszych stronach www.szulc-euphenics.com

PONIŻEJ:
Aby zobrazować - jak zdaniem Wnioskodawcy - powinna wyglądać prawidłowo udzielona odpowiedź w trybie ustawy o dostępie do informacji publicznej
wnioskodawca załącza - dwie przykładowe odpowiedzi z innych Jednostek.
Obrazują one prawidłowy tryb udzielania informacji publicznej - przez Sądy - posiadające duże know how w obszarze prawnym - jak widać nawet Sądy podlegają obowiązkowi udzielania informacji publicznej - i wywiązują się z tego wzorowo.
Co prawda - odpowiedzi dotyczą pytań z innego zakresu merytorycznego - ale wnioskodawca chce jedynie pokazać idee fixe - prawidłowego podejścia do obszaru udzielania informacji publicznej - krótkie treściwe odpowiedzi - sensu stricto.