

W odpowiedzi na wniosek uprzejmie informuję:

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,

Wszystkie stacje robocze posiadają aktualny system operacyjny.

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.

Tak. PBI zawiera ogólne zasady ochrony danych osobowych w tym zasady ochrony danych osobowych w systemach informatycznych. Została wprowadzona zarządzeniem Wójta Gminy.

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.

Rok 2020

4) Na mocy wyżej wzmiankowanych przepisów wnosimy o udzielenie informacji publicznej w przedmiocie, czy Urząd posiada na dzień dostarczenia niniejszego wniosku - bilateralnie 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 (...)

Tak

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

Dawid Tylus, gmina@wilkolaz.pl, 81 8212001,

6) Czy zostały zrealizowane wszystkie zadania Administratora wskazane w raporcie NIK ?
<https://www.nik.gov.pl/kontrole/P/18/006/>.

Raport NIK nie stanowi źródła obowiązującego prawa

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>

Tak

8) Podanie liczby żądań określonych w art. 15 – 21 RODO jakie wpłynęły do adresata niniejszego wniosku w roku 2020.

Brak

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?

Tak

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, www.nbip.pl czy inny (jaki?)), Proszę podać ilu pracowników przeszkolono i jaki był koszt brutto szkolenia za pracownika oraz łącznie, a także czy były to szkolenia zamknięte czy otwarte, stacjonarne(w siedzibie czy wyjazdowe), zdalne (stacjonarne czy telekonferencja)

Nie z uwagi na ograniczone środki budżetowe

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?

Decyzje UODO dotyczą konkretnego Administratora. Decyzja ZSPR.421.2.2019 dotyczyła firmy komercyjnej Morele

12) Zgodnie ze stanowiskiem UODO wyrażonym w podręczniku UODO <https://uodo.gov.pl/pl/p/ochrona-danych-osobowych-w-szkolach-i-placowkach-oswiatowych>-poradnik i na stronie uodo.gov.pl

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?

Wójt Gminy Wilkołaz nie jest adresatem pytania gdyż nie jest ADO w szkołach

13) Wnosimy o informację w zakresie:

• danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD

Dane IOD są udostępniane w BIP UG Wilkołaz

• zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO;

Zadania IOD są zgodne z art. 39 RODO i zawartą umową, został zgłoszony do PUODO

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

Nie

• informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

IOD stale doskonalili swoją wiedzę

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

Metodyka realizacji zadań IOD w tym komunikacja IOD z pracownikami UG Wilkołaz nie stanowi informacji publicznej

• 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)

Metodyka realizacji zadań IOD w tym komunikacja IOD z pracownikami UG Wilkołaz nie stanowi informacji publicznej, IOD nie może ponadto naruszać tajemnicy korespondencji

• rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

• rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

Zgodnie z art.30 ust.4 RODO rejestr czynności przetwarzania i rejestr kategorii przetwarzania można udostępnić jedynie UODO

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

Dokumentacja analizy ryzyka nie stanowi informacji publicznej, ujawnienie dokumentu spowodowałoby nieuzasadnione dodatkowe ryzyko

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

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

Art.13 i art 14 RODO realizowany jest zgodnie z przepisami m.in przez publikację klauzul w BIP/na stronie internetowej, przez umieszczenie klauzul na tablicy informacyjnej, w treści dokumentów np. wniosków. Treści klauzul są do pobrania z w/w źródeł

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

Wymagane audyty są realizowane w niezbędnym zakresie. Ustawodawca nie zdefiniował pojęcia "audyt RODO"

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.

Nie istnieje

15. Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

Tak

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

<https://uodo.gov.pl/pl/225/1577>

Tak

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

Patrz odpowiedź na pyt nr.13

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

Tak

Z poważaniem

Jacek Stec