Czarna Białostocka, dn. 05 stycznia 2021 r.

GMINA
CZARNA BIAŁOSTOCKA

BURMISTRZ
CZARNEJ BIAŁOSTOCKIEJ

Znak pisma: RM.1431.109.2020

Pan Tomasz Piotrowicz

e-mail:

W odpowiedzi na wniosek z dnia 22 grudnia 2020 r. o udostępnienie informacji publicznej 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 są wykorzystywane systemy operacyjne Windows 7 lub starsze.

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

Tak Urząd opracował, ustanowił, eksploatuje, monitoruje i doskonali System Zarządzania Bezpieczeństwem Informacji. SZBI zawiera wymogi prawne w zakresie ochrony danych osobowych i bezpieczeństwa informacji oraz uwzględnia dobre praktyki wynikające z norm ISO serii 27000.

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 w zakresie bezpieczeństwa informacji został wykonany we wrześniu 2020 r. (data sprawozdania – 3.09.2020 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

Tak, posiada.

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

Pan Wojciech Skorulski, email: informatyk@czarnabialostocka.pl, telefon: 85 7131 360

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

W związku z aktualizację dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji, Urząd jest w trakcie wdrażania zaktualizowanych procedur – zgodnie z przyjętym przez Administratora Danych harmonogramem wdrożenia.

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

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

Tak, zostały przeprowadzone o których mowa w art. 108a Prawa Oświatowego w zakresie monitoringu wizyjnego.

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

Tak, w ostatnich trzech latach pracownicy urzędu uzupełniali wiedzę podczas szkoleń z zakresu dostępu do informacji publicznej/prowadzenia BIP/poprawnej obsługi wniosków o informację publiczną, szkolenia otwarte:

- 1 płatne w 2019 roku - 505 zł brutto, dostawcą szkolenia był Ośrodek Wspierania Administracji Lokalnej s.c. w Dobrzyniewie Dużym, udział wziął 1 pracownik;
- 3 bezpłatne, dostawcą szkoleń był Narodowy Instytut Samorządu Terytorialnego – w każdym udział wziął 1 pracownik.

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

Tak, zostały opracowane procedury – ujęte w ramach obowiązującego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Niezależnie Zespół IOD przeprowadził członkom personelu ADO szkolenia w zakresie stosowania zasad bezpieczeństwa informacji.

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:*

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

Odp.: Stanisław Sakowicz

iod_um_czarna_bial@podlaskie.pl

b) zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO;

Odp.: Zakres czynności zgodny z art. 39 RODO. W załączeniu przesyłam skan zawiadomienia o wyznaczeniu nowego inspektora ochrony danych.

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

Odp.: Doradztwo, opiniowanie, szkolenia i przeglądy w zakresie bezpieczeństwa informacji, w tym w ramach obowiązków nałożonych na Urząd jako jednostkę publiczną, a wynikających z rozporządzenia KRI i ustawy o krajowym systemie cyberbezpieczeństwie.

d) informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

Odp.: Ze względu na brak możliwości udziału w szkoleniach stacjonarnych w roku 2020 IOD uczestniczył w webinariach i wideo-konferencjach organizowanych przez PUODO.

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

Odp.: Zadania realizowane w zakresie obowiązków RODO są dokumentowane w formie załączników do Systemu Zarządzania Bezpieczeństwem Informacji.

f) *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)*

Odp.: Szkolenia w przedmiotowym zakresie są realizowane przez Zespół IOD w formie szkoleń stacjonarnych co najmniej 1 raz w roku.

Szkolenie prowadzone przez Inspektora Ochrony Danych Pana Wiesława Majewskiego.

Zakres szkolenia:

1. Inspektor Ochrony Danych –zadania;
2. Akty prawne regulujące przetwarzanie i ochronę danych osobowych;
3. Dane osobowe, definicja, pojęcia;
4. Rodzaje danych osobowych;
5. Przetwarzanie danych osobowych, pojęcia;
6. Warunki przetwarzania danych osobowych, dopuszczalność przetwarzania;
7. Czynności przetwarzania danych osobowych – rejestr czynności przetwarzania;
8. Prawa osób, których dane są przetwarzane – obowiązek informacyjny;
9. Powierzenie danych osobowych – umowa powierzenia;
10. Sankcje karne za naruszenie przepisów o ochronie danych osobowych;
11. Zasady bezpieczeństwa informacji;
12. Urząd Ochrony danych Osobowych zadania i kompetencje.

Szkolenie prowadzone przez Zespół Inspektora Ochrony Danych.

Zakres szkolenia:

1. Podstawowe akty prawne RODO,UODO i KRI;
2. Podstawowe definicje i formy danych osobowych;
3. Przesłanki legalności przetwarzania danych osobowych;
4. Obowiązek informacyjny i komunikacja z osobami, których dane dotyczą;
5. Wymagana dokumentacja: SZBI, Polityki ochrony danych i inne zabezpieczenia organizacyjne;

6. Inspektor Ochrony Danych;
7. Punkt konsultacyjny dla osób, których dane przetwarza administrator danych;
8. Powierzenie przetwarzania danych – Umowy powierzenia;
9. Przetwarzanie z upoważnienia administratora;
10. Rejestrowanie czynności przetwarzania;
11. Postępowanie w przypadku naruszeń ochrony danych;
12. Działania zwiększające świadomość personelu;
13. Zachowanie w tajemnicy informacji o zabezpieczeniach i pozyskanych danych;
14. Podstawowe zabezpieczenia informatyczne;
15. Odpowiedzialność: cywilna, karna i administracyjna wynikająca z RODO oraz prawa krajowego.

Szkolenia są dokumentowane poprzez imienne zaświadczenia stanowiące element dokumentacji kadrowej.

g) *rejestr czynności przetwarzania danych osobowych oraz jego zmiany.*

Odp.: Prowadzony jest rejestr czynności przetwarzania danych osobowych.

h) *rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.*

Odp.: Prowadzony jest rejestr kategorii czynności przetwarzania danych osobowych.

i) *dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych.*

Odp.: Analiza ryzyka związana z przetwarzaniem danych jest prowadzona.

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

Odp.: Urząd jest w trakcie wdrożenia zaktualizowanej Polityki realizacji obowiązku informacyjnego. Klauzule obowiązku informacyjnego są dostępne na stronie Biuletynu Informacji Publicznej Urzędu.

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

Odp.: Urząd jest w trakcie wdrożenia zaktualizowanej Polityki realizacji obowiązku informacyjnego. Klauzule obowiązku informacyjnego są dostępne na stronie Biuletynu Informacji Publicznej Urzędu.

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

Odp.: Tak, ostatni audyt w tym zakresie został wykonany we wrześniu 2020r. (data sprawozdania – 3.09.2020r.) Niezależnie IOD dokonuje okresowe sprawdzenia/przeglądy obowiązującego Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z przyjętym zakresem i harmonogramem.

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. Zakres zadań oraz sposób ich realizacji zostały opisane w wewnętrznej dokumentacji – Systemie Zarządzania Bezpieczeństwem Informacji.

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 art. 13 i 14 RODO zgodnie z wymogami rozporządzenia. Obowiązujące w Urzędzie zasady realizacji przedmiotowych obowiązku zostały poddane przeglądowi i aktualizacji. Urząd jest w trakcie wdrożenia zaktualizowanych zasad.

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

Odpowiedź na pytanie nr 17

Tak, Urząd realizuje wymogi wynikające z art. 13 i 14 RODO zgodnie z wymogami rozporządzenia. Obowiązujące w Urzędzie zasady realizacji przedmiotowych obowiązku zostały poddane przeglądowi i aktualizacji. Urząd jest w trakcie wdrożenia zaktualizowanych zasad.

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

IOD uczestniczy w realizacji obowiązków nałożonych na ADO z mocy Rozporządzenia RODO. Niezależnie udziela informacji i rekomendacji w bieżących sprawach związanych z przetwarzaniem danych osobowych.

Ze względu na brak obowiązku prawnego w tym zakresie oraz w oparciu o zakres, cele i sposoby przetwarzanych danych, Urząd podjął decyzję o nieformalizowaniu tego obszaru – zgodnie z zasadą proporcjonalności i adekwatności.

Ponadto informuję, że zgodnie z Pana wnioskiem odpowiedź niniejsza wraz z wnioskiem i petycją zostanie zamieszczona na stronie internetowej BIP Urzędu Miejskiego w Czarnej Białostockiej, w zakładce „Petycje"

(https://bip-umczarnabialostocka.wrotapodlasia.pl/petycje/).

Z up. BURMISTRZA

mgr Agnieszka Dyda
Z-CA BURMISTRZA