URZĄD GMINY GRÓDEK
ul. A. i G. Chodkiewiczów 2
16-040 GRÓDEK
tel. 85 718 06 64, fax 85 811 00 10

Gródek, dnia 5 stycznia 2021 r.

IOD.1431.5.2020

Pan Tomasz Piotrowicz
tomaszpiotrowicz_informacjapubl@protonmail.com

W odpowiedzi na wniosek o udostępnienie informacji publicznej z dnia 22 grudnia 2020 r. na podstawie art. 10 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176) uprzejmie informuję, zgodnie z wnioskowanym zakresem informacji:

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,

   W chwili obecnej posiadamy 11 stacji roboczych z zainstalowanym Systemem operacyjnym Windows 7, nieposiadającym wsparcia producenta oprogramowania. W roku bieżącym planowane jest wyeliminowanie tego problemu.

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.

   PBI określa podstawowe zasady, normy i wymagania zgodności w zakresie bezpieczeństwa informacji przetwarzanej w Urzędzie. Dotyczy wszystkich pracowników w Urzędzie oraz osób mających dostęp do chronionych informacji. Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy w jakiej są przechowywane (papierowej, elektronicznej i innej), z wyjątkiem informacji niejawnych. Obszar informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada także struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformacyjnych. Dokument ten dotyczy również wszystkich systemów informatycznych zlokalizowanych w budynkach Urzędu z wyjątkiem systemów służących do przetwarzania informacji niejawnych.

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 wewnętrzny audyt z zakresu bezpieczeństwa informacji został przeprowadzony w listopadzie 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 (...)

Urząd posiada obowiązującą umowę główną z firmą świadczącą usługi w zakresie hostingu oraz umowę powierzenia przetwarzania danych, sporządzoną zgodnie z normami wynikającymi z Rozporządzenia 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 (...).

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

Piotr Supronik – Informatyk, admin@grodek.pl , tel. 857180664.

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

Pojedyncze zalecenia w zakresie informatycznym są w trakcie realizacji.

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

Gmina Gródek posiada zawartą i obowiązującą umowę powierzenia przetwarzania w zakresie administrowania systemem Biuletynu Informacji Publicznej.

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

Nie było takich żądań.

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. Szkoła podstawowa w Gródku konsultowała z Wójtem możliwość zakupu monitoringu w szkole, gdyż dany wydatek musiał być uwzględniony w planie finansowym placówki.

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 2017 r. – 1 pracownik – koszt brutto szkolenia 490,00 zł, szkolenie otwarte wyjazdowe, organizator: Fundacja Rozwoju Demokracji Lokalnej – Podlaskie Centrum, ul. Choroszczańska 31, 15-742 Białystok.

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?

W Urzędzie obowiązuje Polityka Bezpieczeństwa Informacji oraz Polityka Ochrony Danych Osobowych Przetwarzanych w Urzędzie. Oba te dokumenty są aktualizowane w razie potrzeb. Zawierają opis procedur i postępowania również w zakresie mającym na celu zapewnienie odpowiednich środków bezpieczeństwa przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych w Urzędzie. Dokumentacja w w/w zakresie służy analizie środków bezpieczeństwa i procedur bezpiecznego przetwarzania danych osobowych. Dokumentacja jest opracowywana w związku z koniecznością wypełnienia obowiązku nałożonego na Administratora Danych Osobowych, mającego na celu zapewnienie właściwej, adekwatnej dla danej jednostki

ochrony przetwarzanych danych. Udostępnianie na zewnątrz takich informacji może osłabić ich skuteczność, przez co zagraża właściwej ochronie 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?

    Nie dotyczy.

13. Wnosimy o informację w zakresie:

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

    Katarzyna Barszczewska, iodo@grodek.pl, tel. 857180664

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

    Zakres czynności jest tożsamy z art. 39 RODO, ponadto obejmuje wykonywanie przez IOD rejestru czynności przetwarzania, uczestnictwo w podejmowaniu decyzji dotyczących przetwarzania danych, konsultowanie zgłoszeń w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi; dokonywanie analiz zachodzących zmian i przygotowywanie opracowań o charakterze analitycznym, mającym znaczenie dla decyzji podejmowanych przez Wójta; kompletowanie i prezentowanie odpowiednich materiałów dotyczących aktualnych wydarzeń mających wpływ na funkcjonowanie gminy; sporządzanie okresowych sprawozdań, analiz i informacji. Zawiadomienie o wyznaczeniu IOD do PUODO zostało wysłane w terminie o którym mowa w art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

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

    Nie.

    d) informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

    IOD w roku 2020 uczestniczył w dwóch szkoleniach oraz w warsztatach z zakresu analizy ryzyka oraz DPIA w zakresie przetwarzania danych.

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

    Realizacja wszelkich zadań IOD posiada odzwierciedlenie w teczkach prowadzonych przez niego spraw.

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)

W dniu 17 kwietnia 2018 r. Fundacja Rozwoju Demokracji Lokalnej zorganizowała i przeprowadziła certyfikowane szkolenie dla Pracowników Urzędu Gminy Gródek pt. *„Zadania użytkowników, inspektora ODO i Administratora Danych w świetle zmian RODO 2018"*. (lista obecności w teczce sprawy ABI. 142.1.2018)

W dniu 20 grudnia 2019 r. IOD przeprowadził szkolenie dla pracowników Urzędu składające się z dwóch części tj. Najczęściej popełniane błędy z zakresu ochrony danych osobowych, omówienie Regulaminu realizacji osób których dane dotyczą. (lista obecności w teczce sprawy IOD. 142.3.2019).

W dniu 20 listopada 2020 r. IOD przeprowadził szkolenie dla pracowników Urzędu za pomocą środków porozumiewania się na odległość, z uwagi na wdrożony system pracy zdalnej. (IOD.142.3.2020).

Ponadto, raz w roku IOD, opracowuje harmonogram spotkań z pracownikami Urzędu oraz na bieżąco szkoli z zakresu ochrony danych osobowych.

g) rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

Rejestr czynność przetwarzania danych jest prowadzony w oparciu o Politykę Ochrony Danych Osobowych Przetwarzanych w Urzędzie zarówno w wersji elektronicznej jak i papierowej. Aktualizowany jest raz w miesiącu, natomiast raz na kwartał jest drukowany i wpinany do teczki sprawy.

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

Rejestr kategorii czynność przetwarzania danych jest prowadzony w oparciu o Politykę Ochrony Danych Osobowych Przetwarzanych w Urzędzie zarówno w wersji elektronicznej jak i papierowej. Aktualizowany jest na bieżąco, drukowany i wpinany do teczki sprawy.

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

Analiza ryzyka obecnie jest wykonywana w oparciu o wprowadzone procedury szacowania ryzyka operacji przetwarzania danych osobowych w Urzędzie. Ostatnia została sporządzona wg stanu na dzień 30 września 2020 r. Dokumentacja w teczce sprawy.

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

Opis procedury w zakresie realizowania obowiązku informacyjnego obowiązujący w Urzędzie zawiera Regulamin realizacji praw osób których dane dotyczą, link do dokumentu poniżej:

http://bip.ug.grodek.wrotapodlasia.pl/urzad-gminy/klauzula_informacyjna_/regulamin-realizacji-praw-osob-ktorych-dane-dotycza-w-urzedzie-gminy-grodek.html

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

Opis procedury w zakresie realizowania obowiązku informacyjnego obowiązujący w Urzędzie zawiera Regulamin realizacji praw osób których dane dotyczą, link do dokumentu poniżej:

http://bip.ug.grodek.wrotapodlasia.pl/urzad-gminy/klauzula_informacyjna_/regulamin-realizacji-praw-osob-ktorych-dane-dotycza-w-urzedzie-gminy-grodek.html

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

Tak, są wykonywane co najmniej raz w roku.

14. Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

NIE.

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

TAK, poprzez odpowiednie zapisy w Specyfikacji Istotnych Warunkach Zamówienia, w zapytaniach ofertowych oraz w umowach.

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

Zgodnie z poniższym Regulaminem:

http://bip.ug.grodek.wrotapodlasia.pl/urzadgminy/klauzula_informacyjna_/regulamin-realizacji-praw-osob-ktorych-dane-dotycza-w-urzedzie-gminy-grodek.html

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

TAK. Zarządzenie Nr 24/19 Wójta Gminy Gródek z dnia 11 lutego 2019 r. w sprawie Regulaminu Organizacyjnego Urzędu Gminy Gródek.

Z poważaniem,

WÓJT

Wiesław Kulesza

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (4.5.2016 L 119/38 Dziennik Urzędowy Unii Europejskiej PL) (RODO) Wójt Gminy Gródek informuje, że:

1. Administratorem Pani/Pana danych osobowych przetwarzanych w Urzędzie Gminy Gródek jest: Wójt Gminy Gródek, mający siedzibę w Urzędzie Gminy Gródek, ul. A. i G. Chodkiewiczów 2, 16-040 Gródek.
2. W razie pytań dotyczących sposobu i zakresu przetwarzania Pani/Pana danych osobowych w zakresie działania Urzędu Gminy Gródek, a także przysługujących uprawnień, może się Pani/Pan skontaktować z Inspektorem Ochrony Danych w Urzędzie Gminy Gródek za pomocą adresu: iodo@grodek.pl, telefonicznie (857180664) lub listownie na adres siedziby Urzędu.
3. Pani/Pana dane przetwarzane są w związku ze złożonym wnioskiem o udostępnienie informacji publicznej w celu jego rozpatrzenia zgodnie z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176), zwanej dalej ustawą oraz ustawą z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2020 r. poz. 256 z późn. zm.). Pani/Pana dane są przetwarzane na podstawie w/w przepisów prawa.
4. Odbiorcami Pana/Pani danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa oraz mogą być podmioty, które będą przetwarzały Pana/Pani dane osobowe w imieniu Administratora na postawie zawartej z Administratorem umowy powierzenia przetwarzania danych osobowych (tj. podmioty przetwarzające).
5. Pana/Pani dane osobowe będą przechowywane przez okres niezbędny do realizacji celu określonego w pkt 3, a po tym czasie przez okres oraz w zakresie zgodnym z rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67).
6. Posiada Pan/Pani prawo do:
   — żądania od Administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych.
7. W przypadku uznania, iż przetwarzanie przez Administratora Pani/Pana danych osobowych narusza przepisy o ochronie danych przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego którym jest Prezes Urzędu Ochrony Danych Osobowych z siedzibą przy ul. Stawki 2, 00-193 Warszawa.
8. Dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.
9. Pani/Pana dane nie podlegają zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.