

Szumowo dn. 19.09.2023 r.

Urząd Gminy Szumowo

ul. 1 Maja 50

18-305 Szumowo

AG. 1431.42.2023

Pan

Paweł Rosolski

Odpowiedź na wniosek z dnia 06.09.2023 r. o dostęp do informacji publicznej.

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;
Umowa została zawarta od 1 stycznia 2023r. do 31 grudnia 2024r
 - 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 posiada wykształcenie z zakresu prawa i administracji oraz bezpieczeństwa informacji i ochrony danych osobowych.
 - c) Jak jest spełniona niezależność IOD? Czy dokonano stosowanych zapisów w przepisach wewnętrznych?
IOD Jest podmiotem zewnętrznym.
 - d) termin i zakres przeprowadzenia ostatniego szkolenia RODO dla pracowników;
Marzec 2022
 - e) termin i zakres przeprowadzenia ostatniego szkolenia z KRI dla pracowników;
Marzec 2022
 - f) termin i zakres przeprowadzenia ostatniego szkolenia z cyberbezpieczeństwa dla pracowników;
Marzec 2022
 - g) Kto w/w szkolenia przeprowadza? Zgodnie z art. 39 ust.1 za w/w szkolenia odpowiada IOD?
Powyższe szkolenia przeprowadza IOD, bądź zewnętrzne firmy
 - h) termin i zakres ostatniego audytu w siedzibie jednostki w zakresie RODO.
Marzec 2022
2. Czy był u Państwa przeprowadzony audyt KRI? Jeżeli tak, to proszę podać:
 - Tak**
 - a) Wykonawca - firma zewnętrzna czy pracownik instytucji
Firma zewnętrzna
 - b) Termin ostatniego audytu KRI;

Marzec 2022

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

Marzec 2022

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 zgodnie z obowiązującymi przepisami

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 począwszy od roku 2020? Proszę opisać na czym polegają zmiany w dokumentacji?

Powyższe zmiany nie dotyczą Urzędu, wprowadzono jednak procedurę weryfikacji podmiotu przetwarzającego.

Odpowiedzi oczekuję na mojego maila.

WNIOSEK 2

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 - 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 dane 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.

Na stronie BIP UG Szumowo są wszystkie dane wskazane w art. 11 ustawy w dnia 10 maja 2018 r. o o.d.o.

<https://ug-szumowo.pbip.pl/index.php?event=kategoria&id=369>

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.

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

Urząd Gminy W Szumowie opracował System Zarządzania Bezpieczeństwem Informacji, dokumentacje stanowią m.in.

- Regulamin ochrony danych osobowych;
- Polityka bezpieczeństwa informacji;
- Procedura Instrukcja Zarządzania bezpieczeństwem informacji;
- Procedura zarządzania ryzykiem i cyberbezpieczeństwem;
- Regulamin monitoringu;

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

Pracownicy potwierdzają zapoznanie z treścią obowiązujących wewnętrznych dokumentów dotyczących ochrony danych osobowych na indywidualnym upoważnieniu do przetwarzania danych osobowych wydawanym przez administratora.

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 przeprowadzone zostały w marcu 2022 roku, lista obecności jest w posiadaniu podmiotu prowadzącego szkolenie, Każdy uczestnik otrzymał zaświadczenie o odbyciu szkolenia.

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

RCP został opracowany i jest aktualizowany.

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

Nie dotyczy

8. W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać.

Przedstawić obowiązujące klauzule informacyjne.

Klauzule wynikające z art. 13 RODO są załączane do poszczególnych dokumentów, wniosków, pism itp., na których przetwarzane są dane osobowe. Klauzule dotyczące ochrony danych osobowych znajdują się również w tablicach ogłoszeniowych budynku Urzędu Gminy w Szumowie.

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

Obowiązek informacyjny jest realizowany w przypadku pozyskiwania danych z innych źródeł niż od osoby, której dane dotyczą, poprzez przygotowanie stosowanych klauzul informacyjnych.

INFORMACJA DOTYCZĄCA OCHRONY DANYCH OSOBOWYCH podatki i opłaty lokalne

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) informujemy, o zasadach przetwarzania Państwa danych osobowych oraz o przysługujących Pani/Panu prawach z tym związanych.

1. Administratorem Pani/Pana danych osobowych jest Wójt Gminy Szumowo, ul. 1 Maja 50, 18-305 Szumowo, tel. 86 4768011, mail: szumowo@szumowo.pl;
2. Kontakt z IOD możliwy jest pod adresem mail: inspektorochronydanych@kowalczyk.pro
3. Pani/Pana dane będą przetwarzane są na podstawie ustawy z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych oraz ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa w celu:
 - naliczania wysokości podatku od nieruchomości, rolnego i leśnego od osób fizycznych i prawnych;
 - naliczania wysokości podatku od środków transportowych od osób fizycznych i prawnych;
 - wydawania decyzji w sprawie podatków i opłat lokalnych;
 - poboru i zwrotu podatków i opłat lokalnych;
 - naliczania wysokości zwrotu podatku akcyzowego producentom rolnym zgodnie z ustawą z dnia 10 marca 2006 r. o zwrocie podatku akcyzowego zawartego w cenie oleju napędowego wykorzystywanego do produkcji rolnej;
 - windykacji niezapłaconych podatków i opłat;
 - wydawania zaświadczeń o figurowaniu w ewidencji podatników podatku rolnego, od nieruchomości i leśnego oraz o niezaleganiu w podatkach lub stwierdzające stan zaległości;
 - wydawania zaświadczeń o pomocy de minimis, zgodnie z ustawą z dnia 30 kwietnia 2004r. o postępowaniu w sprawach dotyczących pomocy publicznej.
4. Pani / Pana dane osobowe przechowywane będą przez okres niezbędny do realizacji ww. celu przetwarzania i w okresie późniejszym, jednakże nie dłużej niż okres 10 lat od stycznia kolejnego roku;
5. Posiada Pani/Pan prawo dostępu do swoich danych oraz ich sprostowania. W celu wykonania swoich praw należy skierować żądanie pod adres e-mail: inspektorochronydanych@kowalczyk.pro;

6. Odbiorcami Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz inne podmioty na podstawie stosownych umów podpisanych z Gminą Szumowo;
7. Mają Państwo prawo do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, iż przetwarzanie danych osobowych, które Państwa dotyczą narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.
8. Podanie przez Państwa danych jest wymogiem ustawowym, wynikającym z ww. przepisów prawa.

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

Regulamin monitoringu jest dokumentem wewnętrznym nie podlega udostępnieniu.

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.).

Audyty/sprawdzenia z zakresu RODO realizowane są poprzez bieżące sprawdzenia, ich zakres obejmuje:

- kompletność zidentyfikowanych czynności przetwarzania danych osobowych,
- Przesłanki legalności;
- Środki organizacyjno-techniczne;
- zasadność, zakres i poprawność stosowania umów powierzenia przetwarzania;
- realizacja obowiązków informacyjnych;
- poprawność strony BIP pod kątem zgodności z RODO.

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:

Nie dotyczy

„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”.

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?

Zasady oraz okres przechowywania danych osobowych określa dokument wewnętrzny wprowadzony na mocy ustawy o narodowym zasobie archiwalnym i archiwach- instrukcja kancelaryjna oraz jednolity rzeczowy wykaz akt.

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, 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?

Czy IOD jest prawnikiem? Jakiego posiada doświadczenia?

Odpowiedz powyżej

Kto i w jaki sposób weryfikował kwalifikacje IOD?

Weryfikacji kandydata na IOD dokonywał ADO (Wójt Gminy Szumowo), na podstawie przedstawionych kwalifikacji i doświadczenia.

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.

Odpowiedzi powyżej.

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

Odp. <https://ug-szumowo.pbip.pl>

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

Odp. Politechnika Białostocka

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.

Odp. Umowne świadczenia są na 1 lub 2 lata

Odp.

- za rok 2017 - 3923,70 zł.
- za rok 2018 -1992,60 zł.
- za rok 2019 -1992,60 zł.
- za rok 2020 - 1992,60 zł.
- za rok 2021 - 1992,60 zł.

- do czerwca 2022 -996,30 zł.

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

Odp. 282

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.

Odp. Wpłynęło 248 wnioski, na wszystkie udzielono odpowiedzi

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

Odp. Wnioski o udostępnienie informacji publicznej wraz z odpowiedzią zamieszczone są na stronie urzędowej BIP

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

Odp. Wnioski o udostępnienie informacji publicznej wraz z odpowiedzią zamieszczone są na stronie urzędowej BIP

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)

Odp.

Kierownik jednostki – 36

Z-ca kierownika jednostki – 16 dni

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?
 - Firmy zewnętrzne bądź IOD
2. Czy IOD realizuje zadania w związku z KRI?
Z mocy samego prawa inspektor nie musi wykonywać czynności związanych z KRI. Przepisy regulujące KRI nie są przepisami z zakresu ochrony danych osobowych.
3. Kto przeprowadza audyt bezpieczeństwa?

Audyty bezpieczeństwa informacji przeprowadzają firmy zewnętrzne bądź IOD

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		

	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	TAK		
	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		
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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W	TAK		
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	
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	

7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	TAK		
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		Informacje o podatnościach nie stanowią informacji publicznej
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	TAK		
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>	TAK		
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		

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? <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?	TAK		
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.

	<p>Należy zaznaczyć stosowane w jednostce rozwiązania.</p>	<p>Poniższe informacje nie stanowią informacji publicznej nie podlegają publikacji zgodnie z art. 5 ust. 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz na podst. art.37 ust.1 ustawy z dnia 5 lipca 2018 r. o k.s.c.</p> <p>Udostępnianie na zewnątrz takich informacji może osłabić ich skuteczność przez co zagraża właściwej ochronie danych osobowych i informacji. Zapoznanie osób trzecich ze szczegółami rozwiązań w zakresie bezpieczeństwa danych i architekturą systemów zastosowanych do ich przetwarzania może ułatwić przestępcom i cyberprzestępcom ingerencję w te systemy poprzez ominięcie zastosowanych zabezpieczeń lub ich „złamanie”.</p>		
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; <i>CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY</i>			

	<i>TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W</i>			
e.	system ochrony zewnętrznej klasy firewall			
f.	system ochrony zewnętrznego dostępu logicznego (urządzenie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;			
g.	stosowanie tokenów z hasłami jednorazowymi			
<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.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? <i>Jeśli TAK proszę o przedłożenie dokumentu</i>		nie	
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? <i>Jeśli TAK proszę o udokumentowanie.</i>	tak		
3.	Czy w pracy na odległość stosują bezpieczne metody połączenia?			Nie dotyczy
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?			Nie dotyczy
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? <i>Jeśli TAK proszę wskazać, w jaki sposób.</i>			Nie dotyczy
<p>Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, 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.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu / oprogramowania?	TAK		

	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	
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?				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.			NIE DOTYCZY
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 istnieje możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			
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 DOTYCZY
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				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?	TAK		
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?	TAK		
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?	TAK		
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)?			
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?			
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?	TAK		
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?		NIE	

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.

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

ODP. Tak

Odpowiedzi w ustawowym terminie tj. do 14 dni proszę kierować na adres poczty elektronicznej.

PAWEŁ ROSOLSKI

WARSZAWA

ŻYCZĘ MIŁEGO WIECZORA

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 udostępnienia 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 z sięgnięciem 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.

Odpowiedzi przygotowali:

P. Ewa Bugajniak

P. Małgorzata Głębocka

P. Robert Kurpiewski