

Odpowiedz, 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,

Takie oprogramowanie nie jest już użytkowane w Urzędzie.

- 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 wprowadzenie polityki bezpieczeństwa informacji i instrukcji Zarządzania Systemem Informatycznym do organizacji łączy systemu bezpieczeństwa informacji oraz ochrony danych osobowych w taki sposób, by zapewnić zapewnienie poufności oraz integralności danych osobowych, oraz realizację podstawowych praw i wolności osób fizycznych, których dane osobowe organizacja przetwarza w związku z realizacją zadań publicznych.

- 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.

Wewnętrzny audyt z zakresu bezpieczeństwa informacji został przeprowadzony w dniach od 7 do 18 grudnia 2020 r.

- 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 (...)

Urząd ma zawartą taką umowę.

- 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.

Łukasz Chlebny, lc@ugb.pl

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

Zadania administratora wskazane w raporcie NIK, są realizowane na bieżąco.

- 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>

Urząd Gminy posiada zawartą umowę powierzenia przetwarzania danych z firmą dostarczającą oprogramowanie do stworzenia BIP oraz realizującą obsługę serwisową w tym zakresie

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

W wymienionym zakresie nie wpłynęły żadne żądania.

- 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?

Pomiędzy szkołami i organem prowadzącym zostały przeprowadzone wymagane konsultacje.

- 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)

W urzędzie nie były przeprowadzane szkolenia z zakresu obsługi BIP.

- 11) Czy IOD podjął działania realne w tym zakresie? Czy zostały opracowane odpowiednie procedury? Jeśli tak to jakie?

Tak, procedura nadawania dostępu do systemu informatycznego oraz inne zgodnie z zasadami zawartymi w Polityce bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym w tym również podczas realizowanych przez IOD sprawdzeń.

- 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?

Tak, takie umowy między jednostkami zostały zawarte.

13) Wnosimy o informację w zakresie:

- danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD Małgorzata Sobieraj.
- zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO;
Zakresy czynności IOD określony został w zakresie czynności oraz procedurach w Polityce bezpieczeństwa informacji.
- czy IOD wykonuje jeszcze jakieś inne dodatkowe czynności/ jeśli tak wskazać jakie;
Nie.
- informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.
Inspektor ochrony danych odbył szkolenia z zakresu stosowania RODO, zabezpieczeń fizycznych, organizacyjnych oraz cyberbezpieczeństwa.
- dokumentacja potwierdzająca realizację zadań przez IOD od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO).
Według orzeczeń sądów administracyjnych udostępnienie zawartości wewnętrznej dokumentacji dotyczącej ochrony danych osobowych na podstawie ustawy o dostępie do informacji publicznej ma charakter informacji niejawnych, dlatego też udostępnienie ich podlega ograniczeniu - art. 5 ust. 1 ustawy o dostępie do informacji publicznej. Polityka jest dokumentem do użytku wewnętrznego - wyrok z dnia 8 grudnia 2005 r. Wojewódzkiego Sądu Administracyjnego w Warszawie (syg. akt II S.A./WA 1539/05) Sąd wskazał, że biorąc pod uwagę wymagania przepisami prawa zawartość Polityki nie powinna być udostępniana publicznie.
- 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)
Dla pracowników IOD prowadził szkolenia z zakresu systemu zarządzania bezpieczeństwem informacji w kontekście RODO, rejestru czynności przetwarzania, rejestru umów powierzenia, analizy ryzyka oraz indywidualne szkolenia i konsultacje dla poszczególnych komórek organizacyjnych. Żądanie natomiast przez wnioskodawcę list obecności, potwierdzeń odbycia szkoleń przez pracowników nie stanowi informacji publicznej i nie podlega udostępnieniu w myśl ustawy o dostępie do informacji publicznej.

- rejestr czynności przetwarzania danych osobowych oraz jego zmiany.
Według orzeczeń sądów administracyjnych udostępnienie zawartości wewnętrznej dokumentacji dotyczącej ochrony danych osobowych na podstawie ustawy o dostępie do informacji publicznej ma charakter informacji niejawnych, dlatego też udostępnienie ich podlega ograniczeniu - art. 5 ust. 1 ustawy o dostępie do informacji publicznej. Polityka taka wraz z załącznikami jest dokumentem do użytku wewnętrznego - wyrok z dnia 8 grudnia 2005 r. Wojewódzkiego Sądu Administracyjnego w Warszawie (syg. akt II S.A./WA 1539/05) Sąd wskazał, że biorąc pod uwagę wymagania przepisami prawa zawartość Polityki nie powinna być udostępniana publicznie.
- rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.
Według orzeczeń sądów administracyjnych udostępnienie zawartości wewnętrznej dokumentacji dotyczącej ochrony danych osobowych na podstawie ustawy o dostępie do informacji publicznej ma charakter informacji niejawnych, dlatego też udostępnienie ich podlega ograniczeniu - art. 5 ust. 1 ustawy o dostępie do informacji publicznej. Polityka taka wraz z załącznikami jest dokumentem do użytku wewnętrznego - wyrok z dnia 8 grudnia 2005 r. Wojewódzkiego Sądu Administracyjnego w Warszawie (syg. akt II S.A./WA 1539/05) Sąd wskazał, że biorąc pod uwagę wymagania przepisami prawa zawartość Polityki nie powinna być udostępniana publicznie.
- dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych.
Według orzeczeń sądów administracyjnych udostępnienie zawartości wewnętrznej dokumentacji dotyczącej ochrony danych osobowych na podstawie ustawy o dostępie do informacji publicznej ma charakter informacji niejawnych, dlatego też udostępnienie ich podlega ograniczeniu - art. 5 ust. 1 ustawy o dostępie do informacji publicznej. Polityka taka wraz z załącznikami jest dokumentem do użytku wewnętrznego - wyrok z dnia 8 grudnia 2005 r. Wojewódzkiego Sądu Administracyjnego w Warszawie (syg. akt II S.A./WA 1539/05) Sąd wskazał, że biorąc pod uwagę wymagania przepisami prawa zawartość Polityki nie powinna być udostępniana publicznie.
- w jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne. Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?
Obowiązek ten jest realizowany dla wszystkich wymaganych czynności, poprzez: BIP, stronę internetową, w korespondencji wychodzącej, w urzędzie na drzwiach wejściowych do danego pokoju oraz do wglądu w każdym referacie;
- w jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne. Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?
Jest realizowany dla wszystkich wymaganych czynności, poprzez: BIP, na tablicy ogłoszeń, w korespondencji wychodzącej, oraz do wglądu w referacie;
- czy są wykonywane audyty z zakresu RODO? Przedstawić realizację w/w obowiązku.

Tak przeprowadzany jest przez IOD cykliczny audyt w zakresie RODO.

- 14) Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

Nie występuje. IOD podlega tylko najwyższemu kierownictwu.

- 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>.

Jeśli jest spełniona przesłanka identyfikowalności osób fizycznych, obowiązki te realizuje się poprzez klauzule informacyjne, które są dołączane do umów z osobami prawnymi.

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

Poprzez odpowiednie klauzule informacyjne, przekazywane bezpośrednio lub dostępne do wglądu na stronie internetowej lub w siedzibie.

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

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