WÓJT
GMINY KRYNICE
22-610 KRYNICE
woj. lubelskie

Krynice, dnia 19 stycznia 2021 r.

OK.431.57.2020

Pan Tomasz Piotrowicz
Proton

W odpowiedzi na wniosek z dnia 22.12.2020 r., o udostępnienie informacji publicznej oraz na pismo z dnia 31 grudnia 2020 r. w sprawie przedłużenia terminu na udzielenie odpowiedzi do 22.01.2021 r. ze względu na szeroki zakres wnioskowanych danych wyjaśniam:

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 na pytanie nr 1
W Urzędzie Gminy nie jest użytkowane oprogramowanie nieposiadające wsparcie producenta

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 na pytanie nr 2
W Urzędzie Gminy Krynice obowiązuje „Polityka Ochrony Danych Osobowych", jest to dokument wewnętrzny i nie podlega udostępnieniu w drodze dostępu do informacji publicznej.
Opis procedur nie jest możliwy ponieważ ujawnienie wskazanych danych może nieść ze sobą zagrożenie dla praw i wolności obywateli, bowiem to właśnie ich dane osobowe przetwarzane są w ramach wykonywania ustawowych zadań w systemach Urzędu. Zgodnie z art. 24 ust. 1 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. W ramach realizacji wskazanych obowiązków Administrator m.in. zobowiązał osoby przetwarzające dane osobowe do zachowania w tajemnicy informacji na temat stosowanych zabezpieczeń w zakresie systemów stosowanych przez Urząd. (stanowisko GIODO, wyrok WSA z 26 października 2015 r. sygn. akt II SA/Wa 1135/15, wyrok z 8 grudnia 2005 r. sygn.

akt II SA/WA 1539/05, wyrok Naczelnego Sądu Administracyjnego z dnia 9 marca 2018 r. I OSK 862/16, Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 21 grudnia 2015 r. II SA/Wa 1261/15).

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 na pytanie nr 3
Ostatni audyt KRI został przeprowadzony w kwietniu 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 na pytanie nr 4
Nie

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 na pytanie nr 5
Rafał Stadnicki, infobitzamosc@gmail.com

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

Odpowiedź na pytanie nr 6
Raport NIK nie jest podstawą prawną w polskim porządku prawnym. Administrator realizuje wszystkie swoje obowiązki wynikające m.in. z RODO oraz innych obowiązujących przepisów prawa.

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 na pytanie nr 7
Pytanie jest nieprecyzyjne „ *Czy IOD poinformował i przygotował umowę (...)*?" Tak, jest zawarta umowa powierzenia przetwarzania danych osobowych

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

Odpowiedź na pytanie nr 8
W roku 2020 do Urzędu nie wpłynęły żądania umocowane w art. 15-21 RODO

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 na pytanie nr 9
Nie

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 na pytanie nr 10
Nie

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 na pytanie nr 11
Zagadnienia wskazane w pytaniu reguluje obowiązująca w jednostce Polityka Ochrony Danych Osobowych, dokument ten jest dokumentem wewnętrznym i nie podlega udostępnieniu w drodze dostępu do informacji publicznej.

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 na pytanie nr 12
Nie dotyczy

Pytanie 13) Wnosimy o informację w zakresie:

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

Odpowiedź:
Inspektor Ochrony Danych: Ewa Fidecka, e.fidecka@ data-partners.pl

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

Odpowiedź:
Zakres czynności zgody z art. 39 RODO. W załączeniu przesyłam skan zarządzenia nr 1/2021 w sprawie wyznaczenia Inspektora Ochorny Danych w Urzędzie Gminy Krynice. Zawiadomienie o wyznaczeniu wysłano do PUODO

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

Odpowiedź:
IOD nie wykonuje dodatkowych czynności.

- informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

Odpowiedź:
IOD bierze udział w szkoleniach w celu podnoszenia kwalifikacji, jednak szkolenia, w których uczestniczy IOD nie są finansowane ze środków publicznych w związku z tym, w mojej ocenie nie stanowią informacji publicznej.

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

Odpowiedź:
Zadania realizowane w zakresie obowiązków RODO są dokumentowane w formie załączników do Polityki Ochrony Danych.

- 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)

Odpowiedź:
Szkolenie pracowników Urzędu Gminy Krynice zostało zrealizowane w dniu 27 listopada 2018 r. przez firmę "ADIGAN Ewa Nowak"
Zakres szkolenia:

- Definicje dot. Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016 r.
- Definicje dot. Ustawy o ochronie danych osobowych z dnia 10 maja 2018r.
- Legalność przetwarzania danych osobowych
- Obowiązek informacyjny
- Zasady ujawniania oraz powierzania danych osobowych
- Prowadzenie rejestru czynności przetwarzania
- Przepisy karne
- Przegląd zbiorów danych osobowych oraz programów służących do ich przetwarzania
- Przegląd treści Polityki Ochrony Danych Osobowych
- Zabezpieczenia fizyczne obszarów przetwarzania
- Zasady bezpiecznego użytkowania sprzętu IT
- Zasady bezpiecznego korzystania z oprogramowania
- Zasady bezpiecznego korzystania z internetu
- Zasady bezpiecznego korzystania z poczty elektronicznej
- Nadawanie upoważnień do przetwarzania danych osobowych
- instrukcja postępowania w przypadku wystąpienia incydentu
- Postępowanie dyscyplinarne

Potwierdzeniem odbytego szkolenia są wydane zaświadczenia o uczestnictwie w szkoleniu pn. „Ochrona danych osobowych w Urzędzie Gminy Krynice"

- rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

Odpowiedź: Rejestr czynności przetwarzania danych osobowych jest prowadzony. Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 12 lutego 2019 roku, II SAB/Łd 181/18, CBOSA rejestr czynności przetwarzania nie stanowi informacji publicznej.

- rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

Odpowiedź: Rejestr kategorii czynności przetwarzania jest prowadzony. Zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 12 lutego 2019 roku, II SAB/Łd 181/18, CBOSA rejestr kategorii czynności przetwarzania nie stanowi informacji publicznej.

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

Odpowiedź: Analiza ryzyka związanego z przetwarzaniem danych osobowych jest prowadzona. Analiza ryzyka jest dokumentem wewnętrznym.

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

Odpowiedź: Obowiązek informacyjny spełniany jest w momencie pobierania danych od osoby, której dane dotyczą. Klauzule informacyjne wywieszone są w siedzibie Administratora i w Biuletynie Informacji Publicznej BIP. Pozostałe klauzule zamieszczono na drukach oraz na wzorach wniosków. Obowiązek informacyjny wypełniany jest przy wszystkich czynnościach tego wymagających.

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

Odpowiedź: Obowiązek informacyjny z art. 14 RODO spełniany jest w sytuacji pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą. W przypadku gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator ma zastosowanie wyłączenie wskazane w art. 14 ust. lit. c. Klauzula z art. 14 jest stosowana z art. 6 ust. 1 lit. b RODO w stosunku do poręczycieli ZFŚS.

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

Odpowiedź: Tak, ostatni audyt w tym zakresie został wykonany w październiku 2018 r. Niezależnie IOD dokonuje okresowe sprawdzenia/przeglądy obowiązującej Polityki Ochrony Danych.

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

Odpowiedź na pytanie nr 14
Nie istnieje konflikt interesów przy pełnieniu funkcji IOD.

Pytanie 15) Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

Odpowiedź na pytanie nr 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 na pytanie nr 16
Tak, Urząd realizuje wymogi wynikające z a art. 13 i 14 RODO zgodnie z wymogami rozporządzenia m.in. poprzez obowiązek informacyjny wobec członków zarządu osób prawnych zamieszczając klauzulę informacyjną na umowie z podmiotami mającymi osobowość prawną.

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

Odpowiedź na pytanie nr 17
Klauzule informacyjne umieszczone są w siedzibie Administratora na tablicach informacyjnych oraz w miejscach obsługi interesantów. Klauzule informacyjne zostały również umieszczone na stronie internetowej Administratora oraz BIP.

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

Odpowiedź na pytanie nr 18
Tak

Ponadto informuję, że zgodnie z Pana wnioskiem odpowiedź niniejsza wraz z wnioskiem i petycją zostanie zamieszczona na stronie Biuletynu Informacji Publicznej Gminy Krynice w zakładce "Petycje"

W Ó J T
Jacek Wiśniewski