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,
– Nie

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.
-Tak Urząd opracował, ustanowił, eksploatuje, monitoruje i doskonali System Zarządzania Bezpieczeństwem Informacji. SZBI zawiera wymogi prawne w zakresie ochrony danych osobowych i bezpieczeństwa informacji oraz uwzględnia dobre praktyki wynikające z norm ISO serii 27000.

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 w zakresie bezpieczeństwa informacji został wykonany grudzień 2019 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

Andrzej Szuberski a.szuberski@gmwm.pl , 86 275 26 27

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

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.

8)
Podanie liczby żądań określonych w art. 15 – 21 RODO jakie wpłynęły do adresata niniejszego wniosku w roku 2020.
-W roku 2020 do Urzędu nie wpłynęły żądania umocowane w 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?
-Nie

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)Proszę o udzielenie odpowiedzi zgodnie ze stanem faktycznym.
- szkolenie w zakresie dostępu do informacji publicznej w 2018, wzięła udział 1 osoba, Szkolenie było bezpłatne otwarte-wyjazdowe prowadzone przez Narodowy Instytut Samorządu Terytorialnego.

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?

Tak, zostały opracowane procedury – ujęte w ramach obowiązującego w Urzędzie Systemu Zarządzania Bezpieczeństwem Informacji. Niezależnie IOD przeprowadza okresowe szkolenia i sprawdzenia w zakresie stosowania zasad bezpieczeństwa informacji.

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?

Obsługa finansowa szkoły jest realizowana przez organ prowadzący, nie zaś celową jednostkę organizacyjną gminy.
Nie dotyczy.

13)
Wnosimy o informację w zakresie:
•
danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD
Agata Wyszomirska iodugwm@gminawysokiemazowieckie.pl

•
zakresu czynności, wyznaczenie, zawiadomienie o wyznaczeniu IOD do PUODO;
Zakres czynności zgodny z art. 39 RODO
Kopia zawiadomienia PUODO w załączniku.

•
czy IOD wykonuje jeszcze jakieś inne dodatkowe czynności/ jeśli tak wskazać jakie;
- prowadzenie spraw z zakresu ochrony przeciwpożarowej (OSP),
- prowadzenie spraw w zakresie obronności państwa,
- prowadzenie spraw w zakresie obrony cywilnej,
- prowadzenie spraw w zakresie zarządzania kryzysowego:

•
informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

IOD w 2020 uczestniczył w szkoleniach realizowanych przez firmę konsultingową
•
dokumentacja potwierdzająca realizację zadań przez IOD od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO).
Zadania realizowane w zakresie obowiązków RODO są dokumentowane w formie załączników do Systemu Zarządzania Bezpieczeństwem Informacji. Dokumentacja SZBI nie podlega dostępowi w trybie dostępu do informacji publicznej.

- 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)

-Szkolenia w przedmiotowym zakresie są realizowane przez IOD w formie szkoleń stacjonarnych. Plan budowania świadomości w zakresie ODO i BI stanowi element SZBI. Dokumentacja SZBI nie podlega dostępowi w trybie dostępu do informacji publicznej.
Szkolenia są dokumentowane poprzez imienne zaświadczenia stanowiące element dokumentacji kadrowej.

- rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

Rejestr czynności przetwarzania jest prowadzony i aktualizowany.

- rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

Rejestr kategorii czynności przetwarzania jest prowadzony i aktualizowany.

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

Jest prowadzona.

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

Klauzule obowiązku informacyjnego są dostępne na stronie Biuletynu Informacji Publicznej pod adresem: http://www.ugwm.biuletyn.net/?bip=2&cid=28&id=18

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

-Jak powyżej.

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

-IOD dokonuje okresowe sprawdzenia/przeglądy obowiązującego Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z przyjętym zakresem i harmonogramem.

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

Nie.

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

- Zgodnie z przepisami.

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

Tak

WÓJT
mgr inż. Krzysztof Krajewski