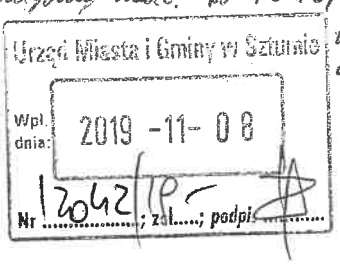
Regina Lukas [termin: do 22.11.2019r. – 14 dni]

identyczny mail: W 12016/19 z dn. 08.11.2019

Od:	stowarzyszenie.1@wp.pl
Wysłano:	8 listopada 2019 11:52
Do:	sztum@sztum.pl
Temat:	zapytanie

OR IX + OR VIII



Kolejne kary UODO na podmioty publiczne. RODO w administracji: Uodo.gov.pl

Na podstawie art. 10 ust. 1 ustawy z dnia 6 kwietnia 2001 r. o dostępie do informacji publicznej wnosimy się o udostępnienie następującej informacji z zakresu ochrony danych:

Pozwalamy sobie również przypomnieć, że ipso iure art. 2 ust. 2 Ustawy o dostępie do informacji publicznej " (...) Od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego.

1. Czy korzystają Państwo z podmiotu zewnętrznego lub pracownika w zakresie Inspektora Ochrony Danych (IOD), a jeżeli tak to proszę o podać:

- daty zawarcia i zakończenia obowiązywania umowy z IOD
- daty zawarcia i zakończenia umów od roku 2015 wszystkich umów zawieranych przez jednostkę
- wysłania kopii zawartej umowy w formie elektronicznej np. skan.
- wartość brutto za okres jej obowiązywania oraz miesięczną kwotę
- w jaki sposób (zapytanie ofertowe, przetarg itd.) zostanie wybrany wykonawca w roku 2020 i następnych latach?
- czy wybór IOD jest zgodny z procedurami wewnętrznymi i regulaminami? Jeżeli zdecydujecie się na wybór zewnętrznego IOD proszę o wysłanie wszystkich dokumentów opisujących wybór wykonawcy
- przedmiot i sposób realizacji usługi przez przedłożenie skanu umowy
- czy w ramach umowy IOD sam wypełnia wszystkie wzory dokumentów np. rejestry systemów informatycznych czy tylko przedkłada dokumenty a wypełnianiem zajmuje się osoba u administratora; jeśli taka jest praktyka to zgodnie z najnowszym stanowiskiem UODO jest to nieprawidłowe
- datę, godzinę wizyt osobistych u administratora z wykazem czynności
- ile razy w tygodniu IOD wykonywał swoje czynności w siedzibie administratora?
- czy duże znaczenie ma gospodarność finansowa? Czy RIO w swojej działalności kontrolnej kontrolowało gospodarki finansową a zwłaszcza umowy IOD z zewnętrznym IOD? Czy w okresie ostatnich 4 lat były takie kontrole?
- proszę o podanie liczby żądań określonych w art. 15 – 21 RODO jakie wpłynęły do adresata niniejszego wniosku
- wydruki dotyczące działań IOD – z naszych informacji wynika, że brak jest potwierdzeń (wydruków), że zostało wszystko przysłane (kto, kiedy i do kogo przesłał przedłożone informacje
- metryka zmian potwierdzająca aktualizację Polityki ochrony danych osobowych (kiedy przeprowadzał aktualizację/przegląd i dokonywał zapisów w metryce).
- czy IOD od 01.01.2019r. poinformował i przygotował umowę zawartą z firmą, która dostarcza oprogramowanie do stworzenia BIP i zajmowała się obsługą serwisową w tym zakresie. P oniżej stanowisko UODO o konieczności zawarcia umowy powierzenia https://uodo.gov.pl/pl/138/1240

Jeśli takiej umowy Państwo nie macie to dlaczego zatrudniacie zewnętrznego IOD, płacąc niebotyczne pieniądze, który nie umieje zadbać o Państwa bezpieczeństwo?
W konsekwencji braku takiej umowy administrator dopuścił się udostępnienia danych osobowych bez podstawy prawnej, czym naruszył określone w RODO: zasadę przetwarzania danych zgodnie z prawem (art. 5 ust. 1 lit. a) oraz zasadę poufności (art. 5 ust. 1 lit. f).
https://uodo.gov.pl/pl/138/1240

Czy opracowano analizę ryzyka tylko a nie ogólną: związanej z publikacją nagrań z posiedzeń rady wyłącznie w serwisie YouTube itp.? Jeśli nie to doszło więc do naruszenia zasady integralności i poufności (art. 5 ust. 1 lit. f) oraz zasady rozliczalności (art. 5 ust. 2).
Proszę o zapoznanie się z stanowiskiem UODO
https://uodo.gov.pl/pl/138/1240

Jeśli takiej analizy ryzyka Państwo nie macie to po co dla Państwa jest zewnętrzny IOD nie umiejący zadbać o Państwa bezpieczeństwo?
Czy IOD audytował BIP pod kątem retencji danych? Jak długo przechowuje się na stronie BIP oświadczenia majątkowe radnych? Czy są m.in. oświadczenia majątkowe z 2010 roku, podczas gdy okres ich przechowywania wynosi 6 lat?
Czy jest przygotowana polityka retencji danych dla BIP?
Jeśli takiej polityki Państwo nie macie to po co dla Państwa jest zewnętrzny IOD nie umiejący zadbać o Państwa bezpieczeństwo?
Poniżej stanowisko UODO:

https://uodo.gov.pl/pl/138/1240
Kto kontroluje IOD? Czy jego praca poddawana jest kontroli zewnętrznego audytora?
Czy radni kontrolują umowy zawarte z IOD?
Prosimy o dane radnych
Czy dokumenty uzupełniane przez iod czy obowiązuje stara zasada : przesyłamy wzory a Ty radź sobie sam?
Czy był u Państwa przeprowadzony audyt KRIO? Kiedy, data, raport, sprawozdanie, kto przeprowadzał?
Prezes UODO w decyzji z 10 września 2019 r. (ZSPR.421.2.2019) wyjątkowo mocno podkreśla: „kontrola dostępu i uwierzytelnianie to podstawowe środki bezpieczeństwa mające na celu ochronę przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Zapewnienie dostępu uprawnionym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów i usług to jeden z wzorcowych elementów bezpieczeństwa".
Czy IOD zewnętrzny podjął działania realne w tym celu czy tylko opracował dokumenty, a realizację pozostawił innym osobom czy też faktycznie dokonał ich realizacji. Zgodnie ze stanowiskiem UODO za realne działania w zakresie bezpieczeństwa odpowiada także IOD.
Jakie realne, a nie teoretyczne działania IOD podjął w celu **wdrożenia dostępu do sieci i usług sieciowych**, w tym sposób autoryzacji użytkowników w sieci i środki wykorzystywane do realizacji dostępu do sieci (np. używanie VPN lub sieci bezprzewodowych), oraz uregulować sposób monitorowania korzystania z usług sieciowych (pkt 9.1.2 PN-EN ISO/IEC 27002).
Czy IOD nie zapomniał o konieczności zmiany domyślnych danych logowania w wykorzystywanych systemach i narzędziach (pkt 9.1.4 PN-EN ISO/IEC 27002; pkt 2.8 i 2.19 OWASP).
Czy IOD **kontroluje użycie programów narzędziowych** umożliwiających obejście zabezpieczeń systemów i aplikacji, m.in. ograniczyć możliwość instalacji takich narzędzi przez użytkowników (pkt 9.4.4 PN-EN ISO/IEC 27002).
Czy IOD kontroluje **dostęp do kodów źródłowych programów oraz związanych z nimi elementów**, takich jak projekty, specyfikacje, plany weryfikacji i badania poprawności (pkt 9.4.5 PN-EN ISO/IEC 27002).
Jakie działanie podjął IOD w celu **zadbania, aby systemy i aplikacje nie były podatne na ataki** SQL Injection, RFI, LFI, XML Injection, XML External Enity, XPath query, XSS, HTTP Parametr Pollution (pkt 5.10, 5.13, 5.14 i 5.15 OWASP).

Preambuła Wniosku:
Najwyższa Izba Kontroli w protokole pokontrolnym nr kap-4101-002-00/2014 - " (...) negatywnie ocenia działania burmistrzów i prezydentów, DYREKTORÓW , KIEROWNIKÓW w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie. (...)"
Zadaniami KRIO zajmuje się IOD. Niedopuszczalną praktyką jest sytuacja, że IOD zleca wszystkie zadania ASI!. Czy IOD uczestniczy w prachac?

☒

Lp.	Zagadnienie	*Tak*	Nie	Uwagi
Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.				
1.	Czy prowadzona jest ewidencja:			
	a) sprzętu informatycznego w ramach ewidencji majątkowej?CZY IOD KONTROLUJE EWIDENCJĘ			
	b) oprogramowania (np. licencje)? IOD KONTROLUJE EWIDENCJĘ			
	c) umów serwisowych?			
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? Jeśli TAK proszę o przedłożenie dokumentu. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ			

	EWIDENCJE			
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.				
1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT? *Jeśli TAK proszę o ich wskazanie.*			
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE?*			

	CZY IOD KONTROLUJE W/W			
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?			
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W* Jeśli TAK proszę o przedłożenie dokumentu.			
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.			
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?			
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO*			

	wniosku?			
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.				
	Należy zaznaczyć stosowane w jednostce rozwiązania.			
1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).			
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:			
a.	ochrona sieci na poziomie portów LAN			
b.	BIOS			
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows			
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
e.	system ochrony zewnętrznej klasy firewall			
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;			
g.	stosowanie tokenów z hasłami			

	jednorazowymi			
Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY*				
1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu.*			
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? Jeśli TAK proszę o udokumentowanie.			
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?			
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?			
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? Jeśli TAK proszę wskazać, w jaki sposób.			
Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu/ oprogramowania? Jeśli TAK proszę o udokumentowanie.			
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?			

Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.			
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?			
3.	Czy istniej możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?			
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?			
Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W*				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?			
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?			
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?			
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?			
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?			

6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?			
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?			
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?			
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?			
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?			
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?			
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?			
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?			
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)			
Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?			
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?			

2. Jeśli korzystacie Państwo z podmiotu zewnętrznego w zakresie Inspektora Ochrony Danych (IOD) lub własnego pracownika, a jeżeli tak to proszę o podać:

- czy podmiot prowadzi BIP i pod jakim adresem internetowym?
- z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub www.bip.edu.pl czy inny (podać jaki)
- jakie są umowne okresy świadczenia tej usługi. Czy podmiot wywiązywał się w tych okresach? Dane odrębnie za poszczególne okresy w latach 2017-2019.

- proszę podać liczbę informacji publicznych opublikowanych w BIP w roku 2018 oraz w 2019r.
- proszę podać liczbę wniosków o informację publiczną jakie wpłynęły do podmiotu, liczbę wniosków na które udzielono odpowiedzi wraz wnioskowaną informacją, liczbę wniosków na które udzielono odpowiedzi odmownej udzielenia informacji, liczbę wniosków na które nie udzielono odpowiedzi, liczbę postępowań sądowych w związku wnioskami o informację publiczną. Jeśli sąd określił, że podmiot pozostawał w bezczynności podać ile razy to określił i w poszczególnych latach (rok wyroku i rok przedmiotowego wniosku). Dane odrębnie za rok 2015, 2016, 2017, 2018 oraz 2019.
- informację czy instytucja planuje zmianę obecnego dostawcy BIP?
- jakie elementy przy zmianie dostawcy BIP są dla instytucji najważniejsze?
- czy w ostatnich trzech latach pracownicy podmiotu uzupełniali wiedzę podczas szkoleń z zakresu dostępu do informacji publicznej/prowadzenia BIP/poprawnej obsługi wniosków o informację publiczną? Jeśli tak to kto był dostawcą szkoleń (www.instytutOS.pl, www.nbip.pl czy inny (jaki?)), Proszę podać ilu pracowników przeszkolono i jaki był koszt brutto szkolenia za pracownika oraz łącznie, a także czy były to szkolenia zamknięte czy otwarte, stacjonarne(w siedzibie czy wyjazdowe), zdalne (stacjonarne czy telekonferencja)

MAMY PRAWO WIEDZIEĆ I CHCEMY WIEDZIEĆ
Nadmieniamy, iż powyższe pytania o informację publiczną - wydają się **szczególnie istotne** z punktu widzenia interesu publicznego pro publico bono - nawiązując do art. 3 ust. 1 pkt. 1 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - gdyż ten obszar **RODO** - wydaje się (jak wynika z uprzednio uzyskanych przez nas odpowiedzi) - szczególnie istotny.

Udzielenie niepełnej informacji lub niezgodnej z treścią żądania przez adresata ocenia się jako bezczynność

Komentarz do Wniosku:
Dodatkowo wnioskodawca Urząd powinien także procedować nasze wnioski - w trybie Ustawy o petycjach (Dz.U.2014.1195 z dnia 2014.09.05). Zatem - wg.
"Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności." - w sensie możliwości otwarcia procedury sanacyjnej.

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-4101-09/2010]. Mamy nadzieję, zmienić powyższą ocenę, być może nasz wniosek choć w niewielkim stopniu – przyczyni się do zwiększenia tych wskaźników.
Oczywiście - wszelkie ewentualne postępowania w zakresie wyboru IOD - ogłoszone przez Jednostkę Administracji Publicznej - będące następstwem niniejszego wniosku - należy przeprowadzić zgodnie z rygorystycznymi zasadami wydatkowania środków publicznych - z uwzględnieniem stosowania zasad uczciwej konkurencji, przejrzystości i transparentności - zatem w pełni lege artis.

WSZYSTKIE UMOWY SĄ JAWNE:
WSA w Warszawie w dniu 30 maja 2017 r. (**sygn. II SAB/Wa 10/17**) rozpatrywał skargę na I Prezesa Sn w zakresie min. żądania udostępnienia „w zakresie kopii wszystkich umów zawartych przez Sąd Najwyższy w sierpniu 2016 roku po dokonaniu „zasłonięcia" w zakresie adresu zamieszkania oraz numeru PESEL, lecz z zachowaniem imion i nazwisk wykonawców oraz nazw przedsiębiorców".
WSA uznał skargę częściowo za zasadną, i w uzasadnieniu przypomniał bardzo ważną kwestię:

„Nie do zaakceptowania jest pogląd organu, że udostępnieniu w trybie ustawy o dostępie do informacji publicznej podlegają tylko te umowy cywilnoprawne, do których zastosowanie ma ustawa – Prawo o zamówieniach publicznych. **Zgodnie z art. 139 ust. 3 tej ustawy, umowy w sprawach zamówień publicznych zawierane w trybie tej ustawy są jawne i podlegają udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej. Jednakże nie można w tej sytuacji, a contrario do powyższego przepisu uznać, że skoro ustawa ta ustanawia zasadę jawności dla umów, których wartość przekracza 14 000 euro i przewiduje ich udostępnianie na zasadach określonych w przepisach o dostępie do informacji publicznej, to do umów o mniejszej wartości wyłącza stosowanie ustawy o dostępie do informacji publicznej. Ze względu na doniosłość umów zawieranych w trybie ustawy Prawo o zamówieniach publicznych ustawodawca zapisem art. 139 ust. 3 poszerzył dostęp do umów zawieranych w trybie tej ustawy.** Jawność umów w sprawach zamówień publicznych na gruncie ustawy o dostępie do informacji publicznej wyłącza możliwość odmowy ich udostępnienia z powołaniem się na którąkolwiek z tajemnic ustawowo chronionych. **Nie jest zatem dopuszczalne wydanie decyzji odmawiającej udostępnienia umów w sprawach zamówień publicznych, gdyż są one jawne (vide: wyrok NSA z dnia 29 lutego 2012 r. sygn. akt I OSK 2215/11).** Nie do przyjęcia jest więc stanowisko organu, że ustawa o dostępie do informacji publicznej nie znajduje zastosowania do udostępniania umów zawartych poza trybem zamówień publicznych„.

Proszę o udzielenie odpowiedzi na maila: stowarzyszenie.1@wp.pl

Aneta Rutkowska
ul. Narutowicza, 20-004 Lublin