Realizacja wniosku o udzielenie informacji publicznej 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

Data wniosku Data: 2020-12-31 17:02

Wnioskodawca: Bartłomiej KUKLIŃSKI

Dane serwera wnioskodawcy: inf_publ@wp.pl

Identyfikacja rejestrowa: brak danych rejestrowych wnioskodawcy

Cel komercyjny: brak informacji

Intencje wnioskodawcy: Pomimo, że nie wnioskujemy o informację przetworzoną w zakresie wymagającym znacznych nakładów pracy, uzasadniamy nasze pytania stosownie do brzmienia art. 3 ust. 1 pkt. 1 Ustawy o dostępie do informacji publicznej – tym, że przedmiotowa informacja oraz ewentualna późniejsza próba optymalizacji tego obszaru wydaje się szczególnie istotna z punktu widzenia Interesu Społecznego - o czym świadczy powołany protokół NIK

Pytanie 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 udzielnie informacji publicznej w przedmiocie - szacunkowej ilości oprogramowania - użytkowanego w Urzędzie i nieposiadającego obecnie wsparcia producenta - *inter alia*: Windows XP, Windows Vista, etc
Odpowiedź 1)
W placówce, wszystkie stacje robocze zostały zaktualizowane do systemu operacyjnego Windows 10
Pytanie 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.

Odpowiedź 2)

W polityce ochrony danych osobowych w dziale „Bezpieczeństwo przetwarzania” –

Administrator uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

a) szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania po przez wdrożenie zabezpieczeń wynikających z:

1) polityki bezpieczeństwa informacji (w ograniczonym zakresie);

2) instrukcji bezpieczeństwa pożarowego;

3) instrukcji kancelaryjnej;

4) instrukcji składnicy akt.

Pytanie 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.
Odpowiedź 3)
Ostatni audyt był przeprowadzony w miesiącach listopad-grudzień 2020 r.
Pytanie 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 (...)
Odpowiedź 4)
Jako Przedszkole, nie dysponujemy taką informacją.
Pytanie 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
Odpowiedź 5)
https://bip.wodzislaw-slaski.pl/bipkod/006/001
Pytanie 6)
Czy zostały zrealizowane wszystkie zadania Administratora wskazane w raporcie NIK ? https://www.nik.gov.pl/kontrole/P/18/006/
Odpowiedź 6)
Przedszkole, uwzględniając stan wiedzy technicznej, **koszt wdrażania** oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić sukcesywnie wdrażać System Zarządzania Bezpieczeństwem Informacji, opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001,

a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym: 1) PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń; 2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; 3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
Pytanie 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
Odpowiedź 7)
Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy. Umowa wiąże podmiot przetwarzający i administratora, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
Pytanie 8)
Podanie liczby żądań określonych w art. 15 – 21 RODO jakie wpłynęły do adresata niniejszego wniosku w roku 2020.
Odpowiedź 8)
Nie zanotowano żądań w 2020 r.
Pytanie 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?
Odpowiedź 9)
Tak
Pytanie 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.instytutOS.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)
Odpowiedź 10)
W czerwcu 2019, IOD przeprowadził szkolenie podstawowe z ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej w którym udział brały osoby zarządzające placówkami. Szkolenia wyjazdowe organizowane przez IOD są w ramach umowy świadczenia usług.
Pytanie 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?
Odpowiedź 11)
IOD podjął działanie, wdrażając zabezpieczenia o którym mowa w pkt. 9, 10, 11,12,13 normy PN-ISO/IEC 27002
Pytanie 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?
Odpowiedź 12)
Nie. Przedszkole nie korzysta z CUW.
Pytanie 13)
Wnosimy o informację w zakresie: • danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD • zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO; • czy IOD wykonuje jeszcze jakieś inne dodatkowe czynności/ jeśli tak wskazać jakie; • informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD. • dokumentacja potwierdzająca realizację zadań przez IOD od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO). • 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) • rejestr czynności przetwarzania danych osobowych oraz jego zmiany. • rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany. • dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych. • 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?

• czy są wykonywane audyty z zakresu RODO? Przedstawić realizacji w/w obowiązku.
Odpowiedź 13)
1) Dane IOD: Krzysztof HAWRYLAK, email: iod@hawrylak.pl, tel. 514519700 2) Zakres czynności zgodnie z art. 39 RODO, zgłoszenia do PUODO dokonano w grudniu 2018 r. 3) IOD nie wykonuje innych dodatkowych czynności. 4) Ostatni szkolenie odbyło się w dniach 12-13.12.2019 r. w Akademii Sztuki Wojennej w Warszawie. 5) Prowadzony jest harmonogram oraz plan audytów. 6) Szkolenia prowadzone są na bieżąco, zgodnie z przyjętą polityką ochrony danych osobowych w Przedszkolu. 7) Rejestr czynności jest aktualizowany co najmniej raz na rok lub po każdej zmianie realizacji celów Administratora. 8) Rejestr wszystkich kategorii czynności przetwarzania jest aktualizowany co najmniej raz na rok lub po każdej zmianie w funkcjonowania lub organizacji Przedszkola. 9) Dokumentacja opracowana jest na podstawie normy ISO/IEC 27005 oraz ISO/IEC 29134 10) KLAUZULA REKRUTACYJNA W ODPOWIEDZI NA OGŁOSZENIE O PRACĘ NA KONKRETNE STANOWISKO ORAZ Z MOŻLIWOŚCIĄ ODEBRANIA ZGODY NA PRZYSZŁE REKRUTACJE NR K/1/2020, KLAUZULA INFORMACYJNA DLA PRACOWNIKA (ZGODNA Z ART. 13 RODO) NR K/2/2020, KLAUZULA INFORMACYJNA W PRZYPADKU ZBIERANIA DANYCH W SPOSÓB INNY NIŻ OD OSOBY, KTÓREJ DANE DOTYCZĄ NR K/3/2020, KLAUZULA INFORMACYJNA DLA PRACOWNIKA W ZWIĄZKU Z PRZETWARZANIEM JEGO DANYCH OSOBOWYCH NA POTRZEBY ZAKŁADOWEGO FUNDUSZU ŚWIADCZEŃ SOCJALNYCH NR K/4/2020, KLAUZULA DLA UCZESTNIKÓW W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO NR K/5/2020, KLAUZULA INFORMACYJNA W ZWIĄZKU

Z WYSTAWIENIEM FAKTURY NR K/6/2020, KLAUZULA INFORMACYJNA – MONITORING WIZYJNY NR K/7/2020, KLAUZULA INFORMACYJNA – KORESPONDENCJA KPA.

11) Strona internetowa Administratora, oraz klauzule do podpisu przez PII

12) W planie audytów na 2021 r., zakłada przeprowadzenie 4 audytów. Po każdym audycie sporządzany jest sprawozdanie

Sprawozdanie z zadania zapewniającego 2020-12-02

2020/A/0913/0001

ORYGINAŁ

1. Oznaczenie podstawy prawnej przeprowadzonych czynności

Art 39, ust.2, lt. b) rozporządzenia PE I RADY (UE) 2016/679 z dnia 27.04.2016r.

2. Imię i nazwisko oraz stanowisko audytora

Krzysztof HAWRYLAK, inspektor ochrony danych, audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg normy ISO 27001

3. Nazwa (nazwisko) oraz adres lub siedzibę audytowanego

PUBLICZNE PRZEDSZKOLE NR 1
Pośpiecha 7
44-300 Wodzisław Śląski

4. Informacje, kto i w jakim charakterze był obecny przy czynnościach

Mirosława KUŹNIK - DYREKTOR

5. Miejsce i termin przeprowadzonych czynności

Wodzisław Śląski, 2020-12-02

6. Wykaz kontrolowanych obiektów, terenów i urządzeń

Polska, Wodzisław Śląski, Pośpiecha, 7

7. Wykaz przeprowadzonych czynności sprawdzających

LP	Zakres audytu	Opis stanu faktycznego, będącego przedmiotem czynności
1	OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM	Wymagania: 12.2 Zabezpieczenia przed szkodliwym oprogramowaniem 12.2.1 Zabezpieczenie. Wdrożenie zabezpieczeń wykrywających lub zapobiegających użyciu znanych szkodliwych stron webowych lub podejrzewanych o to. Sprawdzenie Podczas audytu w dniu: 2020-12-02, stwierdzono że: 1) na stacjach roboczych, służących do przetwarzania informacji, zainstalowane jest aktualne oprogramowanie antywirusowe.
2	ZGODNOŚĆ Z WYMAGANIAMI PRAWNYMI I UMOWNYMI	Wymagania: Art. 29 Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Sprawdzenie Podczas audytu w dniu: 2020-12-02, stwierdzono że: 1) Osoby, które przetwarzają dane osobowe, posiadają stosowne upoważnienie administratora.

8. Zalecenia

Pytanie 14)

Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

Odpowiedź 14)

Nie. Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.
Pytanie 15)
Czy istnieje dokumentacja z zakresu realizacji zadań IOD?
Odpowiedź 15)
Tak
Pytanie 16)
Czy jednostka realizuje obowiązek wskazany w najnowszym stanowisku UODO? Jeśli proszę wskazać w jaki sposób. https://uodo.gov.pl/pl/225/1577
Odpowiedź 17)
Administrator wypełnienia w stosunku do takich osób obowiązek informacyjny określony w art. 13 lub 14 RODO, o ile nie zachodzi jedna z przesłanek zwalniających go z tego obowiązku.
Pytanie 18)
W jaki sposób są realizowane obowiązki informacyjne względem osób, które dane dotyczą?
Odpowiedź 18)
Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje: a)swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela; b) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania; jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią; e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją; f) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach

uzyskania kopii danych lub o miejscu udostępnienia danych. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Obowiązek informacyjny realizowany jest głownie przez klauzule informacyjne na stronie Przedszkola lub/i siedzibie podmiotu. Obowiązek informacyjny realizowany jest również w formie szkolenia, realizowanego przez IOD oraz Dyrektor Przedszkola. Informacje są również dostępne na tablicach informacyjnych Przedszkola.

Pytanie 19)

Czy w jednostce funkcjonują przepisy wewnętrzne i dokumenty, z których zapisów wynika, w jaki sposób IOD został włączony w bieżące funkcjonowanie jednostki.
Odpowiedź 19)
Umowa o świadczenie usług