Inowłódz, 15 grudnia 2022 r.

Urząd Gminy Inowłódz
ul. Spalska 2
97-215 INOWŁÓDZ
pow. tomaszowski, woj. łódzkie
tel./fax (44) 710-12-33
NIP 773-16-47-317

RO.1431.59.2022

Odpowiedzi na wniosek z dnia 5 grudnia 2022 r.

Pyt. nr 1. Urząd nie udostępnił Poczcie Polskiej danych z rejestru PESEL na potrzeby organizacji „Kopertowych" wyborów.

Pyt. nr 2. Nie dotyczy.

Pyt. nr 3. Urząd nie korzysta z usług zewnętrznych w zakresie pełnienia IOD.

Pyt. nr 4. Nie dotyczy.

Pyt. nr 5. IOD uczestniczy w przygotowywaniu opiniowaniu umów powierzenia.

Pytanie z numeracji UODO. IOD zatrudniony w Urzędzie nie jest prawnikiem, posiada duże doświadczenie zawodowe.

Pyt nr 10. Czy IOD przeprowadza szkolenia? IOD organizuje i przeprowadza szkolenia. Jaka skuteczność szkoleń? – np. brak naruszeń w urzędzie.

Pyt. nr 11. IOD bezpośrednio podlega Administratorowi. Brak konfliktu interesów.

Pyt. nr 12. IOD opracowuje wzory dokumentów zgodnie z RODO.

Pyt. nr 13. IOD monitoruje przestrzeganie przepisów RODO – np. polityka dostępu do stacji roboczych oraz do plików i programów.

Pyt nr 14. Odnośnik URL:
https://bip.inowlodz.pl/urzad-gminy/inspektor-danych-osobowych/5104-inspektor-ochrony-danych

Pyt. nr 15. Tak klauzula ogólna lub szczególna.

Pyt. nr 16.
W związku z realizacją zadania Cyfrowa Gmina we wrześniu 2022 roku wykonaliśmy audyt diagnozy cyberbezpieczeństwa w Urzędzie.
Budżet Gminy Inowłódz nie przekracza 40 000 zł - poniżej wyjaśnienia:
Kolegium Regionalnej Izby Obrachunkowej w Opolu z dnia 4 marca 2013 r. NA.III.-0221-4/2013.

Kierownik Referatu Organizacyjnego

TEZA aktualna

Na mocy przepisu § 20 ust. 2 pkt 14 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, kierownictwo podmiotu publicznego, poza wyjątkami przewidzianymi w art. 2 ust. 3 i 4 ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235), jest zobowiązane do zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

UZASADNIENIE

Uzasadnienie faktyczne

Regulacje prawne dotyczące audytu wewnętrznego zostały zamieszczone w ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2009 r. Nr 157, poz. 1240, z późn. zm.). Zgodnie z art. 274 ust. 3 powołanej ustawy, audyt wewnętrzny prowadzi się w jednostkach samorządu terytorialnego, jeżeli ujęta w uchwale budżetowej jednostki samorządu terytorialnego kwota dochodów i przychodów lub kwota wydatków i rozchodów przekroczyła wysokość 40.000 zł. Audyt wewnętrzny prowadzi się również w jednostkach sektora finansów publicznych, których kierownicy podejmą decyzję o prowadzeniu audytu wewnętrznego (art. 274 ust. 4 powołanej ustawy).

Z dniem 31 maja 2012 r. weszło w życie 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 (Dz. U. z 2012 r. poz. 526). Na mocy przepisu § 20 ust. 2 pkt 14 tego aktu, kierownictwo podmiotu publicznego, poza wyjątkami przewidzianymi w art. 2 ust. 3 i 4 ustawy z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235), jest zobowiązane do zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. W tak ukształtowanym stanie prawnym audytor wewnętrzny - usługodawca niezależnie od wyników analizy ryzyka powinien corocznie objąć audytem wewnętrznym powyższy obszar, chyba że zostaną spełnione warunki określone w § 20 ust. 3 ww. rozporządzenia. Jeżeli realizacja zadania audytowego we wskazanym obszarze będzie konieczna ze względu na niespełnienie ww. warunków, wówczas zadanie to jako obligatoryjne należy ująć w rocznym planie audytu, o ile jednostka jest zobligowana do prowadzenia audytu wewnętrznego na mocy powołanych przepisów ustawy o finansach publicznych.

Pyt. nr 17. Urząd posiada Politykę Bezpieczeństwa Informacji.

1. Polityka Bezpieczeństwa Informacji zwana dalej „Polityką" jest **dokumentem wewnętrznym Urzędu Gminy Inowłódz i nadrzędnym dla innych procedur oraz regulaminów z zakresu ochrony danych osobowych przyjętych w Urzędzie Gminy.**
2. Celem niniejszego dokumentu jest wprowadzenie spójnych zasad zachowania bezpieczeństwa danych osobowych w Urzędzie Gminy Inowłódz, zwanym dalej urzędem, zgodnie z Rozporządzeniem 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, zwanym w dalszej części Polityki „RODO".
3. Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania system chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających urzędem oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby obsługujące systemy przetwarzające dane osobowe są ogniwem

zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

4. Zastosowanie niniejszej polityki powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych oraz w systemach informatycznych urzędu.
5. Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.
6. Polityka dotyczy wszystkich danych przetwarzanych przez Urząd Gminy Inowłódz, niezależnie od formy przetwarzania danych oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych. Polityka reguluje w szczególności przetwarzanie danych w zbiorach ewidencyjnych prowadzonych w formie papierowej oraz systemach informatycznych.

W związku z realizacją zadania Cyfrowa Gmina we wrześniu 2022 roku wykonaliśmy audyt diagnozy cyberbezpieczeństwa w Urzędzie.

Pyt. nr 18. Pierwsza część pytania -nie dotyczy. Druga część. W urzędzie w miarę potrzeb realizowane są zadania z poniższego paragrafu.

§ 20. System zarządzania bezpieczeństwem informacji

1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
   W urzędzie zarządzanie bezpieczeństwem informacji realizowane jest poprzez egzekwowanie działań wskazanych w poniższym art. w odniesieniu do zapisów dotyczących urzędu
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:
   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
      a) zagrożenia bezpieczeństwa informacji,
      b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
      c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
   7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
      a) monitorowanie dostępu do informacji,

b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
a) dbałości o aktualizację oprogramowania,
b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

Zapytanie bez numeracji strona 5 dotyczące osoby odpowiedzialnej za cyberbezpieczeństwo.
Urząd wyznaczył osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
https://bip.inowlodz.pl/images/zarzadzenia/2020/Zarz%C4%85dzenie_Nr_32_2020_W%C3%B3jta_Gminy_Inow%C5%82%C3%B3dz.pdf

Pyt. nr 17. Powiadomiono NASK. Osoba wyznaczona posiada długoletnie doświadczenie zawodowe. W PBI określono sposób zarządzania incydentem. O ewentualnych zagrożeniach np. wydanych Zarządzeniach o alarmie ALFA CRP wszyscy pracownicy są informowani i zobowiązani do zgłaszania niejasnych treści do wyznaczonej osoby.

Pyt. nr 19. Nie zachodzi konieczność wprowadzenia zmian w zakresie zgody na przetwarzanie danych wynikających z wytycznych Europejskiej Rady Ochrony Danych.

Pyt. nr 20. Urząd posiada stosowną procedurę w zakresie naruszeń mieści się ona w wymaganiach Europejskiej Rady Ochrony Danych.
IOD nie wydał rekomendacji, aby udostępnić dane Poczcie Polskiej. Wręcz to IOD przestrzegał Administratora o braku przesłanek do procedury wydania danych, co potwierdziło doświadczenie i reagowanie IOD w ewentualnych sytuacjach mających znamiona incydentu.

WÓJT
Bogdan Rącki