URZĄD MIEJSKI
ul. Stanisława Moniuszki 6
06-200 Maków Mazowiecki
woj. mazowieckie
tel. 29 71 71 002

Maków Mazowiecki, 28.12.2020 r.

WO.1431.12.2020

Sz. P. Tomasz Piotrowicz
Proton
Odział w Krośnie,
Nowym Sączu, Zakopanem

W odpowiedzi na Pana wniosek o udzielenie informacji publicznej z dnia 21.12.2020 r. poniżej przesyłam odpowiedź na zadane pytania.

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,**

Szacunkowa liczba oprogramowania użytkowanego w Urzędzie Miejskim nieposiadającego wsparcia producenta to 10 stanowisk.

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.**

Urząd Miejski w Makowie Mazowieckim posiada Politykę Ochrony Danych Osobowych. Zostały w niej określone obowiązki osób, przetwarzających dane osobowe, a także ich odpowiedzialność za dane. Wdrożono procedury dotyczące m. in. nadawania i odbierania upoważnień, tworzenia kopii zapasowych, wykonywania przeglądów i konserwacji, zarządzania systemem monitoringu wizyjnego, przeprowadzania szkoleń, czy zarządzania ryzykiem. Zostały wyznaczone odpowiednie zbiory danych, a opisane środki ochrony są adekwatne do zagrożeń oraz sposobów realizacji obowiązków wynikających z ogólnego rozporządzenia o ochronie danych.

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.

Ostatni audyt odbył się w dniu 2.11.2020 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 (...)**

Tak.

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**

Firma NetBis, pracownik Hubert Brzostek, email: hubert.brzostek@netbis.pl

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

Tak, wdrożyliśmy prawie wszystkie zalecenia NIK. Jesteśmy na etapie realizacji prowadzenia aktualnej i kompletnej elektronicznej ewidencji sprzętu informatycznego.

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**

Tak, została podpisana umowa.

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

Nie wystąpiły takie sytuacje.

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?**

Tak.

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).**

W ostatnich trzech latach pracownicy nie brali udziału w takich szkoleniach.

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?

Każdy pracownik posiada swoje loginy i hasła dostępu do komputera oraz programów zawierających dane osobowe. Zostało to opisane w Polityce Ochrony Danych Osobowych.

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?

Na terenie Miasta nie funkcjonuje CUW. Pomiędzy jednostkami oświatowymi a miastem Maków Mazowiecki (organem prowadzącym) zawarto umowy powierzenia danych.

13) **Wnosimy o informację w zakresie:**

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

Inspektorem Ochrony Danych Osobowych jest Pani Agnieszka Szołtysek.

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

Zakres czynności wynika z art. 39 RODO, a także podpisanej umowy w zakresie outsourcingu funkcji IOD. Inspektor został wyznaczony Zarządzeniem Burmistrza Miasta, zaś Urząd Miejski w Makowie Mazowieckim dokonał zgłoszenie IOD.

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

IOD nie wykonuje innych czynności.

- **informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.**

Informacje dot. szkoleń w zakresie ochrony danych dla IOD można znaleźć na stronie: www.grupaformat.pl

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

Dokumentacja dot. realizacji zadań IOD jest tworzona na bieżąco.

- **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**

Pracownicy są szkoleni przez firmę zewnętrzną na platformie udostępnionej przez Grupę Format. Każdy pracownik po zapoznaniu się z materiałami szkoleniowymi przystępuję do rozwiązania testu. Osoba, która otrzyma pozytywną ocenę otrzymuje certyfikat, którego kopia znajduje się w aktach osobowych pracownika.

- **rejestr czynności przetwarzania danych osobowych oraz jego zmiany**

Przygotowany został Rejestr Czynności Przetwarzania Danych w Urzędzie.

- **rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.**

Przygotowany został Rejestr Kategorii Czynności Przetwarzania w Urzędzie.

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

Przygotowana została analiza ryzyka w zakresie ochrony danych w Urzędzie.

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

Obowiązek informacyjny (art. 13 i 14 RODO) jest spełniony poprzez publikację klauzul na stronie internetowej https://www.makowmazowiecki.pl/300,klauzule-informacyjne, w siedzibie Urzędu na tablicach informacyjnych oraz w toku prowadzonych spraw.

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

Przeprowadzane są audyty w zakresie RODO. Z każdego Audytu sporządzany jest protokół.

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.

Nie istnieje konflikt interesów przy pełnieniu funkcji IOD w Urzędzie Miejskim w Makowie Mazowieckim.

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

Klauzula informacyjna przedstawiana jest przy pierwszym kontakcie (np. podczas podpisywania umowy).

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

Obowiązki informacyjne względem osób, których dane dotyczą realizowane są poprzez umieszczanie klauzul informacyjnych RODO na stronie Urzędu Miejskiego, na tablicach informacyjnych Urzędu Miejskiego w Makowie Mazowieckim oraz prowadzonej korespondencji.

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

Tak.

Zgodnie z art. 13 ust. 1 Ogólnego Rozporządzenia o Ochronie Danych (RODO) informujemy, że:

1) administratorem danych osobowych **osób wnioskujących o udostępnienie informacji publicznej** jest Burmistrz Miasta Maków Mazowiecki, adres: ul. Stanisława Moniuszki 6;
2) administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować w sprawach przetwarzania Państwa danych osobowych za pośrednictwem poczty elektronicznej: urzad@makowmazowiecki.pl;
3) administrator będzie przetwarzał Państwa dane osobowe na podstawie art. 6 ust. 1 lit. c) RODO, tj. w celu wypełnienia obowiązku prawnego ciążącego na administratorze przewidzianego w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej;
4) dane osobowe mogą być udostępnione innym uprawnionym podmiotom, na podstawie przepisów prawa, a także na rzecz podmiotów, z którymi administrator zawarł umowę powierzenia danych w związku z realizacją usług na rzecz administratora (np. kancelarią prawną, dostawcą oprogramowania, zewnętrznym audytorem, zleceniobiorcą świadczącym usługę z zakresu ochrony danych osobowych);
5) administrator nie zamierza przekazywać Państwa danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
6) mają Państwo prawo uzyskać kopię swoich danych osobowych w siedzibie administratora.

Dodatkowo zgodnie z art. 13 ust. 2 RODO informujemy, że:

1) Państwa dane osobowe będą przechowywane przez okres przewidziany w przepisach prawa, tj. w ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz w Rozporządzeniu Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej;;
2) przysługuje Państwu prawo dostępu do treści swoich danych, ich sprostowania lub ograniczenia przetwarzania, a także prawo do wniesienia skargi do organu nadzorczego;
3) podanie danych osobowych jest dobrowolne, jednakże niezbędne do realizacji ww. celów. Konsekwencją niepodania danych będzie nierozpatrzenie skargi lub wniosku;
4) administrator nie podejmuje decyzji w sposób zautomatyzowany w oparciu o Państwa dane osobowe.