Gołdap, 16.12.2022 r.

Burmistrz Gołdapi

Plac Zwycięstwa 14

19-500 Gołdap

WA.1431.124.2022

*Dotyczy: wniosku o udostępnienie informacji publicznej z dnia 05.12.2022 r.*

Na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) odpowiadając na wniosek o udostępnienie informacji publicznej z dnia 06.11.2022 r. informuję co następuję:

1. Czy organ udostępnił Poczcie Polskiej danych z rejestru PESEL na potrzeby organizacji „kopertowych” wyborów? Na chwilą obecną toczą się postępowania w sprawie wójtów GMIN: TOKARNIA; LUBIEŃ   
   I INNI. Informacja jest niezwykle ważna celem wysłania zawiadomień do odpowiednich organów   
   i fundacji Watchdog?

Odp.: *Burmistrz Gołdapi nie udostępnił Poczcie Polskiej danych z rejestru PESEL.*

1. W przypadku udostępnienia danych Poczcie Polskiej czy taka informacja była konsultowana   
   z prawnikami czy Inspektorem Ochrony Danych? Jeśli tak jakie stanowisko zajęli prawnicy czy Inspektor Ochrony Danych?

Odp.: *Nie dotyczy.*

1. Czy Państwa jednostka korzysta z usług osób fizycznych lub podmiotów zewnętrznych w zakresie pełnienia obowiązków Inspektora Ochrony Danych, a jeżeli tak prosimy o podanie: daty zawarcia i zakończenia obowiązywania umowy?

Odp.: *Urząd Miejski w Gołdapi korzysta z usług podmiotu zewnętrznego w zakresie pełnienia* *obowiązków Inspektora Ochrony Danych.*

*Data zawarcia 29 grudnia 2021 r. (obowiązuje od 1 stycznia 2022 r.).*

*Data zakończenia 31 grudnia 2022 r.*

1. UODO nałożył administracyjną karę pieniężną w wysokości 8 tys. zł na wójta gminy Dobrzyniewo Duże za niezapewnienie odpowiedniego bezpieczeństwa danych osobowych, brak wdrożenia odpowiednich środków technicznych i organizacyjnych, brak odpowiednich regulacji wewnętrznych:

<https://uodo.gov.pl/pl/138/2487?fbclid=IwAR3IrqDhElG__mAfaXoCH3ulpttBC9H3ApB0RgfcYkpU-CBTy_tuQ0yOzaE>

<https://www.uodo.gov.pl/decyzje/DKN.5131.8.2022>.

Między innymi w  stanie faktycznym przedmiotowej sprawy, ryzyko dotyczyło zagrożenia polegającego na kradzieży służbowego sprzętu komputerowego z prywatnego mieszkania pracownika Urzędu Gminy Dobrzyniewo Duże. Dlatego w naszym  wniosku pytamy: jakie środki i procedury wdrożono odnośnie wynoszenia sprzętu oraz korzystania z prywatnego sprzętu IT?

Odp.: *Zasady określa:*

*- Zarządzenie Nr 804/X/2020 Burmistrza Gołdapi z dnia 16 października 2020 r. w sprawie wprowadzenia Regulaminu pracy zdalnej w Urzędzie Miejskim w Gołdapi,*

*- Zarządzenie Nr 123/II/2019 Burmistrza Gołdapi z dnia 19 lutego 2019 r. w sprawie wprowadzenia „Polityki Ochrony Danych Osobowych” w Urzędzie Miejskim w Gołdapi m.in.:*

*Procedura korzystania z internetu.*

*Procedura korzystania z komputera służbowego.*

*Procedura korzystania z urządzeń przenośnych.*

1. Powierzenie przetwarzania danych trzeba udokumentować zgodnie z <https://uodo.gov.pl/pl/138/2450>. Żądamy informacji czy IOD uczestniczy w opiniowaniu czy przygotowaniu umów powierzenia? W jakich sytuacjach podmiot zawiera umowy powierzenia?

Odp.: *Tak, IOD uczestniczy w opiniowaniu czy przygotowaniu umów powierzenia.*

*Urząd Miejski w Gołdapi zawiera umowy powierzenia w każdym przypadku gdy dochodzi do udostępnienia danych osobowych innym podmiotom w inny sposób niż regulowany przepisami prawa.*

W jaki sposób dokonuje się weryfikacji podmiotu przetwarzającego jeszcze przed podpisaniem umowy powierzenia? Czy w tym procesie uczestniczy IOD?

Odp.: *W każdej umowie sprawdzane są zapisy dot. klauzul poufności.*

1. Mamy już pełną listę pytań jakie PUODO kieruje do administratorów danych weryfikując sposób realizacji przez nich przepisów dotyczących Inspektorów Ochrony Danych - link do strony UODO z pełną informacją   
   i wszystkimi pytaniami na stronie UODO. My uprzedzając UODO  mamy  kilka wybranych pytań (numeracja zgodnie z tą stosowaną przez PUODO).  I przy okazji zwracam uwagę na pytania dotyczące wykonywanych zadań przez IOD'a, w tym audytów

Wybrane pytania jakie zadajemy i oczekujemy odpowiedzi jako informacja publiczna:

a)     na podstawie jakich kwalifikacji administrator wyznaczył IOD (np. wykształcenie, doświadczenie, wiedza prawnicza)?  Proszę wykazać wiedzę lub wykształcenie prawniczą. Przypominamy, że  IOD jest [wyznaczany](https://uodo.gov.pl/pl/121/193) na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 [RODO](https://uodo.gov.pl/pl/131/539). Bardzo dużo Urzędów nie weryfikuje kwalifikacji IOD i wyznacza IOD (firmy zewnętrzne informatyczne, informatycy)

Odp.: *Administrator wyznaczył IOD zgodnie z rozporządzeniem RODO oraz podpisaną umową w zakresie pełnienie obowiązków IOD. Wykonawca posiada wieloletnie doświadczenie zarówno w zarządzaniu procesami ochrony danych osobowych jak i systemami IT. Od 2016 roku świadczył usługi ABI i ASI   
w jednostkach administracji publicznej, a od 2018 roku wdraża RODO zarówno w jednostkach administracji publicznej jak i w sektorze ochrony zdrowia, NGO a także w podmiotach działających w branży produkcyjnej, handlowej, hotelarskiej, itp..*

10.  Czy IOD przeprowadza szkolenia? Jeśli nie to kto odpowiada za szkolenia pracowników pod kątem RODO   
i KRI? W jaki sposób potwierdza się skuteczność szkoleń?

Odp.: *Tak, IOD przeprowadza szkolenia zarówno indywidualne dla każdej osoby dopuszczonej do przetwarzania danych (pracownicy, stażyści praktykanci) jak i szkolenia tematyczne grupowe.*

11.  Wyjaśnienia jak w praktyce zapewniono niezależność IOD od Administratora Danych i brak konfliktu interesów w szczególności jeśli IOD realizuje także inne obowiązki;

Odp.: *Usługę świadczy podmiot zewnętrzny - osoba pełniąca IOD wykonuje tylko zadania w zakresie wynikającym z przepisów dotyczących ochrony danych osobowych, w szczególności RODO.*

12.  Czy IOD ocenia i/lub opracowuje wzory dokumentów w Państwa organizacji pod kątem zgodności z RODO?

Odp.: *Tak.*

13.  Czy IOD monitoruje przestrzeganie przepisów RODO lub wewnętrznych przepisów dot. ochrony danych osobowych w Państwa jednostce, a jeżeli tak to w jaki sposób?

Odp.: *Tak, raz w roku przeprowadzane jest kompleksowe szacowanie ryzyka dla bezpieczeństwa danych osobowych pod kątem integralności dostępności oraz poufności danych osobowych całego obszaru przetwarzania danych. IOD pozostaje w stałym kontakcie z pracownikami urzędu, na bieżąco monitorując poprawność procesów przetwarzania danych.*

14.  Jeżeli zgodnie z art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000) udostępniono na stronie internetowej dane inspektora ochrony danych (imię nazwisko, adres email oraz telefon) to proszę o podanie miejsca publikacji na stronie internetowej (dokładnego odnośnika URL) czy też wskazany obowiązek nie został spełniony?

Odp.: *Dane dot. ochrony danych znajdują się w poniższych linkach:*

<https://www.goldap.pl/pl/229/24050/rodo-klauzula-informacyjna-o-przetwarzaniu-danych-osobowych.html>

15.  Czy dla każdej czynności przetwarzania jest opracowana klauzula informacyjna RODO?

Odp.: *Tak.*

16.  Czy w podmiocie był przeprowadzany audyt z KRIO: zgodnie z Rozporządzeniem R. M. 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 (Dz. U. z 2012r. poz. 526) zgodnie z § 20 ust.2 pkt 14) KRI

Odp.: *Tak.*

17.  Czy podmiot dysponuje całościową Polityką Bezpieczeństwa Informacji, wymaganą w § 20 ust. 1   
i 3 ww. Rozporządzenia oraz polityki ochrony danych, rejestrów czynności, analiz ryzyka wraz   
z procedurami? Jeśli odpowiedź jest twierdząca - wnosimy o krótkie - w kilku ogólnych zdaniach - opisanie przedmiotowej polityki oraz procedur?

Odp.: *W Urzędzie Miejskim w Gołdapi wprowadzono „Politykę Ochrony Danych Osobowych” z kompletem procedur charakterystycznych dla całościowej Polityki Bezpieczeństwa Informacji oraz stosownymi rejestrami i wzorcowym szablonem analizy ryzyka wraz z instrukcją jej przeprowadzania.*

18.  Czy zgodnie z art. 20 ust. 2 pkt 14 KRI (*Rozporządzenie 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*) realizują Państwo w jednostce okresowy (nie rzadziej niż raz na rok) audyt wewnętrzny w zakresie bezpieczeństwa informacji? Jeśli tak to proszę o wskazanie:

Odp.: *Tak.*

W przypadku jeżeli audyt przeprowadzał podmiot zewnętrzny:

1. danych podmiotu (nazwa + siedziba), z którym została zawarta taka umowa;
2. daty zawarcia umowy;
3. całkowitej wartości brutto umowy;
4. terminu wykonania ostatniego audytu KRI;
5. w jaki sposób udokumentowany jest audyt;

Odp.: *od 1 do 5 - W związku z tym, że wnioskodawca nie określił za jaki okres żąda ww. informacji proszę   
o doprecyzowanie w tym zakresie.*

Jednocześnie proszę o przedłożenie (przesłanie na adres e-mail podany poniżej) kopii (skanu) umowy   
z podmiotem zewnętrznym w zakresie realizacji okresowego audytu w zakresie bezpieczeństwa informacji;

W przypadku jeżeli audyt przeprowadzał pracownik lub współpracownik jednostki:

1. imienia i nazwiska osoby lub osób przeprowadzających audyt KRI;
2. daty wykonania ostatniego audytu;
3. w jaki sposób udokumentowany jest audyt;
4. jakie osoba przeprowadzająca audyt posiada doświadczenie i kwalifikacje?

Odp.: *od 1 do 4 – Nie dotyczy.*

Czy zgodnie z wymogiem art. 20 ust. 1 ww. *Rozporządzenia* Państwa jednostka opracowała   
i ustanawiła, wdrożyła i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność́, dostępność́ i integralność́ informacji z uwzględnieniem takich atrybutów, jak autentyczność́, rozliczalność́, niezaprzeczalność́ i niezawodność́?

Czy zarzadzanie bezpieczeństwem informacji w Państwa jednostce realizowane jest poprzez realizację   
i egzekwowanie działań wskazanych w art. 20 ust. 2 ww. Rozporządzenia?

*Odp.: Tak.*

W jaki sposób ww. działania, wskazane w art. 20 ust. 2 ww. Rozporządzenia, są realizowane?

***Odp.:*** *Urząd Miejski w Gołdapi posiada system elektroniczny do ewidencji sprzętu i oprogramowania, raz   
w roku przeprowadzana jest analiza ryzyka, zarządzenie uprawnieniami określa Procedura kontroli dostępu do systemu informatycznego.*

19. Czy macie Państwo wyznaczoną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zgodnie z wymogiem art. 21 *ustawy z dnia 5 lipca 2018 r.   
o Krajowym Systemie Cyberbezpieczeństwa*? Jeśli tak to proszę o wskazanie:

Czy, zgodnie z art. 22 ust. 1 pkt 5 ww. ustawy dane tej osoby zostały przekazane do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV?

Odp.: *Tak.*

Jakie ta osoba posiada doświadczenie i kwalifikacje?

*Odp.: Wykształcenie wyższe informatyczne, 12 letni staż pracy na stanowisku informatyka w służbach administracji rządowej i w jednostkach samorządowych.*

W jaki sposób w Państwa jednostce zapewnione jest zarządzanie incydentem?

*Odp.: Zarządzanie incydentem w Urzędzie Miejskim w Gołdapi określa Procedura postępowania   
z incydentami bezpieczeństwa informacji.*

Czy Państwa jednostka zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń́ cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się̨ przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

Odp.: *Tak.*

19.  Jakie zostały wprowadzone zmiany w zakresie wytycznych EROD dotyczących zgody na przetwarzanie danych oraz w sprawie praw :[https://edpb.europa.eu/guidelines-your-rights\_pl](https://edpb.europa.eu/guidelines-your-rights_pl" \t "_blank)

Odp.: *Zmodyfikowano procedurę realizacji żądań podmiotu danych regulującą powyższe zagadnienie.*

20.  Czy podmiot  posiada  procedurę w zakresie oceny powagi naruszeń według wymagań EROD <https://edpb.europa.eu/about-edpb/about-edpb_pl>?

Odp.: *Stosujemy wdrożoną procedurę postępowania z naruszeniami danych osobowych oraz procedurę postępowania z incydentami bezpieczeństwa informacji regulujące powyższe zagadnienie.*

Z poważaniem

Z up. BURMISTRZA

Sekretarz Gminy Gołdap

mgr Anna Rawinis

Sporządził: Piotr Mietliński i Sebastian Liwak.

Sprawdziła: Anna Rawinis.