[redacted]

Od: [redacted]
Wysłano: środa, 23 listopada 2022 16:01
Do: [redacted]
Temat: odpowiedź na wniosek o udostępnie informacji publicznej z 10.11.2022 - 1

Stalowa Wola dnia 16.11.2022 r.

178/11/22/MZK

[redacted]
Adresy e-mail:
[redacted]

W odpowiedzi na Wniosek o udzielenie informacji publicznej z dnia 10.11.2022 r. wyjaśniamy co następuje:

W naszej ocenie zdecydowana większość zadanych przez Pana pytań nie mieści się w definicji informacji publicznej o której mowa w art. 6 ustawy z dnia 06.09.2001 r. – o dostępie do informacji publicznej. Nadmieniamy, że otrzymaliśmy sygnał od firmy bezpieczne – dane, że nie jest Pan ich pracownikiem i „podszywa się pod jej adres e-mail".

Niezależnie od tego informujemy, że wniosek z identycznymi pytaniami otrzymaliśmy również od innej osoby co wskazuje, że przeciwko naszej spółce prowadzona jest zmasowana akcja nękająca.

Obawiamy się, że Pana wystąpienie nie służy dobru publicznemu, ale interesom prywatnym których treści się domyślamy. Nie pozwolimy się szantażować.

W przypadku kolejnego wystąpienia uznamy to za nękanie i poinformujemy o tym fakcie organy ścigania oraz zaangażujemy renomowaną kancelarię prawną do ochrony naszych interesów.

Duża ilość zadanych pytań angażuje znaczne siły i środki po naszej stronie.

Informacja publiczna powinna stwarzać realną możliwość wykorzystania uzyskanych danych dla poprawy funkcjonowania organów administracji i lepszej ochrony interesu publicznego (Wyrok NSA z 07.12.2011 r., I OSK 1737/1).

Jeśli wnioskodawca nie wykaże, że uzyskanie danej informacji publicznej jest szczególnie istotne dla interesu publicznego – a taką sytuację mamy w przedmiotowej sprawie, są podstawy do odmowy udzielenia tej informacji na podstawie przepisu art. 16 ust. 1 cyt. ustawy o dostępie do informacji publicznej (wyrok NSA 11.09.2012r., I OSK 1015/12).

W odniesieniu do zadanych pytań zajmujemy następujące stanowisko:

W uzasadnieniu wniosku o udzielenie informacji publicznej jako podstawa prawna żądania wskazywany jest Wyrok WSA w Warszawie z dnia 30.05.2017 r. (sygn. II SAB/Wa 10/17) powołujący się na art. 139 ust. 3 ustawy prawo o zamówieniach publicznych.

Informujemy że przepis ten zawarty był w ustawie z dnia 29.01.2004 r. – Prawo zamówień publicznych. Ustawa ta obowiązywała do dnia 31.12.2020 r. i z tym dniem utraciła moc prawną bowiem weszła w życie nowa ustawa z dnia 11.09.2019 r. – Prawo zamówień publicznych. Wprawdzie art. 18 nowej ustawy Prawo zamówień publicznych wprowadza zasadę,
że postępowanie o udzielenie zamówienia jest jawne ale dodatkowo wprowadza ograniczony dostęp do informacji i zakaz ujawniania tajemnicy przedsiębiorstwa. Ustawodawca nie uznał za konieczne wprowadzenie do nowej ustawy analogicznego przepisu zawartego
w art. 139 ust. 3 poprzednio obowiązującej ustawy z dnia 29.01.2004 r. – Prawo zamówień publicznych mówiącego o tym, że 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. Nie ma więc prawnego obowiązku przekazywania do wiadomości innym podmiotom umów zawartych w ramach zamówień publicznych.
Takiego obowiązku co do zasady nie można doszukać się w zakresie pozostałych umów cywilnoprawnych a nie tylko tych zawieranych w ramach zamówień publicznych.
Nadmieniamy też że zgodnie z art. 448 ustawy z dnia 11.09.2019 r. – Prawo zamówień publicznych zamawiający są zobowiązani do zamieszczania w biuletynie zamówień publicznych ogłoszeń po wykonaniu umowy.
W tej sytuacji brak jest podstaw prawnych do pozytywnego uwzględnienia Pana wniosku
o przesłanie skanów wszystkich umów cywilnoprawnych zawartych przez jednostkę w okresie od 2018 r. do końca czerwca 2022 r.
Nie wiemy też, jakie dobro publiczne chciałby Pan wspierać poprzez zgromadzenie wszystkich umów cywilnoprawnych zawartych przez naszą Spółkę w wymienionym okresie a jest ich niemało.
Zwracamy nadto uwagę, że Pańskie wystąpienie jest nie usystematyzowane, mało czytelne przez co znacznie utrudnia jego zrozumienie i przygotowanie odpowiedzi.
Odnośnie pozostałych wniosków zawartych w Pana wystąpieniu informujemy:

I WNIOSEK INFORMACJA PUBLICZNA
Wniosek informacja publiczna zawarte umowy cywilnoprawne
WNOSIMY O SKANY WSZYSTKICH UMÓW CYWILNOPRAWNYCH ZAWARTYCH PRZEZ JEDNOSTKĘ W OKRESIE 2018 do końca czerwca 2022r.
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**,,.

ZAPYTANIE

PREAMBUŁA WNIOSKU O INFORMACJĘ PUBLICZNĄ

Wnioskodawca jest świadomy, że nie zawsze administrator zna przepisy RODO, jednak to na nim spoczywa obowiązek wyboru INSPEKTORA OCHRONY DANYCH ZGODNIE Z KWALIFIKACJAMI.
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 prawniczej. Co gorsza często takie funkcje piastują osoby z wykształceniem informatycznym.
Media i UODO donoszą o sytuacjach typu - vide - http://www.tvp.info/35; **(Materiał TVP info z 2019 r.)**
Powyższe informacje utwierdzają nas w tym, że sanacja i wydatkowanie pieniędzy podatników w tym obszarze wydaje się niezbędne, ale wyłącznie na osoby mające odpowiednie kwalifikacje zgodnie z rzeczonym art. 37 ust. 5 RODO.
Zdaniem Wnioskodawcy:
Dzięki działaniom sfer Rządowych (w skali makro) w ostatnim czasie sytuacja ulega poprawie, jednakże bez szybkiej sanacji tego obszaru (w skali mikro) również w Gminach
- proces ten będzie w dalszym ciągu przebiegał zbyt wolno -często są to osoby przypadkowe lub informatycy, zewnętrzni 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 udzielnie informacji publicznej w przedmiocie :
Po analizie jednostek :

- Jeśli odpowiedź jest twierdząca wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej?

Odpowiedź: W odpowiedzi na Pana pytanie informujemy, że zgodnie z 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.
Zgodnie z art. 39 RODO Inspektor Ochrony Danych ma następujące zadania:
a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych
i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie

ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
d) współpraca z organem nadzorczym;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
2.Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
W odpowiedzi na zadane pytanie informujemy, że Pana stwierdzenie dotyczące wiedzy prawniczej IOD cyt." *To na administratorze spoczywa ciężar wyznaczenia IOD zgodnie z kwalifikacjami* ***i wiedzą prawniczą",*** wprowadza w błąd, ponieważ jak już wcześniej informowaliśmy, zgodnie z 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, co nie oznacza, że IOD powinien posiadać wykształcenie stricte prawnicze, lecz powinien wykazać się fachową wiedzą na temat prawa.
Potwierdzeniem naszego stanowiska jest stanowisko Prezesa UODO z dnia 07.01. 2019r., zamieszczonego na stornie Urzędu Ochrony Danych Osobowych, pod adresem: https://uodo.gov.pl/pl/223/612, cytujemy: *„W jaki sposób należy oceniać kwalifikacje osoby kandydującej do pełnienia funkcji IOD?*
IOD 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.

Wymagany od inspektora poziom wiedzy fachowej nie jest jednoznacznie określony, ale zgodnie z Wytycznymi dotyczącymi IOD musi być on współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Wyższy poziom wiedzy powinien być wymagany np. w przypadku:

- *wyjątkowo skomplikowanych procesów przetwarzania,*
- *przetwarzania dużej ilości danych szczególnych kategorii,*
- *podmiotów regularnie przekazujących dane do państw trzecich.*

IOD powinien mieć odpowiednią wiedzę z zakresu krajowych, europejskich oraz sektorowych przepisów i praktyk w zakresie ochrony danych osobowych, a także dogłębną znajomość RODO. Jednocześnie powinien posiadać odpowiednią wiedzę na temat:

- *procesów przetwarzania, systemów informatycznych oraz zabezpieczeń stosowanych u administratora,*
- *sektora, w którym działa administrator,*
- *procedur administracyjnych i funkcjonowania jednostki*

Jeśli chodzi o osobiste cechy IOD kwalifikujące go do wykonywania funkcji, to są to: rzetelne podejście i wysoki poziom etyki zawodowej.

Ocena kompetencji osoby do wykonywania zadań wymaga uwzględnienia charakteru i zakresu zadań inspektora. Zgodnie z przepisami RODO, inspektor będzie miał m.in. obowiązek identyfikowania poszczególnych obowiązków ciążących na mocy RODO na administratorze (w tym kierownictwie i wszystkich osobach przetwarzających dane) oraz podmiocie przetwarzającym (w tym kierownictwie i wszystkich osobach przetwarzających dane osobowe), informowania o nich oraz doradzania w zakresie tych obowiązków. Specjalnego merytorycznego przygotowania wymaga udzielanie administratorowi i podmiotowi przetwarzającemu zaleceń co do oceny skutków dla ochrony danych (więcej

na temat roli inspektora w ocenie skutków dla ochrony danych w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (DPO) oraz w Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych). Ważnym zadaniem IOD jest obowiązek pełnienia roli punktu kontaktowego dla organu nadzorczego i punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO)

Grupa Robocza Art. 29 w Wytycznych dotyczących inspektorów ochrony danych (DPO)w odniesieniu do umiejętności wykonywania zadań inspektora wskazuje, że priorytetem dla niego powinno być zapewnienie przestrzegania RODO. IOD ma zatem odgrywać kluczową rolę w zakresie wspierania „kultury ochrony danych" oraz pomagać w implementacji niezbędnych elementów RODO, tj.:

- *zasad przetwarzania danych osobowych,*
- *praw osób, których dane dotyczą,*
- *ochrony danych w fazie projektowania oraz domyślnej ochrony danych,*
- *rejestru czynności przetwarzania,*
- *wymogów bezpieczeństwa przetwarzania,*
- *zgłaszania naruszeń.*

Znaczenie fachowej wiedzy w zakresie prawa i praktyki zostało dodatkowo podkreślone przez zobowiązanie administratorów i podmiotów przetwarzających do zapewnienia IOD zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy (art. 38 ust. 2 RODO). Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest uzasadniony wobec zmieniającego się stale stanu wiedzy technicznej, rozwoju technologicznego i postępu wielkoskalowych metod przetwarzania danych.

IOD powinien kształcić się, rozwijać swoje doświadczenia i umiejętności w różnych formach edukacyjnych, a możliwość powołania się na wskazany art. 38 ust. 2 RODO może być mu bardzo pomocny w uzyskaniu niezbędnych na to środków finansowych.

Mimo, iż RODO bardzo mocno akcentuje wymóg wiedzy i fachowości IOD, nie reguluje zasad czy trybu weryfikacji spełnienia tego wymogu. Niemniej certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora niewątpliwie w większości przypadków będą ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej do pełnienia tej funkcji."

W związku z powyższym wyjaśnieniem, informujemy, że IOD 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.

- Kto weryfikował kwalifikacje IOD przed podpisaniem umowy?

Odpowiedź – Prezes Miejskiego Zakładu Komunalnego Sp. z o. o. w Stalowej Woli poprzez przeprowadzoną rozmowę oraz zapoznanie się z dokumentacją potwierdzającą kwalifikację Inspektora Ochrony Danych.

- Przypominamy, że funkcją IOD dotyczy osoby fizycznej i konkretna osoba musi się legitymować odpowiednimi kwalifikacjami (wiedza praktyczna i prawnicza).

3. Dane osobowe będą przetwarzane w celu realizacji obowiązków prawnych ciążących na Administratorze.

- 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.

Odpowiedź: Szkolenia prowadzone są w formie bezpośredniej - indywidulanej lub grupowej, odbywają się cyklicznie. Ostatnie szkolenia odbyły się w 2022 roku, zakres szkoleń dotyczących ochrony danych osobowych odbywa się według planu szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych i obejmował miedzy innymi: legalność przetwarzania danych osobowych, realizacja obowiązku

informacyjnego, postępowanie
w przypadku wystąpienia incydentu, bezpieczne użytkowanie sprzętu IT, bezpieczne korzystanie z Internetu, zabezpieczenia fizyczne obszarów przetwarzania.

- 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.

Odpowiedź: TAK

§1.2) Dodatkowo, w kontekście pytania - w trybie wyżej powołanych przepisów
- wnosimy o :
- wyszczególnienie szkoleń jakie iod przeprowadził w podmiocie (data, plan, czas trwania, podpisy)

Odpowiedź: IOD przeprowadzał szkolenia wstępne pracowników oraz szkolenia cykliczne według planu szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych.
Czas trwania szkoleń: od 2-5 godzin.
Daty szkoleń:

a) 2019 – 13. 02, 22.03, 15.05, 06,06;
b) 2020 – 03.02, 02.03, 03.07, 15.07;
c) 2021 – 26.01, 01.10;
d) 2022 – 31.01, 01.03, 10.03, 22.03, 10.05, 02.06, 03.06, 09.06, 14.06, 20.06, 12.07, 18.07, 02.08, 09.08, 02.09, 04.10, 08.11.

Prosimy o doprecyzowanie we wniosku kwestii „podpisów" – co mamy rozumieć pod hasłem „podpisy"?
-czy posiadacie dyplomy z wykształcenia prawniczego IOD?

Odpowiedź: Informujemy, że IOD 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, co nie oznacza, że powinien posiadać wykształcenie prawnicze.

Stan na dzień złożenia niniejszego wniosku – dotyczący 2019 -2022r.

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**.** Według UODO działanie polegające na wysyłaniu zdalnie raportów i dostęp do folderów jednakowych dla wszystkich podmiotów jest nieprawidłowe.

II - Petycja Odrębna

- procedowana w trybie Ustawy o petycjach (Dz.U.2018.870 t.j. z dnia 2018.05.10)

§1P) Wnosimy - w trybie Ustawy o petycjach (Dz.U.2018.870 t.j. z dnia 2018.05.10) - o opublikowanie w Podmiotowej Stronie Biuletynu Informacji Publicznej – wniosku oraz odpowiedzi na nasze pytania.
Wnosimy o wskazanie wiedzy prawniczej IOD. Wnosimy o zmianę IOD na osobę z kwalifikacjami o których mowa w art. 37 ust.5 RODO .

§2P) **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 .Chcemy działać w pełni jawnie i transparentnie.**
Każdy Podmiot mający styczność z Urzędem - ma prawo i obowiązek - usprawniać struktury administracji samorządowej I MY TO CZYNIMY.
Nazwa Wnioskodawca - jest dla uproszczenia stosowna jako synonim nazwy "Podmiot Wnoszący Petycję" - w rozumieniu art. 4 ust. 4 Ustawy o petycjach (Dz.U.2014.1195 z dnia 2014.09.05)
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.

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

II. WNIOSEK

WNIOSEK INFORMACJA PUBLICZNA

Na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (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 - głownie 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

Odpowiedź: TAK

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

Odpowiedź:

Zgodnie z wytycznymi IOD podejmuje następujące działania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

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

Odpowiedź: TAK – Polityka Ochrony Danych Osobowych Miejskiego Zakładu Komunalnego Sp. z o.o. w Stalowej Woli, w tym Instrukcja Zarządzania Systemami Informatycznymi służącymi do przetwarzania danych osobowych w MZK Sp. z o. w Stalowej Woli, Instrukcja postępowania z kluczami oraz zabezpieczenia budynków i pomieszczeń MZK Sp. z o. o.
w Stalowej Woli wraz z pozostałymi załącznikami.

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

Odpowiedź: Pracownicy zostają zapoznani z treścią obowiązujących przepisów wewnętrznych zgodnie z wewnętrznymi zasadami przyjętymi przez Spółkę.

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 prowadził IOD.

a) 2018 – 28.05, 03.07, 05.10, 09.10;
b) 2019 – 13. 02, 22.03, 15.05, 06,06;
c) 2020 – 03.02, 02.03, 03.07, 15.07;
d) 2021 – 26.01, 01.10;
e) 2022 – 31.01, 01.03, 10.03, 22.03, 10.05, 02.06, 03.06, 09.06, 14.06, 20.06, 12.07, 18.07, 02.08, 09.08, 02.09, 04.10, 08.11.

Zakres szkoleń: ochrona danych osobowych.
Czas trwania szkoleń: od 2-5 godzin.
Żądane natomiast przez Pana listy obecności nie stanowią informacji publicznej i nie podlegają udostępnieniu w myśl ustawy o dostępie do informacji publicznej. Dokumenty te (listy obecności) nie zawierają danych publicznych i związane są z aktywnością organu związaną z wewnętrzną organizacją jego funkcjonowania. Mają charakter wyłącznie organizacyjny oraz porządkowy i stanowią jeden ze sposobów dokumentowania odbycia przez pracownika szkoleń.

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

Odpowiedź: TAK

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

Odpowiedź: TAK

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

Odpowiedź: Zgodnie z obowiązującymi przepisami prawa. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskania danych osobowych podaje wszystkie wymagane informacje zgodnie z art. 13 RODO.
Treść większości obowiązujących klauzul informacyjnych zamieszczony jest na naszej stronie internetowej, pod adresem: https://www.mzk.stalowa-wola.pl/rodo/
Obowiązujące klauzule:
Klauzula informacyjna – ws. zgłoszenia/wniosku/pisma przesłanego pocztą elektroniczną
Klauzula informacyjna - wobec osoby wyznaczonej do kontaktu (Art. 14 RODO)
Klauzula informacyjna – Umowa zaopatrzenie w wodę oraz odprowadzenie ścieków
Klauzula informacyjna – Umowa kompleksowa dostarczenia ciepła
Klauzula informacyjna – Faktura Vat
Klauzula informacyjna – Monitoring wizyjny
Klauzula informacyjna – Bilet
Klauzula informacyjna - monitoring w pojazdach MZK
Klauzula informacyjna – Klient (Potencjalny klient)
Klauzula informacyjna – Kontrahent
Klauzula informacyjna - Dla kandydatów do pracy
Klauzula informacyjna – Sygnalista
Klauzula informacyjna – YouTube
Klauzula informacyjna – Rupieciarnia I, II

Klauzula informacyjna – Uczestnicy wycieczek
9. W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne.
Odpowiedź: Zgodnie z obowiązującymi przepisami prawa. Jeżeli danych osobowych nie pozyskujemy od osoby, której dane dotyczą, wówczas podajemy osobie, której dane dotyczą wszystkie wymagane informacje zawarte w art. 14 RODO. Dane te przekazujemy w rozsądnym terminie, najpóźniej jednak w ciągu miesiąca.
Treść obowiązującej klauzuli informacyjnej wobec osoby wyznaczonej do kontaktu (Art. 14 RODO) jest zamieszczona na naszej stronie internetowej, pod adresem: https://www.mzk.stalowa-wola.pl/rodo/
Obowiązujące klauzule informacyjne:
Klauzula informacyjna – Art. 14 RODO
Klauzula informacyjna – dla klienta reprezentowanego przez Pełnomocnika
Klauzula informacyjna – wobec osoby wyznaczonej do kontaktu
Klauzula informacyjna – wobec osoby uprawnionej
10. Wnosimy o regulacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.
Odpowiedź: „Regulamin Systemu Monitoringu Wizyjnego w MZK Sp. z o. o." zamieszczony jest w Regulaminie Pracy Miejskiego Zakładu Komunalnego Sp. z o. o.
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.).
Odpowiedź: TAK – szczegółowa metodyka objęta jest klauzulą poufności – wytworzone dokumenty zawierające zagrożenia oraz podatności nie podlegają udostępnieniu na podstawie ustawy o dostępie do informacji publicznej.
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:
„Jezeli 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".
Odpowiedź: Żądanie przez Pana informacji dotyczących oceny skutków nie stanowi informacji publicznej i nie podlega udostępnieniu w myśl ustawy o dostępie do informacji publicznej.
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?
Odpowiedź: Zasady i procedury obowiązujące przy przetwarzaniu danych osobowych zawarte są w Polityce Ochrony Danych Osobowych Miejskiego Zakładu Komunalnego Sp. z o.o. w Stalowej Woli wraz z załącznikami.
14. PREAMBUŁA WNIOSKU O INFORMACJĘ PUBLICZNĄ W ZAKRESIE KWALIFIKACJI IOD W ZWIĄZKU Z RAPORTEM https://www.nik.gov.pl/kontrole/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 prawniczej. 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, zewnętrzni 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 udzielnie informacji publicznej w przedmiocie :
Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej?
Odpowiedź: IOD 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.

Czy IOD jest prawnikiem? Jakie posiada doświadczenie?
Odpowiedź: Zgodnie z wytycznymi zawartymi w RODO, „IOD 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", co nie oznacza, że powinien posiadać wykształcenie prawnicze.
Kto i w jaki sposób weryfikował kwalifikacje IOD?
Odpowiedź: Prezes Miejskiego Zakładu Komunalnego Sp. z o. o. w Stalowej Woli poprzez przeprowadzoną rozmowę oraz zapoznanie się z dokumentacją potwierdzającą kwalifikację Inspektora Ochrony Danych.

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.

Odpowiedź: Szkolenie odbywają się w formie spotkań z pracownikami.

Szkolenia odbyły sią w roku: 2018, 2019. 2020, 2021, 2022r.

Zakres szkoleń dotyczących ochrony danych osobowych odbywa się według planu szkolenia wewnętrznego z zakresu znajomości zasad ochrony danych osobowych i obejmował miedzy innymi: legalność przetwarzania danych osobowych, realizacja obowiązku informacyjnego, postępowanie w przypadku wystąpienia incydentu, bezpieczne użytkowanie sprzętu IT, bezpieczne korzystanie z Internetu, zabezpieczenia fizyczne obszarów przetwarzania.

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.

Odpowiedź: 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

Odpowiedź: TAK, https://bip.mzk.stalowa-wola.pl/

2. Z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub

www.bip.edu.pl czy inny (podać jaki)?

Odpowiedź: https://www.bip-e.pl/

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.

Odpowiedź: Umowa zawarta na rok. 2018: 1 461.24 zł, 2019: 1 461.24zł, 2020: 1 461.24 zł, 2021: 1 461.24zł, 2022: 1 461.24.

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

Odpowiedź: Na stronie BIP sukcesywnie zamieszczane są wnioski o udostępnienie informacji publicznej. https://bip.mzk.stalowa-wola.pl/sw/udostepnienie-informacj/wykaz-wnioskow-i-odpowi

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.

Odpowiedź: Na stronie BIP sukcesywnie zamieszczane są wnioski o udostępnienie informacji publicznej. https://bip.mzk.stalowa-wola.pl/sw/udostepnienie-informacj/wykaz-wnioskow-i-odpowi

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

Odpowiedź: Na stronie BIP sukcesywnie zamieszczane są wnioski o udostępnienie informacji publicznej. https://bip.mzk.stalowa-wola.pl/sw/udostepnienie-informacj/wykaz-wnioskow-i-odpowi

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

Odpowiedź: Na stronie BIP sukcesywnie zamieszczane są wnioski o udostępnienie informacji publicznej. https://bip.mzk.stalowa-wola.pl/sw/udostepnienie-informacj/wykaz-wnioskow-i-odpowiedzi

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

Odpowiedź: Informacja w tym punkcie ma charakter informacji przetworzonej dlatego wzywamy pana/Panią do wskazania w terminie trzech dni, dlaczego uzyskanie tej informacji publicznej jest szczególnie istotne dla interesu publicznego. Taką przesłankę – zdaniem sądów administracyjnych – można uznać za spełnioną, gdy wnioskodawca jest w stanie wykazać w chwili składania wniosku swoje indywidualne, realne i konkretne możliwości wykorzystania dla dobra ogółu informacji publicznej, której przygotowania się domaga, tj. uczynienia z niej użytku dla dobra ogółu w taki sposób, który nie jest dostępny dla każdego posiadacza informacji publicznej (por. wyrok NSA z 10 stycznia 2014 r., I OSK 2111/13).

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 - głownie 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?

Odpowiedź: Osoba wyznaczona przez Spółkę, na podstawie wiedzy fachowej z zakresu bezpieczeństwa informacji.

2. Czy IOD realizuje zadania w związku z KRIO?

Odpowiedź: Co mamy rozumieć pod skrótem KRIO? Prosimy o doprecyzowanie.

3. Kto przeprowadza audyt bezpieczeństwa?

Odpowiedź: Prosimy o doprecyzowanie o jaki rodzaj audytu z zakresu bezpieczeństwa Pan pyta?

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).

Czy jedynym kryterium wyboru dla IOD i innych usług bezpieczeństwa informacji niezależnie od formy świadczenia tych usługi jest cena?

Odpowiedź: NIE

IOD 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.

Jeśli tak to prosimy o wyjaśnienie czy w związku z tym oznacza to, że ochrona informacji ma niski priorytet w zarządzaniu Państwa organizacją?
Odpowiedź: Nie dotyczy
Jeśli nie, to jakie inne kryteria Państwo stosujecie i z jaką wagą. Prosimy o uszczegółowienie tej kwestii.
Odpowiedź: IOD 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.

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?			
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ 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 EWIDENCJĘ			
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 ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu 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?			

Odpowiedź: Informujemy, że wystosowane żądanie przez Pana, dotyczące pytań zawartych w załączonej tabeli nie stanowi informacji publicznej i nie podlega udostępnieniu w myśl ustawy o dostępie do informacji publicznej. Dokumenty te nie zawierają danych publicznych,
a związane są z aktywnością Spółki, związanej z wewnętrzną organizacją jej funkcjonowania. Ponadto wytworzone dokumenty zawierające zagrożenia oraz podatności nie podlegają udostępnieniu na podstawie ustawy o dostępie do informacji publicznej. Dokumenty te mają charakter organizacyjny, porządkowy i stanowią narzędzie pracodawcy w zakresie kierowania sposobem wykonywania pracy oraz jej dokumentowania.
Czy Państwa jednostka organizacyjna wdrożyła wewnętrzną procedurę schematów podatkowych (MDR – Mandatory Disclosure Rules), zgodnie z wymaganiami ustawy ordynacja podatkowa ?
Odpowiedź: TAK

Z poważaniem
Zarząd MZK Sp. z o.o.

Sekretariat MZK Stalowa Wola
T: (15) 842 34 11 w. 300
mail: sekretariat@mzk.stalowa-wola.pl
