

## Odpowiedź na Wniosek o udostępnienie informacji publicznej

1) Na mocy art. 61 Konstytucji RP w związku z art. 6 ust. 1 pkt. lit. c Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - w związku z §20 pkt. 12 lit. a - scilicet "(...) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: dbałości o aktualizację oprogramowania,(...) " - wnosimy o udzielenie informacji publicznej w przedmiocie - szacunkowej ilości oprogramowania - użytkowanego w Urzędzie i nieposiadającego obecnie wsparcia producenta - inter alia: Windows XP, Windows Vista, etc,

*ad.1) W Urzędzie Miasta i Gminy w Wąchocku znajdują się kilka stacji roboczych z systemem Windows 7 które są w trakcie wymiany lub aktualizacji systemu operacyjnego do wersji 10*

2) Czy podmiot dysponuje całościową Polityką Bezpieczeństwa Informacji, wymaganą w §20 ust. 1 i 3 ww. Rozporządzenia? Jeśli odpowiedź jest twierdząca - wnosimy o krótkie - w kilku ogólnych zdaniach - opisanie przedmiotowej dokumentacji RODO.

*ad. 2) Polityka bezpieczeństwa ochrony danych została wdrożona.*

*Celem wdrożenia polityki bezpieczeństwa ochrony danych jest zapewnienie należytej ochrony danych osobowych będących w zasobach Administratora danych, w szczególności odpowiedniej do zagrożeń i kategorii danych osobowych objętych ochroną. Dokument zawiera kwestie związane m.in. z IOD, przetwarzaniem danych, planowanych sprawdzeń, określeniem środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, postępowania w razie zaistnienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych lub naruszenia zasad przetwarzania.*

*Dokument zawiera ponadto załączniki, w tym : rejestr czynności przetwarzania, rejestr kategorii przetwarzania, rejestr żądań podmiotu danych, rejestr incydentów, wzór umowy powierzenia przetwarzania danych osobowych wraz z rejestrem umów, ewidencję osób upoważnionych wraz z tekstem upoważnienia, Instrukcja obsługi żądań podmiotów danych, Instrukcja reagowania na incydenty, Instrukcja użytkownika kluczy, Instrukcja monitorowania, Instrukcja informowania IOD, Instrukcja ochrony danych poza obszarem przetwarzania.*

3) Przepis § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanego dalej rozporządzeniem, określa ciążące na kierownictwie podmiotu publicznego obowiązki związane z systemem zarządzania bezpieczeństwem informacji. Istnieje obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Kiedy Urząd ostatni raz przeprowadzał wewnętrzny audyt z zakresu bezpieczeństwa informacji - stosownie do wymogów §20 ust. 2 pkt. 14 ww. Rozporządzenia.

*ad.3) Ostatni audyt został przeprowadzony w 2019.*

4) Na mocy wyżej wzmiankowanych przepisów wnosimy o udzielenie informacji publicznej w przedmiocie, czy Urząd posiada na dzień dostarczenia niniejszego wniosku - bilateralne sygnowaną umowę (ze strony Urzędu przez upoważnioną osobę) w przedmiocie usług poczty elektronicznej - spełniającą wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (...)

ad.4) *Urząd Miasta i Gminy w Wąchocku na dzień dostarczenia niniejszego wniosku nie posiadał umowy powierzenia danych.*

\_5)\_ \_Na mocy wyżej wymienionych przepisów wnosimy o podanie danych Pracownika Urzędu, który w zakresie wykonywanych zadań i powierzonych kompetencji odpowiada operacyjnie za wyżej wzmiankowany obszar związany z informatyzacją Urzędu. Mówiąc o danych Pracownika Urzędu - Wnioskodawca ma na myśli - imię i nazwisko, adres e-mail, nr tel. Etc

od.5) *Krzysztof Mazurkiewicz, [krzysztof.mazurkiewicz@wachock.pl](mailto:krzysztof.mazurkiewicz@wachock.pl), 412736130*

\_6)\_ \_Czy zostały zrealizowane wszystkie zadania Administratora wskazane w raporcie NIK ?  
<https://www.nik.gov.pl/kontrola/P/18/006/>

ad.6) *Nie wszystkie zadania Administratora wskazane w raporcie NIK zostały zrealizowane.*

\_7)\_ \_Czy IOD poinformował i przygotował umowę zawartą z firmą, która dostarcza oprogramowanie do stworzenia BIP i zajmowała się obsługą serwisową w tym zakresie. Poniżej stanowisko UODO o konieczności zawarcia umowy powierzenia :  
<https://uodo.gov.pl/pl/138/1240> [2]

od.7) *Urząd Miasta i Gminy w Wąchocku zawarł umowę powierzenia z firmą, która dostarcza oprogramowanie BIP i zajmują się obsługą serwisową w tym zakresie.*

\_8)\_ \_Podanie liczby żądań określonych w art. 15 – 21 RODO jakie wpłynęły do adresata niniejszego wniosku w roku 2020.

od.8) *Do tut. Urzędu nie wpłynęły żadne żądania dot. art. 15 – 21 RODO*

\_9)\_ \_Czy zostały przeprowadzone konsultacje o których mowa w art. 108a Prawa Oświatowego w zakresie konsultacji między jednostkami oświatowymi a organem prowadzącym w zakresie monitoringu wizyjnego?

ad.9) *NIE*

\_10)\_ \_Czy w ostatnich trzech latach pracownicy podmiotu uzupełniali wiedzę podczas szkoleń z zakresu dostępu do informacji publicznej/prowadzenia BIP/poprawnej obsługi wniosków o informację publiczną? Jeśli tak to kto był dostawcą szkoleń ([www.institutOS.pl](http://www.institutOS.pl) [4] [3], [www.nbip.pl](http://www.nbip.pl) [5] [4] czy inny (jaki?)), Proszę podać ilu pracowników przeszkolono i jaki był koszt brutto szkolenia za pracownika oraz łącznie, a także czy były to szkolenia zamknięte czy otwarte, stacjonarne(w siedzibie czy wyjazdowe), zdalne (stacjonarne czy telekonferencja)

ad.10) *W ostatnich 3 latach z zakresu dostępu do informacji publicznej przeszkolony został jeden pracownik przez firmę Fundacja Rozwoju Demokracji Lokalnej <https://frdl.kielce.pl> , koszt szkolenie około 450,00 brutto.*

\_11)\_ \_Prezes UODO w decyzji z 10 września 2019 r. (ZSPR.421.2.2019) wyjątkowo mocno podkreśla:

„kontrola dostępu i uwierzytelnianie to podstawowe środki bezpieczeństwa mające na celu ochronę przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Zapewnienie dostępu uprawnionym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów i usług to jeden z wzorcowych elementów bezpieczeństwa”.\_

W związku z powyższym czy IOD podjął działania realne w tym zakresie? Czy zostały opracowane odpowiednie procedury? Jeśli tak to jakie?

*ad.11) Ogólne zasady dotyczące postępowania z dokumentacją zawierającą dane osobowe zostały zawarte w Polityce bezpieczeństwa ochrony danych ( rozdział dot. Określenie środków technicznych organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych ). Obecnie jest aktualizowana Instrukcja zarządzania systemem informatycznym;*

*\_12)\_ Zgodnie ze stanowiskiem UODO wyrażonym w podręczniku UODO <https://uodo.gov.pl/pl/p/ochrona-danych-osobowych-w-szkolach-i-placowkach-oswiatowych-poradnik> [5] i na stronie uodo.gov.pl [6] należy zawrzeć umowy powierzenia pomiędzy jednostkami oświatowymi a podmiotami obsługującymi te jednostki w zakresie księgowym czy administracyjnym np. CUW: „,Ponadto podmiot, któremu administrator danych powierzył ich przetwarzanie, odpowiada wobec administratora danych za przetwarzanie danych niezgodnie z zawartą umową. Zawarcie takiej umowy nie zmienia statusu ich administratora jest on w dalszym ciągu odpowiedzialny za ich prawidłowe przetwarzanie. Odnosi się to również do sytuacji ustawowego powierzenia przetwarzania danych, np., gdy obsługę administracyjną, czy księgową pełni jednostka powołana przez organ prowadzący”\_*

*\_ \_ Czy takie umowy między jednostkami zostały zawarte?*

*ad.12) Urząd Miasta i Gminy w Wąchocku nie prowadzi tzw. CUW . Umowy powierzenia pomiędzy jednostkami oświatowymi powołanymi przez organ prowadzący zostały zawarte.*

*\_13)\_ Wnosimy o informację w zakresie:*

*I. danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD*

*ad. I)- IOD: Krzysztof Kowal tel. +48 605-044-905, email: iod@wachock.pl;*

*z-ca IOD - Krzysztof Mazurkiewicz, email: iod@wachock.pl*

*II. zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO;*

*ad.II) zakres czynności wynika z PBOD i umowy z RODO.pl*

*1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:*

*a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora;*

*b) nadzorowanie opracowania i aktualizowania dokumentacji, ochrony danych osobowych oraz przestrzegania zasad w niej określonych;*

*c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych („szkolenie”).*

*2) pomoc w przeprowadzaniu analizy ryzyka, na zasadach opisanych w art.32 Rozporządzenia.*

*W celu sprawnej realizacji nałożonych zadań, Inspektora Ochrony Danych przysługują uprawnienia określone w art.37 – 39 RODO;*

III. czy IOD wykonuje jeszcze jakieś inne dodatkowe czynności/ jeśli tak wskazać jakie;

*ad.III) nie*

IV. informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD;

*ad.IV) odpowiedzialna za to jest firma zewnętrzna, która gwarantuje, że IOD będzie posiadał odpowiednie kwalifikacje*

V. dokumentacja potwierdzająca realizację zadań przez IOD od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO).

*ad.V) dokumentacja ze sprawdzeń za lata 2019, 2020*

VI. informacje dotyczące szkoleń pracowników w zakresie ochrony danych osobowych przeprowadzanych po 25 maja 2018 roku z zakresu RODO oraz Krajowych Ram Interoperacyjności (informacje tj. zakres szkolenia, osoba prowadząca, listy obecności, potwierdzenie odbycia szkolenia)

*ad.VI) Pracownicy Urzędu Miasta i Gminy są sukcesywnie szkoleni z zakresu ochrony danych osobowych oraz zostali zapoznani z polityką bezpieczeństwa.*

VII) rejestr czynności przetwarzania danych osobowych oraz jego zmiany,

*ad.VII) Rejestr czynności przetwarzania jest obecnie aktualizowany - nie stanowi on informacji publicznej*

<https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sab-ld-181-18-rejestry-czynnosci-przetwarzania-oraz-522720873>

VIII) rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany

*ad.VIII) Rejestr kategorii czynności przetwarzania, prowadzenie powyższego Rejestru spoczywa na podmiotach przetwarzających (czyli takich, które przetwarzają dane osobowe należące do administratora).*

*(ale nie stanowi on informacji publicznej*

<https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sab-ld-181-18-rejestry-czynnosci-przetwarzania-oraz-522720873>

IX. dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych.

*ad. IX) Urząd Miasta i Gminy w Wąchocku posiada dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych ale nie jest informacją publiczną)*

X. w jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne. Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?

*ad.X) Klauzule informacyjne wraz z opisem ich zamieszczenia w zakresie:*

*1. Klauzula informacyjna ogólna UMiG Wąchock - na stronie www., przy wejściu do UMiG*

2. Klauzula informacyjna – dowody osobiste – umieszczony na stronie www, przy wniosku,
3. Klauzula informacyjna – ewidencja ludności – umieszczony na stronie www, przy wniosku,
4. Klauzula informacyjna – urząd stanu cywilnego - umieszczony na stronie www, przy wniosku,
5. Klauzula informacyjna – nagrywanie sesji Rady Gminy - umieszczona przy wejściu na salę obrad, dodatkowo odczytana na początku sesji,
6. Klauzula informacyjna – dot. listy osób odwiedzających w związku z COVID - umieszczona w miejscu pobierania danych,
7. Klauzula informacyjna dot. postępowania o udzieleniu zamówienia publicznego – na stronie www, przy dokumentacji w sprawie ogłaszania postępowania o udzieleniu zamówienia publicznego,
8. Klauzula dołączana do umów

W Urzędzie przyjęto ogólną zasadę, że przy każdej pierwszej czynności kierowanej do osoby fizycznej przekazujemy jej klauzulę informacyjną z art. 13 RODO.

XI) w jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne. Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?

ad.XI) W kwestii przekazania obowiązku informacyjnego z art. 14 RODO zgodnie z art. 14 ust. 5 lit. c RODO informowanie o obowiązkach wynikających z art. 14 RODO, o których mowa w ust. 1-4 nie mają zastosowania gdy:

„pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub”.

Przyjęliśmy jednak zasadę, że kiedy dane nie są pozyskiwane od osoby, której dane dotyczą, stosujemy klauzulę informacyjną określoną w polityce informacyjnej, której nazwę oraz instrukcję do niej zamieszczamy poniżej:

**„Dane pozyskane z powszechnie dostępnych źródeł**

W przypadku pozyskania danych ze źródeł zewnętrznych, najpóźniej w przeciągu 30 dni należy poinformować osobę, której dane dotyczą o przetwarzaniu jej danych i podać źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych. Każdorazowo należy konsultować klauzulę z Inspektorem Ochrony Danych.

Klauzulę należy dołączyć/przekazać przy pierwszej czynności organu skierowanej do osoby fizycznej, w przypadku otrzymania danych z innego Urzędu.”

XII) czy są wykonywane audyty z zakresu RODO? Przedstawić realizację w/w obowiązku.

ad.XII) ostatni audyt został przeprowadzony w grudniu 2019 roku;

14. Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

IOD nie może podlegać jakimkolwiek innym osobom niż najwyższe kierownictwo (art. 38 ust. 3 RODO), co ma mu gwarantować niezależne, prawidłowe i skuteczne wykonywanie funkcji. Najwyższym kierownictwem jednostki organizacyjnej - w zależności od jej rodzaju – może być osoba lub osoby (np. wchodzące w skład organu), które kierują jej pracami (np. ministrowie kierujący działami administracji rządowej, dyrektorzy szkół), prowadzą jej sprawy (np. zarząd spółki) albo podejmują zarobkową działalność (np. przedsiębiorcy jednoosobowi), działając jako administrator. W przypadku jednoczesnego pełnienia funkcji IOD i ASI wykluczone jest rozwiązanie, w którym osoba taka podlegałaby np. SEKRETARZ GMINY, dyrektorowi ds. informatycznych, kierownikowi działu IT lub jakiegokolwiek innej osobie (np. dyrektorowi generalnemu urzędu publicznego), która nie jest najwyższym kierownictwem w rozumieniu art. 38 ust. 3 RODO.

Zgodnie z art. 38 ust. 6 RODO IOD może wykonywać inne zadania i obowiązki przy czym administrator lub podmiot przetwarzający powinni zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. RODO nie precyzuje w jakich sytuacjach będzie zachodził, wskazany w art. 38 ust. 6 RODO, konflikt interesów. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Oznacza to, że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych.

Za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT, sekretarz gminy) oraz niższe stanowiska, jeśli osoby je piastujące biorą udział w określaniu celów i sposobów przetwarzania danych.

Dlatego też ww. konflikt interesów może obejmować również stanowiska związane z bezpieczeństwem w organizacji, o ile z ich piastowaniem wiąże się decydowanie - w jakikolwiek sposób o sposobach i celach przetwarzania danych osobowych w organizacji.

Podsumowując, ocena czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności.

Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny zaistnienia takiego konfliktu mogą występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD.

*ad.14) Nie istnieje konflikt interesów przy pełnieniu funkcji IOD ( firma zewnętrzna )*

15. Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

*ad.15) Sprawdzenia 2019, 2020*

16. Czy jednostka realizuje obowiązek wskazany w najnowszym stanowisku UODO? Jeśli proszę wskazać w jaki sposób.

<https://uodo.gov.pl/pl/225/1577> [7]

***(czy jest spełniany obowiązek informacyjny wobec członków zarządu reprezentujących osobę prawną, pełnomocników osób prawnych, a także pracowników, którzy są osobami kontaktowymi osoby prawnej ( dot. sytuacji **gdy w treści dokumentacji dotyczącej postępowań administracyjnych*****

***pojawiają się dane osób upoważnionych do reprezentacji spółek np. członków zarządu (organów spółek) bądź osób uprawnionych do składania oświadczeń w imieniu określonego podmiotu?)***

*ad.16)*

*Do dokumentu polityki informacyjnej określającej zasady realizowania obowiązków informacyjnych, dodano klauzulę „klauzula dołączana do umów”, która realizuje wskazany powyżej obowiązek.*

17. W jaki sposób są realizowane obowiązki informacyjne względem osób, które dane dotyczą?

*ad. 17) UMiG - jeżeli zostały wdrożone przekazane klauzule informacyjne, to zgodnie z opisem:*

- 1. Klauzula informacyjna ogólna UMiG Wąchock - na stronie www., przy wejściu do UMiG*
- 2. Klauzula informacyjna – dowody osobiste – umieszczony na stronie www, przy wniosku,*
- 3. Klauzula informacyjna – ewidencja ludności – umieszczony na stronie www, przy wniosku,*
- 4. Klauzula informacyjna – urząd stanu cywilnego - umieszczony na stronie www, przy wniosku,*
- 5. Klauzula informacyjna – nagrywanie sesji Rady Gminy - umieszczona przy wejściu na salę obrad, dodatkowo odczytana na początku sesji,*
- 6. Klauzula informacyjna – dot. listy osób odwiedzających w związku z COVID - umieszczona w miejscu pobierania danych,*
- 7. Klauzula informacyjna dot. postępowania o udzieleniu zamówienia publicznego – na stronie www, przy dokumentacji w sprawie ogłaszania postępowania o udzieleniu zamówienia publicznego,*
- 8. Klauzula dot. „Dane pozyskane z powszechnie dostępnych źródeł”*
- 9. Klauzula dołączana do umów*

18. Czy w jednostce funkcjonują przepisy wewnętrzne i dokumenty, z których zapisów wynika, w jaki sposób IOD został włączony w bieżące funkcjonowanie jednostki.

*ad.18) Umowa współpracy z rodo.pl, PBOD*