

S.1431.80.2020

W odpowiedzi na wniosek o udostępnienie informacji publicznej przesyłam odpowiedzi na postawione 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 udzielenie informacji publicznej w przedmiocie - szacunkowej ilości oprogramowania - użytkowanego w Urzędzie i nieposiadającego obecnie wsparcia producenta - inter alia: Windows XP, Windows Vista, etc,

Odpowiedź

Urząd Gminy wykorzystuje wyłącznie oprogramowanie posiadające wsparcie producenta.

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.

Odpowiedź

Urząd Gminy posiada politykę bezpieczeństwa przetwarzania danych osobowych która zawiera m. in.:

- opis procedur obowiązujących dla ochrony danych osobowych
- opis środków organizacyjnych i technicznych stosowanych przy przetwarzaniu danych osobowych
- sposób prowadzenie rejestrów czynności i kategorii przetwarzania danych osobowych
- opis procedury realizacji obowiązku informacyjnego
- instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych
- zasady udostępniania danych osobowych
- zasady bezpiecznej pracy w systemach IT dla użytkowników oraz zasady zarządzania bezpieczeństwem zasobów informatycznych
- zasady ochrony systemu przed wirusami oraz zasady korzystania z nośników informacji i oprogramowania
- przechowywanie i likwidacja sprzętu, nośników informacji i wydruków
- regulacje dotyczące oceny skutków dla ochrony danych,
- procedury wykonywania kopii zapasowych
- procedury zachowania ciągłości działania,

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 publicznej 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.

Odpowiedź

W styczniu oraz we wrześniu 2020 r. zostały przeprowadzone audyt systemów IT, wyniki audytów zostały wykorzystane do analizy ryzyka przetwarzania danych osobowych.

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 (...)

Odpowiedź

Urząd Gminy posiada umowę.

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

Odpowiedź

Ireneusz Baka, email: i.baka@gminasiedlce.pl

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

Odpowiedź

Zgodnie z przyjętą w raporcie definicją Administratora (RODO) - Administrator realizuje na bieżąco wszystkie swoje zadania

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>

Odpowiedź

IOD informował o konieczności przygotowania umowy ale sam jej nie przygotowywał, umowa została zawarta w oparciu o wzór firmy realizującej hosting strony BIP.

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

Odpowiedź

Na skrzynkę IOD nie wpłynęły żadne żądania

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?

Odpowiedź

Konsultacje nie były prowadzone.

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.institutOS.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)

Odpowiedź

Pracownicy przechodzili szkolenia realizowane przez IOD oraz firmę świadczącą usługi IOD w zakresie ochrony danych osobowych publikowanych na BIP – np. okresu publikacji oświadczeń majątkowych

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?

Odpowiedź

Zadaniem IOD jest nadzorowanie zgodności przetwarzania danych zgodnie z regulacjami określonymi przez Administratora. Administrator posiada w Polityce bezpieczeństwa procedury w zakresie regulacji dostępu do systemów, wykorzystania zasobów oraz zabezpieczenia przed utratą danych a IOD sprawdza ich przestrzeganie.

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?

Odpowiedź

W Urzędzie Gminy nie funkcjonuje CUW.

13) Wnosimy o informację w zakresie:

· danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD

Odpowiedź

Stefan Książek, iod-sk@tbdsiedlce.pl

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

Odpowiedź

Firma zewnętrzna, zakres czynności zgodnie z art. 38 i 39 właściwych dla IOD,

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

Odpowiedź

IOD nie wykonuje innych czynności, natomiast firma (zespół IOD) w ramach umowy uczestniczyła w szacowaniu ryzyka, opracowaniu dokumentacji bezpieczeństwa, prowadzenia rejestrów czynności i kategorii, opracowaniu klauzul informacyjnych i umów powierzenia.

- informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

Odpowiedź

firma realizująca zadania IOD zapewnia posiadanie przez osoby pełniące funkcje IOD stosownych kwalifikacji (np. uczestniczenie w szkoleniach w ramach forum IOD FRDL), ponadto posiada wdrożony certyfikowany system zarządzania bezpieczeństwem informacji zgodny z normą ISO 27001 - wsparcie administracji samorządowej w zakresie świadczenia usług informatycznych i usługi w obszarze ochrony danych osobowych.

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

Odpowiedź

Informacje te za wyjątkiem informacji o szkoleniach pracowników nie stanowią informacji publicznej i są związane z relacją Administrator - IOD- UODO. Ujawnienie informacji w tym związanych z udzielonymi konsultacjami może spowodować naruszenie ochrony bezpieczeństwa lub praw i wolności osób których konsultacje dotyczyły.

- 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)

Odpowiedź

- rejestr czynności przetwarzania danych osobowych oraz jego zmiany. Prowadzący: Stefan Książek.
- rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany. Prowadzący: Stefan Książek.

Odpowiedź

Rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych nie podlegają udostępnieniu, poniżej link do wyroku sądu w tym zakresie

<https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-sab-ld-181-18-rejestry-czynnosci-przetwarzania-oraz-522720873>

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

Odpowiedź

Nie podlega udostępnieniu z uwagi na obowiązek zapewnienia poufności dla mechanizmów ochrony danych, w tym występujących realnych ryzyk i podatności systemów.

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

Odpowiedź

Zgodnie z art. 65 par 5 kpa osoby których dane dotyczą są informowane przy pierwszym kontakcie poprzez udostępnienie klauzul informacyjnych wyłożonych przy stanowiskach pracy bądź zintegrowanych z wnioskiem lub formularzem lub dołączonych do nich (zależnie od wymagań w przepisach szczegółowych). Klauzule są też wywieszone na stronach www i BIP oraz na tablicach informacyjnych. W przypadku w którym z jakiś powodów informacja o przetwarzaniu danych nie została podana przy pierwszym kontakcie, zamieszcza się ją w powiadomieniach i zawiadomieniach oraz wezwaniach kierowanych do osoby której dane dotyczą. Klauzule informacyjne zostały utworzone dla wszystkich czynności przetwarzania w których dane są pozyskiwane bezpośrednio od osób.

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

Odpowiedź

Klauzule są wywieszone na stronach www i BIP oraz na tablicach informacyjnych

Obowiązek informacyjny zrealizowano poprzez przygotowanie szczegółowych klauzul informacyjnych dla wszystkich czynności przetwarzania danych osobowych pozyskiwanych z innych źródeł niż osoba której dane dotyczą.

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

Odpowiedź

IOD oraz osoby z zespołu IOD wykonują audyty systemów IT pod kątem podatności które mogą być wykorzystane przez określone zagrożenia (skan sieci i urządzeń sieciowych, sprawdzenie poprawności konfiguracji kluczowych urządzeń – np. UTM, sprawdzenie wykonywania kopii zapasowych itp.). Sprawdzana też była kompletność i prawidłowość umów powierzenia oraz sposób realizacji obowiązku informacyjnego.

Klauzule na podst. Art.13 RODO

Klauzula informacyjna szczegółowa- GKRPA.docx

Klauzula informacyjna szczegółowa- OSP.docx

Klauzula informacyjna szczegółowa- GZZK.docx

Klauzula informacyjna szczegółowa- OC.docx

Klauzula informacyjna szczegółowa- awans nauczycieli.docx

Klauzula informacyjna szczegółowa- konkurs na dyrektora.docx

Klauzula informacyjna szczegółowa- baza azbestowa.docx

Klauzula informacyjna szczegółowa- decyzja o lokalizacji zjazdu.docx

Klauzula informacyjna szczegółowa- dofinansowanie kształcenia młodocianych pracowników.docx

Klauzula informacyjna szczegółowa- dowóz dzieci.docx

Klauzula informacyjna szczegółowa- finanse.docx

Klauzula informacyjna szczegółowa- gospodarka nieruchomościami.docx

Klauzula informacyjna szczegółowa- klęski żywiołowe.docx

Klauzula informacyjna szczegółowa- koncesje na alkohol.docx

Klauzula informacyjna szczegółowa- książka wejść i wyjść.docx

Klauzula informacyjna szczegółowa- mieszkania komunalne.docx

Klauzula informacyjna szczegółowa- numeracja.docx

Klauzula informacyjna szczegółowa- oczyszczalnie.docx

Klauzula informacyjna szczegółowa- podatki.docx

Klauzula informacyjna szczegółowa- podziały nieruchomości.docx

Klauzula informacyjna szczegółowa- podłączenie do kanalizacji.docx

Klauzula informacyjna szczegółowa- pomoc nauczycielom.docx

Klauzula informacyjna szczegółowa- pomoc uczniom.docx

Klauzula informacyjna szczegółowa- promocja.docx

Klauzula informacyjna szczegółowa- przedsiębiorcy.docx

Klauzula informacyjna szczegółowa- przekazanie zgodnie z właściwością.docx

Klauzula informacyjna szczegółowa- przewoźnicy.docx

Klauzula informacyjna szczegółowa- psy.docx

Klauzula informacyjna szczegółowa- radni.docx

Klauzula informacyjna szczegółowa- rozgraniczenia.docx

Klauzula informacyjna szczegółowa- sołtysi.docx

Klauzula informacyjna szczegółowa- sprzedaż nieruchomości.docx

Klauzula informacyjna szczegółowa- stosunki wodne.docx

Klauzula informacyjna szczegółowa- usługi hotelarskie.docx

Klauzula informacyjna szczegółowa- wycinka.docx

Klauzula informacyjna szczegółowa- zajęcie pasa drogowego.docx

Klauzula informacyjna szczegółowa- zaświadczenia rolnik.docx

Klauzula informacyjna szczegółowa- zaświadczenia.docx

Klauzula informacyjna szczegółowa- ławnicy.docx

Klauzula informacyjna szczegółowa- świadczenia na rzecz obrony.docx

Klauzula informacyjna szczegółowa- informacja publiczna.docx

Klauzula informacyjna szczegółowa- opłaty za odpady.docx

Klauzula informacyjna szczegółowa- prace społeczne.docx

Klauzula informacyjna szczegółowa- roboty publiczne.docx

Klauzula informacyjna szczegółowa- zamówienia publiczne.docx

Klauzula informacyjna szczegółowa- PPK.docx

Klauzule na podst. Art.14 RODO

Klauzula informacyjna szczegółowa- stypendia sportowe.docx

Klauzule na podst. Art.13 i 14 RODO

Klauzula informacyjna ogólna gmina.docx

Klauzula informacyjna szczegółowa- ZFŚS.docx

Klauzula informacyjna szczegółowa- archiwum.docx

Klauzula informacyjna szczegółowa- decyzje środowiskowe.docx

Klauzula informacyjna szczegółowa- kwalifikacja wojskowa.docx

Klauzula informacyjna szczegółowa- medale.docx

Klauzula informacyjna szczegółowa- warunki zabudowy.docx

Klauzula informacyjna szczegółowa- zagospodarowanie przestrzenne.docx

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 jakiegokolwiek 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.

Odpowiedź

Nie występuje konflikt interesów, IOD z zewnętrznej firmy jest podległy bezpośrednio najwyższemu kierownictwu.

15. Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

Odpowiedź

Nie każda czynność sprawdzająca jest dokumentowana notatką IOD, są raporty z audytów bezpieczeństwa.

16. Czy jednostka realizuje obowiązek wskazany w najnowszym stanowisku UODO? Jeśli proszę wskazać w jaki sposób.

<https://uodo.gov.pl/pl/225/1577>

Odpowiedź

Zostały stworzone klauzule informacyjne dla członków zarządu reprezentujących osobę prawną, pełnomocników osób prawnych oraz dla pracowników, którzy są osobami kontaktowymi osoby prawnej. Klauzule są dołączane do umów z osobami prawnymi

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

Odpowiedź

Zgodnie z art. 65 par 5 kpa osoby których dane dotyczą są informowane przy pierwszym kontakcie poprzez udostępnienie klauzul informacyjnych wyłożonych przy stanowiskach pracy bądź zintegrowanych z wnioskiem lub formularzem (zależnie od wymagań w przepisach szczegółowych). Klauzule są też wywieszone na stronach www i BIP oraz na tablicach informacyjnych. W przypadku w którym z jakiś powodów informacja o przetwarzaniu danych nie została podana przy pierwszym kontakcie, zamieszcza się ją w powiadomieniach i zawiadomieniach oraz wezwaniach kierowanych do osoby której dane dotyczą.

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

Odpowiedź

W Polityce bezpieczeństwa przetwarzania danych osobowych jest opisana rola IOD oraz jego kompetencje i zakres działania

#####

Z poważaniem,

Ireneusz Baka

_____ ESET Endpoint Antivirus _____

Ta wiadomość e-mail została przeskanowana. Nie znaleziono zagrożen.

wiadomość e-mail do: tomaszpiotrowiczinformacjapub@gmail.com z tematem odpowiedź na wniosek o udostępnienie informacji publicznej - bez zagrożen

Wersja silnika detekcji: 22564 (20201230)

<https://www.eset.pl> lub <https://www.eset.com>

_____ ESET Endpoint Antivirus _____

Ta wiadomość e-mail została przeskanowana. Nie znaleziono zagrożen.

wiadomość e-mail od: Ireneusz Baka do: 'tomaszpiotrowiczinformacjapub@gmail.com' z tematem odpowiedź na wniosek o udostępnienie informacji publicznej - bez zagrożen

Wersja silnika detekcji: 22564 (20201230)

<https://www.eset.pl> lub <https://www.eset.com>