URZĄD MIASTA I GMINY
w STASZOWIE
ul. Opatowska 31, 28-200 Staszów

Staszów, 11.02.2021 rok

Znak: Or.1.1431.84.2020.III

Pan
Tomasz Piotrowicz
tomaszpiotrowiczzinformacjapub@gmail.com

W odpowiedzi na wniosek o udostępnienie informacji publicznej, Urząd Miasta i Gminy w Staszowie przesyła wnioskowane informacje.

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,

Ad 1) W chwili obecnej następuje wymiana systemów operacyjnych nie posiadających wsparcia producenta. Liczbę komputerów, na których jest zainstalowany system Windows 7 Pro szacujemy na 25 jednostek.

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.

Ad 2) Procedury wynikające z Polityki Bezpieczeństwa Informacji, o których mowa w Krajowych Ramach Interoperacyjności są zawarte w Polityce Ochrony Danych. Polityka ze względu na swój charakter przede wszystkim opis zabezpieczeń i różnych procedur nie podlega udostępnieniu, nawet w zakresie opisu dokumentu i procedur tam zawartych. Jest ona na bieżąco aktualizowana przez Inspektora Ochrony Danych i jest zgodna z przepisami prawa.

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.

Ad 3) W dniu 19.02.2020 r. w Urzędzie Miasta i Gminy w Staszowie został przeprowadzony audyt bezpieczeństwa informacji, o którym mowa w § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Audyt ten został wykonany przez zewnętrzną firmę na podstawie umowy dot. świadczenia usługi Inspektora Ochrony Danych, której integralną częścią jest wykonanie audytu bezpieczeństwa.

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 (…)

Ad 4) Urząd Miasta i Gminy w Staszowie posiada własny serwer poczty elektronicznej, w związku z tym nie zachodziła potrzeba zawarcia takiej umowy.

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

Ad 5)

- Kamil Malinowski, kamil.malinowski@staszow.pl **, nr tel. (15) 864 83-86;**

- Paweł Przewoźniak, pawel.przewozniak@staszow.pl **, nr tel. (15) 864 83-85**

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

Ad 6) Raport NIK był analizowany przez IOD i tam, gdzie było to zasadne, zostały podjęte w Urzędzie stosowne działania.

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

Ad 7) Urząd posiada BIP na własnym serwerze, w związku z tym nie zachodziła potrzeba zawarcia takiej umowy.

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

Ad 8) Brak żądań w 2020 roku wynikających z art. 15-21 RODO.

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?

Ad 9) W szkołach, dla których organem prowadzącym jest Gmina Staszów monitoring wizyjny został wprowadzony przed wejściem w życie przepisu 108a ustawy Prawo Oświatowe. Miało to na celu poprawę bezpieczeństwa w placówkach, co było przedmiotem rozmów pomiędzy dyrektorami, a organem prowadzącym.

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)

Ad 10) W ostatnich trzech latach pracownicy tut. Urzędu nie brali udziału w szkoleniach z zakresu dostępu do informacji publicznej/prowadzenia BIP/poprawnej obsługi wniosków o informację publiczną.

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?

Ad 11) IOD podjął realne działania w postaci opracowania odpowiednich procedur, które opisane są w Polityce Ochrony Danych. Brak jednak podstaw wskazania, jakie to procedury, ponieważ takie informacje nie stanowią informacji publicznej.

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?

Ad 12) Umowy nie zostały zawarte, ponieważ Urząd nie stworzył wyspecjalizowanej jednostki do obsługi kadrowo- administracyjnej jednostek oświatowych.

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;

Ad 13)

- Daniel Koguciuk

- Zakres czynności zgodny z art. 39 RODO. IOD został wyznaczony oraz zgłoszony do PUODO.

- IOD nie wykonuje innych czynności.

- IOD uczestniczy w szkoleniach z zakresu ochrony danych osobowych podnoszących kwalifikacje.

- Notatki, audyty, raporty prowadzone przez IOD.

- Pracownicy UMiG w Staszowie biorą udział w szkoleniach z zakresu „ Ochrona danych osobowych w świetle 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, praktyczne aspekty stosowania RODO". Udział w szkoleniu potwierdzany jest certyfikatem. IOD przeprowadził szkolenia pracowników w dniu: 14.05.2018 r., 22.05.2019 r. (skany list obecności na szkoleniach w załączeniu).

Podczas szkoleń poruszone zostały elementy zawarte w KRI, jednak dedykowanego szkolenia obejmującego kompleksowo omawiającego zadania wynikające z KRI nie było.

- Rejestr czynności przetwarzania danych osobowych jest prowadzony i podlega regularnym aktualizacjom a zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Łodzi, z dnia 12 lutego 2019 r., sygn. akt II SAB/Łd 181/18, rejestr nie stanowi informacji publicznej.

- Rejestr kategorii czynności przetwarzania danych osobowych jest prowadzony i podlega regularnym aktualizacjom a zgodnie z wyrokiem Wojewódzkiego Sądu Administracyjnego w Łodzi, z dnia 12 lutego 2019 r., sygn. akt II SAB/Łd 181/18, rejestr nie stanowi informacji publicznej.

- Dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych jest wykonywana regularnie.

- Obowiązek informacyjny jest zamieszczony na tablicy ogłoszeń w budynku Administratora oraz na stronie internetowej BIP w zakładce Obowiązek informacyjny. Obowiązek informacyjny jest realizowany na stanowiskach pracy, oraz w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego, mającego zastosowanie dla pracy w poszczególnych komórkach organizacyjnych jednostki.

- Urząd korzysta ze zwolnienia z realizacji obowiązku informacyjnego na podstawie art. 14 ust. 1 i 2, RODO znajduje zastosowanie, gdy zostanie spełniona jedna z przesłanek wyszczególnionych w art. 14 ust. 5 RODO.
- Audyty RODO wykonywane są przez IOD, niemniej jednak zgodnie z art. 38 ust. 5 RODO, działalność IOD podlega tajemnicy i dokumenty potwierdzające ich realizację nie mogą zostać udostępnione.

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 jakiejkolwiek 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.

Ad 14) Nie.

IOD nie jest pracownikiem Urzędu Miasta i Gminy w Staszowie. Funkcja IOD jest pełniona przez pracownika firmy zewnętrznej, zatem nie zachodzi konflikt interesów. IOD nie bierze również udziału w określaniu celów i sposobów przetwarzania danych.

15) Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

Ad 15) Tak.

IOD w ramach swoich zadań monitoruje przestrzeganie przepisów oraz wewnętrznych polityk, poprzez szkolenia, konsultacje dot. wymaganej dokumentacji (m.in. umowy powierzenia, klauzule informacyjne) oraz ściśle współpracuje z Administratorem.

16) Czy jednostka realizuje obowiązek wskazany w najnowszym stanowisku UODO? Jeśli proszę wskazać w jaki sposób.
https://uodo.gov.pl/pl/225/1577

Ad 16) Stanowisko UODO nie jest wiążącą podstawą prawną, jest to kierunek podejmowania pewnych działań, jednak nie może być uznawane za wiążące. Obowiązek informacyjny jest realizowany w sposób zatwierdzony przez Administratora.

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

Ad 17) Obowiązek informacyjny jest realizowany w sposób zatwierdzony przez Administratora, w zależności od rodzaju realizowanego zadania i wymogów prawnych w zakresie spełniania obowiązku informacyjnego.

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

Ad 18) Tak, funkcjonują.

Burmistrz Miasta i Gminy Staszów

/-/ Leszek Kopeć

Otrzymują:
1) adresat
2) a/a

OBOWIĄZEK INFORMACYJNY

Na podstawie art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.U.UE.L. z 2016r. Nr 119, s.1 ze zm.) - dalej: „RODO" informuję, że:

1) Administratorem Państwa danych jest Urząd Miasta i Gminy w Staszowie.
2) Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: inspektor@cbi24.pl lub pisemnie na adres Administratora.
3) Państwa dane osobowe będą przetwarzane w celu udzielenia odpowiedzi na wniosek o udostępnienie informacji publicznej, jak również w celu realizacji praw oraz obowiązków wynikających z przepisów prawa (art. 6 ust. 1 lit. c RODO).
4) Państwa dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach szczególnych, w tym przepisów archiwalnych.
5) Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegać profilowaniu.
6) Państwa dane osobowe nie będą przekazywane poza Europejski Obszar Gospodarczy (obejmujący Unię Europejską, Norwegię, Liechtenstein i Islandię).
7) W związku z przetwarzaniem Państwa danych osobowych, przysługują Państwu następujące prawa:
   a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
   b) prawo do sprostowania (poprawiania) swoich danych osobowych;
   c) prawo do ograniczenia przetwarzania danych osobowych;
   d) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa), w sytuacji, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO);
8) Podanie przez Państwa danych osobowych jest obowiązkowe. Nieprzekazanie danych skutkować będzie brakiem realizacji celu, o którym mowa w punkcie 3.
9) Państwa dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych osobowych, a także podmiotom lub organom uprawnionym na podstawie przepisów prawa.