

Wniosek 1

Wniosek o dostęp do informacji publicznej

na podstawie art. 61 Konstytucji RP z dnia 2 kwietnia 1997r. oraz art.10 ust.1 z dnia 6 września 2001 roku ustawy o dostępie do informacji publicznej (Dz.U. z 2019 r., poz.1429)
składam wniosek o dostęp do informacji publicznej:

1. Czy korzystają Państwo z podmiotu zewnętrznego w zakresie funkcji Inspektora Ochrony Danych (IOD)? Jeżeli tak, to proszę o podanie:

a) datę zawarcia i zakończenia umowy;

01.01.2023r. do 31.12.2023r.

b) art. 37 ust. 5 RODO wskazuje, że Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa art. 39 RODO. Proszę wykazać kwalifikacje i wiedzę prawniczą IOD. Czy IOD jest prawnikiem?

IOD nie jest prawnikiem.

Inspektor Danych Osobowych ma niezbędną wiedzę i odpowiednie kwalifikacje do pełnienia tej funkcji - świadczą o tym przedłożone dla Administratora Danych dyplomy, certyfikaty i przebyte kursy szkoleniowe:

- ukończone studia podyplomowe z zakresu bezpieczeństwa i ochrony danych osobowych w sektorze publicznym -2018r

- certyfikat kompetencji IOD - ekspert dokumentowania systemu ochrony danych osobowych - 2018r

- certyfikat kompetencji IOD - ekspert stosowania przepisów RODO i zarządzania systemem ochrony danych osobowych 2018r

- certyfikat kompetencji IOD & Specjalisty ds. Ochrony Danych Osobowych 2020 r.

- ukończone szkolenie: audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg EN ISO/IEC 27001:2017

c) Jak jest spełniona niezależność IOD? Czy dokonano stosowanych zapisów w przepisach wewnętrznych?

IOD jako podmiot zewnętrzny podlega wyłącznie Administratorowi Danych osobowych

d) termin i zakres przeprowadzenia ostatniego szkolenia RODO dla pracowników; ostatnie szkolenie miało miejsce w III kwartale 2022r.

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia 10 Maja 2018r.
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

e) termin i zakres przeprowadzenia ostatniego szkolenia z KRI dla pracowników; elementy zagadnień z KRI były omawiane podczas ostatniego szkolenia z RODO w III kwartale 2022r.

f) termin i zakres przeprowadzenia ostatniego szkolenia z cyberbezpieczeństwa dla pracowników; elementy zagadnień z KRI były omawiane podczas ostatniego szkolenia z RODO w III kwartale 2022r.

g) Kto w/w szkolenia przeprowadza? Zgodnie z art. 39 ust.1 za w/w szkolenia odpowiada IOD?
za szkolenia z RODO odpowiada IOD

h) termin i zakres ostatniego audytu w siedzibie jednostki w zakresie RODO. ostatni audyt miał miejsce w 2021r. kolejny zaplanowany na IV kwartał 2023r - zakres audytu - zabezpieczenia fizyczne i techniczne przetwarzanych danych osobowych oraz przegląd rozwiązań IT zabezpieczających przed pshisingiem.

2. Czy był u Państwa przeprowadzony audyt KRI? Jeżeli tak, to proszę podać:

Audyt KRI został przeprowadzony w ramach audytu RODO w 2019r., 2022r. oraz zaplanowany III kwartale 2023r.

a) Wykonawca - firma zewnętrzna czy pracownik instytucji;
nie dotyczy

b) Termin ostatniego audytu KRI;
patrz punkt 1 lit.f

c) Jeżeli jest to firma zewnętrzna - proszę o wskazanie wartości netto i brutto przeprowadzonego audytu KRI .

audyt KRI przeprowadzono w ramach świadczonej usługi ochrony danych

**osobowych z firmą MW CONSULTING Marcin Wieczorek - Umowa nr G/1/2023
na kwotę 320 zł miesięczne brutto**

3. Czy w roku 2022 miały miejsce u Państwa następujące zdarzenia:
 - a) Naruszenie ochrony danych osobowych: kiedy, czego dotyczyły, czy były zgłoszone do PUODO;
nie
 - b) Incydent cyberbezpieczeństwa: kiedy, czego dotyczył, czy był zgłoszony do CSIRT.
nie
4. Czy dokumentacja RODO została aktualizowana? Jeśli tak to kiedy?
Dokumentacja RODO jest aktualizowana na bieżąco w zależności od zdefiniowanych procesów przetwarzania danych oraz zmieniających się przepisów prawa (np. ostatnie zmiany w kodeksie pracy)
5. Czy dokumentacja RODO uwzględnia zmiany EROD 21.06.2021r
https://edpb.europa.eu/news/news/2021/edpb-adopts-final-version-recommendations-supplementary-measures-letter-eu_pl oraz stanowiska organu nadzorczego poczynwszy od roku 2020? Proszę opisać na czym polegają zmiany w dokumentacji?
Dokumentacja spełnia wszelkie wymagane przez RODO wymagania oraz bierze pod uwagę dobre praktyki i orzecznictwo w zakresie danych osobowych

Wniosek 2

WNIOSEK INFORMACJA PUBLICZNA

Na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001r. (Dz. U. Nr 112, poz. 1198) zwracam się z prośbą o udostępnienie informacji publicznej.

Pozwalamy sobie 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.

Przedmiotowy wniosek/wnioski - nie powinny być rozpatrywane w trybie KPA. Urząd powinien procedować nasze wnioski W TRYBIE Ustawy o dostępie do informacji publicznej

Celem naszych wniosków jest - sensu largo - usprawnienie, naprawa - na miarę istniejących możliwości - funkcjonowania struktur Administracji Publicznej - głównie w Gminach/Miastach/szkołach - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych. W takiej sytuacji KPA nie ma zastosowania; więcej na jawność.pl

W przypadku braku odpowiedzi na informację publiczną **złożymy wniosek do Wojewódzkiego Sądu Administracyjnego skargę na bezczynność.**

Treść wniosku:

W maju-czerwcu Prezes UODO nałożył już 3 kary pieniężne na administratorów danych. Co je łączy? Każda z nich podyktowana została brakiem właściwej współpracy administratorów z organem nadzorczym, brak odpowiednich kwalifikacji IOD oraz uchybień w zakresie wdrożenia RODO. Czy w najbliższym czasie możemy spodziewać się kolejnych kar? Tak.

My natomiast zwracamy się do Państwa o udzielenie informacji publicznej oraz przesłania odpowiedzi na maila : rodo.rodo55@wp.pl

1. Czy na stronie www są pełne danych IOD?

Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 11) wprost zobowiązują podmiot, który wyznaczył IOD, by udostępnił jego dane na swojej stronie internetowej. Administrator, który wyznaczył IOD powinien opublikować jego następujące dane: imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu

tak , znajdują się tam wymagane dane IOD w zakładce RODO

2. Wnosimy o dokumentację potwierdzającą realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO)

Odnosząc się do żądania udostępnienia dokumentacji potwierdzającej realizację zadań przez IOD od dnia 25 maja 2018 r (zadań wynikających z art. 39 RODO) należy stwierdzić, że jest ono nieprecyzyjne i zbyt ogólne, a co za tym idzie nie stanowi informacji publicznej, która mogłaby być udostępniona w trybie i na zasadach przewidzianych w ustawie o dostępie do informacji publicznej.

Przywołany przez wnioskodawcę przepis art 39 RODO określa jedynie zadania inspektora ochrony danych oraz wskazuje ogólnie sposób ich realizacji. Ustawodawca wylicza wprawdzie

zadania takie jak : informowanie o obowiązkach dotyczących ochrony danych i doradzanie w tym zakresie, monitorowanie przestrzegania przepisów o ochronie danych i polityk ochrony danych, podział obowiązków, działania edukacyjne i audyty, udzielanie zaleceń co do oceny skutków dla ochrony danych i monitorowanie jej wykonania, współpracę z organem nadzorczym, pełnienie funkcji punktu kontaktowego dla organu nadzorczego i prowadzenie konsultacji z organem nadzorczym. W ust. 2 ww. przepisu ustawodawca określa sposób ogólny, w jaki inspektor ochrony danych powinien wykonywać swoje zadania. Zgodnie z tym przepisem przy wykonywaniu tych zadań inspektor powinien uwzględnić ryzyko związane z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Prawodawca unijny nie wskazuje jednak konkretnych rozwiązań w zakresie wykonywania przez IOD swoich zadań, jak i nie wskazuje rodzaju dokumentów które powinny powstać w tym procesie oraz nie przesądza czy i w jaki sposób IOD ma dokumentować powierzone mu zadania.

Dodatkowo, dokumentacja dotycząca realizacji zadań przez IOD, dotyczy m.in. realizowanych sprawdzeń, opinii dotyczących stosowanych zabezpieczeń. Dokumentacja prowadzona przez IOD zawiera zatem środki techniczne oraz organizacyjne, które mają zagwarantować ciągłą dostępność, rozliczalność oraz integralność danych. Ujawnienie tych informacji mogłoby mieć zatem negatywny wpływ na poziom bezpieczeństwa danych zapewniany przez organ do którego skierowano wniosek.

3. Czy zostały opracowane i wdrożone przepisy wewnętrzne, procedury, instrukcje i inne dokumenty dotyczące przetwarzania danych osobowych oraz bezpieczeństwa informacji. Jeśli tak to jakie?

tak zostały opracowane odpowiednie procedury.

Odnosząc się również do udostępnienia dokumentacji informuję, iż dokumenty te mają charakter wewnętrzny - organizacyjny i porządkowy i nie mogą być udostępnione w trybie ustawy o dostępie do informacji publicznej. Stanowią one dokumentację wewnętrzną wspomagającą pracę administratora i inspektora ochrony danych w zakresie wdrażania odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z przepisami rozporządzenia oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru. Z uwagi na fakt, że powyższe rejestry zawierają ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlegają ujawnianiu i powszechnemu dostępowi. Żądane rejestry nie zawierają informacji o sprawach publicznych, lecz informację o sposobie gromadzenia danych osobowych. Są więc nośnikami informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym, który ma służyć zapewnieniu m.in. porządku i bezpieczeństwa. Takie rejestry nie odnoszą się natomiast do publicznej sfery działania organu i jako takie nie zawierają informacji publicznej (patrz Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. Sygn. Akt. II SAB/Łd 181/18).

4. Wnosimy o przedłożenie dokumentu potwierdzającego zapoznanie się pracowników z treścią obowiązujących przepisów wewnętrznych, ewentualnie wskazanie w jaki sposób zostali oni zapoznani.

Odnosząc się do dokumentu, zapoznającego pracownika z dokumentacją wewnętrzną z zakresu ochrony danych osobowych, informuję, że każdy z pracowników otrzymał Regulamin Ochrony Danych Osobowych, który zawiera najważniejsze procedury obowiązujące w szkole i które pracownik składając podpis zobowiązał się znać i stosować. Dodatkowo prowadzone zostały szkolenia dla pracowników.

5. Informacje dotyczące szkoleń pracowników w zakresie ochrony danych osobowych przeprowadzanych po 25 maja 2018 roku (informacje tj. data szkolenia, zakres szkolenia, osoba prowadząca, listy obecności, czas trwania).

szkolenia przeprowadzane są co roku lub w zależności od zapotrzebowani danego działu/ zagadnienia. Ostatnie szkolenie odbyło się w III kwartale 2022r.

Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia 10 Maja 2018r.
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

6. Czy został opracowany Rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

tak został opracowany i jest aktualizowany przez IOD

7. Czy został opracowany Rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany?

tak został opracowany i aktualizowany

8. W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne

Obowiązek informacyjny o który pyta wnioskodawca realizowany jest w formie elektronicznej oraz w formie pisemnej (tradycyjnej , za pośrednictwem operatora pocztowego), w zależności od świadczonych usług.

Obowiązek informacyjny realizowany jest zgodnie z dyspozycją art. 13 i 14 RODO, a treść klauzul informacyjnych zawiera informacje w zakresie realizacji wynikających z ww. przepisów obowiązków i dotyczy czynności przetwarzania danych ujętych w rejestrze czynności przetwarzania danych.

Poniżej przekazuję linki do przykładowej klauzuli informacyjnej zamieszczonej na stronie internetowej: <https://sp4.grajewo.com/obowiazek-informacyjny/>

9. W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne.

patrz punkt 8

10. Wnosimy o regulacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.

Został opracowany regulamin monitoringu wizyjnego.

Odnosząc się również do udostępnienia dokumentacji informującej, iż dokumenty te mają charakter wewnętrzny - organizacyjny i porządkowy i nie mogą być udostępnione w trybie ustawy o dostępie do informacji publicznej. Stanowią one dokumentację wewnętrzną wspomagającą pracę administratora i inspektora ochrony danych w zakresie wdrażania odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z przepisami rozporządzenia oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru. Z uwagi na fakt, że powyższe rejestry zawierają ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlegają ujawnianiu i powszechnemu dostępowi. Żądane rejestry nie zawierają informacji o sprawach publicznych, lecz informację o sposobie gromadzenia danych osobowych. Są więc nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym, który ma służyć zapewnieniu m.in. porządku i bezpieczeństwa. Takie rejestry nie odnoszą się natomiast do publicznej sfery działania organu i jako takie nie zawierają informacji publicznej (patrz Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. Sygn. Akt. II SAB/Łd 181/18).

11. Czy IOD w ramach monitorowania przeprowadza regularne i systematyczne sprawdzenia/audyty w zakresie prawidłowości przetwarzania danych osobowych oraz przestrzegania rozporządzenia RODO, ustawy o.d.o. oraz regulacji wewnętrznych? Dokumentacja w tym zakresie (plany, sprawozdania, raporty, itp.).

Odnosząc się do audytów z zakresu prawidłowego przetwarzania danych osobowych, informuję że audyty/sprawdzenia z zakresu RODO realizowane są poprzez sprawdzenia planowe wynikające z planu sprawdzeń oraz incydentalne w przypadku zgłoszeń dokonanych przez pracowników szkoły bądź w przypadku zidentyfikowania problemów związanych z ochroną danych osobowych.

Zakres realizowanych sprawdzeń obejmuje m.in.

- kompletność zidentyfikowanych czynności przetwarzania danych osobowych,
- zakres i cel przetwarzania danych,
- przesłanki legalności przetwarzania danych osobowych, w tym danych szczególnej kategorii,
- zabezpieczenia: organizacyjne i techniczne danych osobowych,
- przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,
- powierzenie przetwarzania danych osobowych (w tym zakres i poprawność konstruowania umów powierzenia przetwarzania danych),
- obowiązek informacyjny (w zakresie realizacji).
- profilowanie,
- system informatyczny służący do przetwarzania danych osobowych.

Odnosząc się również do udostępnienia dokumentacji informującej, iż dokumenty te mają charakter wewnętrzny - organizacyjny i porządkowy i nie mogą być udostępnione w trybie

ustawy o dostępie do informacji publicznej. Stanowią one dokumentację wewnętrzną wspomagającą pracę administratora i inspektora ochrony danych w zakresie wdrażania odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z przepisami rozporządzenia oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru. Z uwagi na fakt, że powyższe rejestry zawierają ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlegają ujawnianiu i powszechnemu dostępowi. Żądane rejestry nie zawierają informacji o sprawach publicznych, lecz informację o sposobie gromadzenia danych osobowych. Są więc nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym, który ma służyć zapewnieniu m.in. porządku i bezpieczeństwa. Takie rejestry nie odnoszą się natomiast do publicznej sfery działania organu i jako takie nie zawierają informacji publicznej (patrz Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. Sygn. Akt. II SAB/Łd 181/18).

Przedmiotowy wniosek/wnioski - nie powinny być rozpatrywane w trybie KPA. Urząd powinien procedować nasze wnioski W TRYBIE Ustawy o dostępie do informacji publicznej

Pozwalamy sobie również przypomnieć, zgodnie z 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.

12. W trybie dostępu do informacji publicznej – zwracamy się z prośbą o informację, czy w związku z monitoringiem wizyjnym miejsc publicznych prowadzonym przez Państwa jednostkę była prowadzona była ocena skutków w rozumieniu art. 35 ust. 1 rodo stosownie do treści tego przepisu:

„Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę”.

tak była przeprowadzana ocena skutków dla ryzyka

2. W Wojewódzkim Sądzie Administracyjnym w Warszawie odbyła się 26 sierpnia 2020 r. rozprawa w sprawie skargi Burmistrza Aleksandrowa Kujawskiego na decyzję Prezesa Urzędu nakładającą administracyjną karę pieniężną. WSA oddalił skargę.

WSA rozpatrywał skargę Burmistrza Aleksandrowa Kujawskiego na decyzje Prezesa UODO z 18 października 2019 r. w związku z przetwarzaniem przez Burmistrza danych osobowych w Biuletynie Informacji Publicznej.

Przypomnijmy, że jednym z powodów nałożenia kary w wysokości 40 tys. zł na Burmistrza miasta było to, że nie zawarł umowy powierzenia przetwarzania danych osobowych z podmiotami, którym przekazywał dane. **Ponadto, w decyzji Prezes UODO zarzucił brak procedur wewnętrznych dotyczących przeglądu zasobów dostępnych w BIP pod kątem ustalenia okresu ich publikowania.** To

spowodowało, że przykładowo w BIP były dostępne m.in. oświadczenia majątkowe z 2010 roku, podczas gdy okres ich przechowywania wynosi 6 lat, co wynika z przepisów sektorowych.

Sąd na rozprawie oddalił skargę Burmistrza. W uzasadnieniu wyroku sąd wskazał, że nie znajduje podstaw do uchylenia zaskarżonej decyzji. Zdaniem sądu Prezes UODO prawidłowo zastosował przepisy ogólnego rozporządzenia o ochronie danych osobowych. Sąd także podkreślił, że RODO ma zastosowanie do danych przetwarzanych w BIP.

Ponadto WSA uznał, że organ nadzorczy w sposób wyczerpujący w wydanej decyzji uzasadnił zajęte stanowisko i wysokość nałożonej kary.

W ocenie sądu nałożona na Burmistrza kara nie stanowi nadmiernego obciążenia dla organu i jest adekwatna do stwierdzonych naruszeń w obszarze przetwarzania danych.

Więcej o decyzji Prezesa UODO o nałożeniu kary w komunikacie dostępnym pod linkiem:
<https://uodo.gov.pl/pl/138/1240>

13. Mając na uwadze powyższe wnosimy o informację czy została opracowana polityka retencji danych? Jakich czynności ona dotyczy?

Retencja danych osobowych odbywa się według przyjętych przepisów i procedur wewnętrznych Szkoły oraz obowiązków nakładanych przez przepisy prawa np. Ustawa o archiwizacji dokumentów.

14. PREAMBUŁA WNIOSKU O INFORMACJĘ PUBLICZNĄ W ZAKRESIE KWALIFIKACJI IOD W ZWIĄZKU Z RAPORTEM <https://www.nik.gov.pl/kontrola/P/19/007/>

GDZIE STWIERDZONO, ŻE W WIELU PODMIOTACH IOD NIE POSIADA ODPOWIEDNICH KWALIFIKACJI ORAZ STWIERDZONO KONFLIKTY INTERESÓW

Art 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Według UODO Karami administracyjnymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych dotyczące także wyznaczania IOD. To na administratorze spoczywa ciężar wyznaczenia IOD zgodnie z kwalifikacjami i wiedzą prawniczą: <https://uodo.gov.pl/pl/225/637>

Jednakże warto zrealizować rekonesans - w tym obszarze i dokonać stosownej analizy - wykazując troskę o bezpieczeństwo danych oraz wydatkowanie środków publicznych na IOD zgodnie z kwalifikacjami. Tymczasem często na IOD są wybierani osoby nie mające kwalifikacji, wiedzy prawnej. Co gorsza często takie funkcje piastują osoby z wykształceniem informatycznym.

Dzięki kontrolom NIK i UODO oraz działaniom sfer Rządowych (w skali makro) w ostatnim czasie sytuacja ulega poprawie, jednakże bez szybkiej sanacji tego obszaru (w skali mikro) również w Gminach i jednostkach oświatowych

- proces ten będzie w dalszym ciągu przebiegał zbyt wolno -często są to osoby przypadkowe lub informatycy, zewnątrzni IOD nie mający wiedzy prawniczej.
W związku z powyższym:

I Wniosek:

1.1) Na mocy art. 61 Konstytucji RP, w trybie inter alia: art. 6 ust. 1 pkt 3 lit. f, art. 6 ust. 1 pkt 5 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - wnosimy o udzielenie informacji publicznej w przedmiocie :

Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej?

IOD nie jest prawnikiem.

Inspektor Danych Osobowych ma niezbędną wiedzę i odpowiednie kwalifikacje do pełnienia tej funkcji - świadczą o tym przedłożone dla Administratora Danych dyplomy, certyfikaty i przebyte kursy szkoleniowe:

- ukończone studia podyplomowe z zakresu bezpieczeństwa i ochrony danych osobowych w sektorze publicznym -2018r
- certyfikat kompetencji IOD - ekspert dokumentowania systemu ochrony danych osobowych - 2018r
- certyfikat kompetencji IOD - ekspert stosowania przepisów RODO i zarządzania systemem ochrony danych osobowych 2018r
- certyfikat kompetencji IOD & Specjalisty ds. Ochrony Danych Osobowych 2020 r.
- ukończone szkolenie: audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg EN ISO/IEC 27001:2017

Czy IOD jest prawnikiem? Jakie posiada doświadczenie?
Kto i w jaki sposób weryfikował kwalifikacje IOD?

IOD nie jest prawnikiem - kwalifikacje weryfikował Administrator

W jaki sposób odbywają się systematyczne szkolenia pracowników prowadzone przez IOD. Proszę wskazać, kiedy miały one miejsce oraz zakres szkolenia – pomijając ogólny instruktaż i zapoznanie się z przepisami dot. ochrony danych.

IOD w ramach umowy przeprowadza szkolenie wstępne, ogólne pod kątem RODO dla wszystkich pracowników oraz bardziej szczegółowe dla konkretnych, kluczowych działów/ stanowisk w Szkole (kadry, księgowość itp.). IOD przeprowadza również szkolenie dla każdego nowego przyjętego pracownika. Osoby przeszkolone potwierdzają swój udział poprzez złożenie podpisu na liście szkoleniowej. Pierwsze Szkolenie miało miejsce w czerwcu 2018 roku, od tego czasu szkoleniu podlegały osoby nowoprzyjęte do pracy w Szkole.

Czy na bieżąco przekazywane są IOD do akceptacji pod względem prawidłowości w zakresie ochrony danych osobowych projekty dokumentów tj. projekty umów, informacji udostępnianych w Biuletynie Informacji Publicznych, projekty przepisów wewnętrznych związanych z udostępnianiem bądź pozyskiwaniem danych osobowych.

Tak

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 i kwalifikacji IOD a zwłaszcza doświadczenia i wiedzy prawniczej wydaje się (jak wynika z uprzednio uzyskanych przez nas odpowiedzi) - szczególnie wymagać - wdrożenia procedur aby takie „przypadkowe” osoby nie pełniły takich funkcji.

Pozostałe pytania:

1. Czy podmiot prowadzi BIP i pod jakim adresem internetowym

Tak, www.sp4.grajewo.com/bip-sp-4/

2. Z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub www.bip.edu.pl czy inny (podać jaki)?

Nie dotyczy

3. Jakie są umowne okresy świadczenia tej usługi. Jaka jest wartość umów brutto w poszczególnych okresach? Dane odrębnie za poszczególne okresy w latach 2017-do czerwca 2022.

Nie dotyczy

4. Proszę podać liczbę informacji publicznych opublikowanych w BIP w latach 2017-do czerwca 2022r.

<https://sp4.grajewo.com/bip-sp-4/>

5. 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 Dane odrębnie za rok 2017, 2018, 2019, 2020, 2021.

<https://sp4.grajewo.com/bip-sp-4/>

6. Wnosimy o udostępnienie wszystkich wniosków o informację publiczną na stronie BIP

<https://sp4.grajewo.com/bip-sp-4/>

7. Wnosimy o udostępnienie wszystkich wniosków o informację publiczną jako informację publiczną w latach 2016 do czerwca 2022r.

<https://sp4.grajewo.com/bip-sp-4/>

8. Wnosimy o udostępnienie informacji publicznej w zakresie ilości dni urlopu wypoczynkowego pozostałych do wykorzystania kierownikowi jednostki oraz poszczególnym zastępcom (jeśli są) także, czy w tym roku któreś z tych osób został lub zostanie wypłacony ekwiwalent za niewykorzystany urlop (jeśli tak w jakiej kwocie i komu).

Dyrektor szkoły - 10 dni

Wicedyrektor szkoły - 21 dni

Wicedyrektor szkoły- 14 dni

Nie zostanie wypłacony ekwiwalent.

Celem zachowania pełnej przejrzystości działań - wnosimy o opublikowanie treści wnioski na stronie internetowej podmiotu wraz z odpowiedziami i uchybieniami na podstawie art. 8 ust. 1 ww. Ustawy o petycjach Chcemy działać w pełni jawnie i transparentnie.

Każdy Podmiot mający styczność z Urzędem - ma prawo i obowiązek - usprawniać struktury administracji samorządowej

Pozwalamy jeszcze raz 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.

Celem naszych wniosków jest - sensu largo - usprawnienie, naprawa - na miarę istniejących możliwości - funkcjonowania struktur Administracji Publicznej - głównie w Gminach/Miastach/szkołach' jednostkach podległych - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych.

PYTANIA Z KRAJOWYCH RAM INTEROPERACYJNOŚCI

Zgodnie z Rozporządzeniem R. M. z dnia 12 kwietnia 2012 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 2012r. poz. 526) "każdy podmiot publiczny zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust.2 pkt 14). "

Pytania informacja publiczna?

1. Kto dokonuje corocznych audytów z KRI?

IOD dokonuje corocznych audytów w zakresie przestrzegania zasad i przepisów ochrony danych osobowych.

2. Czy IOD realizuje zadania w związku z KRIO?

IOD wykonuje te zadania w zakresie przestrzegania zasad i przepisów ochrony danych osobowych (w corocznym audycie znajdują się zagadnienia z KRI)

3. Kto przeprowadza audyt bezpieczeństwa?

IOD dokonuje corocznych audytów w zakresie przestrzegania zasad i przepisów ochrony danych osobowych.

Wewnętrzną kontrolę stanu bezpieczeństwa danych osobowych i przestrzegania zasad i przepisów z zakresu ochrony danych osobowych powinien regularnie, w przyjęty przez siebie sposób, przeprowadzać **inspektor ochrony danych**.

Podstawa:

- rozporządzenie Rady Ministrów z 12 kwietnia 2012 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 2012 r. poz. 526)

Pytania informacja publiczna:

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 KONTROLUJĘ EWIDENCJĘ	tak		wyznaczona osoba przez administratora
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	tak		wyznaczona osoba przez administratora
	c) umów serwisowych?	tak		-
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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W	tak		audyt przeprowadzany jest raz w roku w ustalonym z administratorem terminie
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	tak		wyznaczona osoba przez administratora

	ZOSTAŁO 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 EWIDENCJĘ		nie	
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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W		nie	zgodnie z Instrukcją zarządzania RODO
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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			nie dotyczy
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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			nie dotyczy
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? <i>Jeśli TAK proszę o ich wskazanie</i>		tak	
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W		tak	
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? CZY IOD W TYM ZAKRESIE		tak	

	<i>PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>			
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?	tak		
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	tak		
<p>Podjęmowanie 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.</p>				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i> Jeśli TAK proszę o przedłożenie dokumentu.	tak		
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	tak		
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	tak		
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	tak		

5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?			zgodnie z procedurą nadawania haseł
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	tak		
7.	Czy prowadzona jest formalna lista zadań /obowiązków /uprawnień takich osób? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	tak		
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).			nie dotyczy
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:			
a.	ochrona sieci na poziomie portów LAN	tak		
b.	BIOS		nie	
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows		nie	
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>		nie	
e.	system ochrony zewnętrznej klasy firewall	tak		
f.			nie	

	system ochrony zewnętrznego dostępu logicznego (urządzenie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;			
g.	stosowanie tokenów z hasłami jednorazowymi		nie	
<p>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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY</p>				
1.	<p>Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość?</p> <p><i>Jeśli TAK proszę o przedłożenie dokumentu</i></p>	tak		regulamin pracy zdalnej
2.	<p>Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT?</p> <p><i>Jeśli TAK proszę o udokumentowanie.</i></p>	tak		
3.	<p>Czy w pracy na odległość stosują bezpieczne metody połączenia?</p>	tak		
4.	<p>Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?</p>	tak		
5.	<p>Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)?</p> <p><i>Jeśli TAK proszę wskazać, w jaki sposób.</i></p>	tak		kopie danych
<p>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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</p>				
1.	<p>Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w</p>	tak		

	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)?			nie dotyczy
<p>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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?</p>				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych?	tak		
	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)?			nie dotyczy
3.	Czy istnieją możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			nie dotyczy
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?			nie dotyczy
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			nie dotyczy
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		nie	
<p>Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W</p>				
1.		tak		

	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?			nie dotyczy
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	tak		
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?	tak		
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?		nie	
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	tak		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?	tak		
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?	tak		e-mail - szyfrowane połączenie
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	tak		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?	tak		
11.	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	tak		
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?	tak		
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?		nie	
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)?	tak		

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?	tak		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	tak		podczas corocznego audytu

Czy jedynym kryterium wyboru dla IOD i innych usług bezpieczeństwa informacji niezależnie od formy świadczenia tych usługi jest cena? Jeśli tak to prosimy o wyjaśnienie czy w związku z tym oznacza to, że ochrona informacji ma niski priorytet w zarządzaniu Państwa organizacją?

Jeśli nie, to jakie inne kryteria Państwo stosujecie i z jaką wagą. Prosimy o uszczegółowienie tej kwestii.

NIE.

Kryterium wyboru IOD były kwalifikacje, kompetencje jakie posiada osoba wybrana na stanowisko IOD w naszej placówce.

Czy Państwa jednostka organizacyjna wdrożyła wewnętrzną procedurę schematów podatkowych (MDR – Mandatory Disclosure Rules), zgodnie z wymaganiami ustawy ordynacja podatkowa ?

TAK.

Pozwalamy sobie również przypomnieć, zgodnie z 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

Jednym z trybów udostępniania informacji publicznej jest jej udostępnianie na wniosek. Wniosek o udostępnienie informacji publicznej może złożyć każdy, jego przekazanie nie nakłada jednak na adresata obowiązku automatycznego udzielenia informacji publicznej. Jest to możliwe dopiero po weryfikacji, że w danym przypadku spełniono zakres podmiotowy i przedmiotowy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, w tym w odniesieniu do wnioskowego trybu udostępniania informacji, a jeśli tak, konieczna jest dodatkowo analiza występowania ustawowych przesłanek ograniczenia dostępu do informacji publicznej.

Jeżeli w danym przypadku mają zastosowanie przepisy u.d.i.p. dotyczące udzielania informacji na wniosek, a jednocześnie nie występują przesłanki ograniczenia dostępu do informacji publicznej, o których mowa w art. 5 ust. 1, 2 i 2a u.d.i.p., i żądana informacja nie jest informacją przetworzoną (lub jej udzielenie jest szczególnie istotne dla interesu publicznego), **podmiot zobowiązany udostępnić informację publiczną. Następuje to w formie czynności materialno-technicznej zgodnie z art. 10 i 12 u.d.i.p. Odmowa udostępnienia informacji publicznej ze względu na jedną z przesłanek ograniczających jawność (ochrona informacji niejawnych, informacji o postępowaniu restrukturyzacyjnym przed jego zakończeniem i innych tajemnic ustawowo chronionych, tajemnica przedsiębiorcy, prawo do prywatności) bądź odmowa udostępnienia informacji przetworzonej, jeżeli za jej udostępnieniem nie przemawia szczególnie istotny interes publiczny, wymaga natomiast zastosowania formy decyzji, do której stosuje się przepisy kodeksu postępowania administracyjnego (por. art. 16 i 17 w zw. z art. 5 u.d.i.p.).**

W przypadku postępowania wszczynanego na wniosek mamy zatem do czynienia w istocie z dwoma postępowaniami o różnym charakterze i dwiema sprawami administracyjnymi. Pierwsze z nich dotyczy udzielenia informacji publicznej, tj. dokonania czynności materialno-technicznej i nie toczy się w trybie k.p.a., a u.d.i.p. reguluje tylko niektóre jego aspekty (np. formę wniosku, termin, opłaty). Drugie zaś jest postępowaniem w sprawie odmowy udostępnienia informacji prowadzonym w trybie k.p.a., które kończy się decyzją administracyjną (por. M. Jaśkowska, *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002, s. 59–60).

Uzasadnienie

Nie ulega wątpliwości, że żądane informacje o które wnioskuje Wnioskodawca stanowią informację publiczną, nie mającą charakteru informacji przetworzonej.

Jak wynika z ugruntowanej linii orzeczniczej sądów administracyjnych (m.in. wyrok Wojewódzkiego Sądu Administracyjnego w Opolu z dnia 22 sierpnia 2018 r.; II SA/Op 334/18) informację publiczną stanowią w szczególności materiały dokumentujące fakt lub sposób zadysponowania majątkiem publicznym, w tym treść i postać umów cywilnoprawnych dotyczących takiego majątku. Tym samym umowy cywilnoprawne z podmiotami wskazanymi w art. 4 ust. 1 ustawy są informacją publiczną.

Z kolei, jak przyjmuje się w orzecznictwie, informacją publiczną przetworzoną jest informacja, która w chwili złożenia wniosku w zasadzie nie istnieje w kształcie objętym wnioskiem, a niezbędnym, podstawowym warunkiem jej wytworzenia jest przeprowadzenie przez podmiot zobowiązany pewnych czynności analitycznych, organizacyjnych i intelektualnych w oparciu o posiadane

informacje proste. Inaczej mówiąc udostępnienie żądanej informacji nie stanowi tylko technicznego przeniesienia danych, lecz wymaga potrzeby przeprowadzenia odpowiednich analiz, obliczeń, zestawień, wyciągów, czy usuwania danych chronionych prawem, które to zabiegi czynią informacje proste, informacją przetworzoną. Informacja przetworzona, to informacja, którą podmiot zobowiązany na dzień złożenia wniosku nie dysponuje (nie posiada gotowej informacji odpowiadającej żądaniu) w związku z czym, jej udostępnienie wymaga podjęcia dodatkowych czynności połączonych zsignięciem do dokumentacji źródłowej oraz zaangażowaniem do tych czynności określonych środków osobowych i finansowych, której wytworzenie wymaga intelektualnego zaangażowania. Informacja przetworzona jest więc jakościowo nową informacją powstałą w wyniku czynności technicznych i określonego działania intelektualnego na zbiorze informacji prostych już znajdujących się w posiadaniu podmiotu zobowiązanego, przygotowaną specjalnie dla wnioskodawcy według wskazanych przez niego kryteriów.

Ponadto, od przetworzenia informacji należy odróżnić proces "przekształcenia", który jest jedynie technicznym zabiegiem, w wyniku którego zewnętrzna forma informacji prostej ulega przekształceniu, zgodnie z wnioskiem strony, głównie poprzez wykonanie kserokopii czy też sporządzenie skanu treści dokumentu. (por. wyrok WSA w Opolu z dnia 28 września 2017 r., sygn. akt II SA/Op 446/17).

Sama natomiast konieczność odnalezienia odpowiednich dokumentów (w tym wielostronicowych umów), a także dokonanie ich analizy w celu wyselekcjonowania żądanych danych, wykonanie kopii, dokonanie anonimizacji danych prawnie chronionych i związany z tym nakład pracy nie prowadzi jeszcze do wytworzenia nowej jakościowo informacji i nie czyni z informacji prostej informacji przetworzonej. Są to zwykle zabiegi związane z procesem udostępniania informacji publicznej.

Biorąc pod uwagę powyższe, nie ulega wątpliwości, że zamawiający dysponuje wnioskowanymi informacjami, a te podlegają udostępnieniu. Powyższe informacje związane są z prowadzeniem postępowań o udzielenie zamówienia lub realizacją umów o udzielenie zamówienia publicznego. Są

wynikiem realizacji tych umów i stanowią typowe informacje, które organ administracji publicznej jest zobowiązany do przechowywania.

Jednocześnie chciałbym zaznaczyć, że na podstawie udzielanych przez Państwa informacji powstała i już działa ogólnopolska baza. Brak udostępnienia danych będzie skutkowało skierowaniem spraw do sądu na bezczynność.