Odpowiedź na wniosek o udzielenie informacji publicznej

1) **Jaką szacunkowo ilością oprogramowania - użytkowanego w Urzędzie i nieposiadającego obecnie wsparcia producenta - inter alia: Windows XP, Windows Vista, etc posługuje się podmiot?**

Jednostka użytkuje komputery z oprogramowaniem Windows 10. Nie pracuje na starszych systemach, które nie posiadają wsparcia producenta.

2) **Czy podmiot dysponuje całościową Polityką Bezpieczeństwa Informacji, wymaganą w §20 ust. 1 i 3 ww. Rozporządzenia?**

Tak

Jeśli odpowiedź jest twierdząca - wnosimy o krótkie - w kilku ogólnych zdaniach - opisanie przedmiotowej dokumentacji RODO.

Dokumentacja RODO określa mapę zasad i obowiązków wynikających z przepisów o ochronie danych osobowych w oparciu o analizę ryzyka oraz wymagań określonych w rozporządzeniu KRI:

1) dla spełnienia wymagań określonych w RODO i UODO, w tym określenie:
   - podstaw przetwarzania danych osobowych;
   - środków (zabezpieczeń) przetwarzania danych osobowych;
   - zasobów danych i informacji;
   - urządzeń i oprogramowania wykorzystywanego do przetwarzania danych osobowych;
   - metody szacowania ryzyka;
   - obowiązku informacyjnego;
   - realizacji uprawnień osób, których dane dotyczą;
   - sposobów powierzenia przetwarzania danych osobowych;
   - postępowania w przypadku wystąpienia incydentów i naruszeń ochrony danych osobowych;
   - monitorowania ochrony danych osobowych;
   - zarządzenia dostępem do obszarów przetwarzania.

2) dla spełnienia wymagań rozporządzenia KRI - procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji, w tym:
   - procedury dotyczące uprawnień do systemów przetwarzających dane osobowe;
   - zasady postępowania z hasłami
   - metody oraz środki uwierzytelniania;
   - zasady tworzenia i używania haseł;
   - procedury rozpoczęcia, zawieszenia i zakończenia pracy;
   - zasady korzystania z służbowej poczty elektronicznej;
   - korzystanie z sieci Internet;
   - zasady postępowania z nośnikami elektronicznymi i sprzętem komputerowym podczas pracy poza obszarem przetwarzania danych;
   - procedury tworzenia kopii zapasowych;
   - użytkowanie sprzętu komputerowego, oprogramowania i nośników danych;

- procedury zdalnego dostępu do systemów informatycznych;
- zabezpieczenie systemu informatycznego przed utratą danych spowodowaną awarią zasilania lub zakłóceniami sieci zasilającej;
- sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

3) **Kiedy Urząd ostatni raz przeprowadzał wewnętrzny audyt z zakresu bezpieczeństwa informacji - stosownie do wymogów §20 ust. 2 pkt. 14 ww. Rozporządzenia.**

Audyt wewnętrzny z zakresu bezpieczeństwa informacji nie został zrealizowany.

4) **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**

AGA elektronics Sp. J. Z. Korzeniecki, P. Kowalczyk
16- 300 Augustów, ul. Ks. Skorupki 3, tel. 87 643 24 30
(zgodnie z umową nr SP2/2019 ,,wykonawca'' w art. 1 pkt. 9 prowadzi dokumentację zgonie z polityką bezpieczeństwa przygotowaną przez Administratora Danych Osobowych.
Wykonawca przyjmuje funkcję administrator systemów informatycznych.)

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

Rzeczowy raport NIK został przeanalizowany przez kierownictwo podmiotu i podjęto niezbędne działania dla spełnienia wymogów określonych w rozporządzeniu KRI.

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**

Umowa powierzenia z dostawcą BIP została zawarta.

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

Do jednostki nie wpłynęły żądania określone 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?**

Tak

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?**

Nie

Jeśli tak to kto był dostawcą szkoleń (www.instytutOS.pl, www.nbip.pl czy inny (jaki?))

Nie dotyczy

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)

Nie dotyczy

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?

IOD w ramach wykonywania zadań określonych w art. 39 RODO monitoruje i doradza w zakresie stosowanych środków bezpieczeństwa mających na celu ochronę przed nieautoryzowanym dostępem do systemu inf. wykorzystywanego do przetwarzania danych osobowych.

Czy zostały opracowane odpowiednie procedury?

Tak

Jeśli tak to jakie?

Instrukcja Zarządzania Systemem Informatycznym

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**

Czy takie umowy między jednostkami zostały zawarte?

Nie dotyczy

13) **Wnosimy o informację w zakresie:**

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

Robert Stańczyk kontakt.itrs@gmail.com

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

Zakres czynności określa art. 39 RODO – Zadania inspektora ochrony danych

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

Nie

- informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

Usługi IOD realizowane są przez podmiot zewnętrzny – jednostka nie posiada informacji, o które pyta wnioskodawca.

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

Realizacja zadań IOD określonych w art. 39 rozporządzenia RODO realizowana jest w postaci kontaktów telefonicznych, e-maili oraz indywidualnych spotkań. Dotyczą najczęściej doradzania w zakresie wdrożenia dokumentacji ochrony danych, pomocy w tworzeniu obowiązków informacyjnych, omawianiu działań, przygotowywania umów. W jednostce nie prowadzi się dokumentacji potwierdzającej w/w czynności.

- 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)

Szkolenie pracowników w zakresie ochrony danych osobowych zostało przeprowadzone przez IOD. Potwierdzeniem udziału w szkoleniu jest lista obecności znajdująca się w zakładzie pracy, data szkolenie 02.10.2018 r.

- rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

Rejestr czynności przetwarzania stanowi element dokumentacji ochrony danych wprowadzonej do stosowania w ramach środków organizacyjnych dla spełnienia wymogu określonego w art. 30 RODO i jest prowadzony i aktualizowany przez IOD.

- rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

Rejestr kategorii czynności przetwarzania stanowi element dokumentacji ochrony danych wprowadzonej do stosowania w ramach środków organizacyjnych dla spełnienia wymogu określonego w art. 30 RODO i jest prowadzony i aktualizowany przez IOD.

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

Analiza ryzyka stanowi element dokumentacji ochrony danych wprowadzonej do stosowania w ramach środków organizacyjnych dla spełnienia wymogu określonego w art. 30 RODO i realizowana jest przez IOD.

- w jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać.

Obowiązki informacyjne udostępniane są osobom, których dane dotyczą poprzez umieszczenie m.in.:

- na wniosku (jeśli sprawa, z którą przychodzi osoba rozpatrywana jest w trybie wnioskowym) lub innej formie dokumentu, który wypełnia osoba, której dane dotyczą,
- w ogólnie dostępnym miejscu (tablica ogłoszeń, sekretariat) w tym na ścianie,
- na stronie internetowej jednostki,
- aplikacjach webowych (udostępnienie klauzuli w regulaminach, zakładkach, przy tworzeniu loginu itd.),
- mailowo i pocztowo (przy pierwszym kontakcie/w piśmie które kierowane jest do osoby, której dane dotyczą),

Przedstawić obowiązujące klauzule informacyjne.

Podmiot nie ma stałych obowiązujących klauzul. Obowiązki informacyjne weryfikowane są przez IOD i aktualizowane w ramach konkretnych celów przetwarzania oraz dostępnej wiedzy i wytycznych Urzędu Ochrony Danych Osobowych. Przykładowy obowiązek informacyjny dostępny jest tu: http://sp2aug.pl/Dokumenty/KLAUZULA%20ogolna%20BIP.pdf

Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?

Jednostka nie posiada informacji, o które pyta wnioskodawca.

- w jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać.

Jednostka co do zasady nie realizuje obowiązków informacyjnych określonych w art. 14 RODO (pozyskiwanie danych osobowych niebezpośrednio od osób, których dane dotyczą). Jeśli zostanie zidentyfikowany taki przypadek to poza informacjami, o których mowa w art. 13 RODO udostępnia się kategorie danych oraz źródło pozyskania danych.

Przedstawić obowiązujące klauzule informacyjne.

Podmiot nie ma stałych obowiązujących klauzul. Obowiązki informacyjne weryfikowane są przez IOD i aktualizowane w ramach konkretnych celów przetwarzania oraz dostępnej wiedzy i wytycznych Urzędu Ochrony Danych Osobowych.

Dla jakich czynności przetwarzania zrealizowano obowiązek informacyjny?

Jednostka nie posiada informacji, o które pyta wnioskodawca.

- czy są wykonywane audyty z zakresu RODO?

Nie

Przedstawić realizacji w/w obowiązku.

Nie dotyczy

14. Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

Nie

15. Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

Nie. Zgodnie z przepisami, nie ma obowiązku prowadzenia dokumentacji z zakresu realizacji zadań IOD.

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

Obowiązki informacyjne realizowane są w umowach zawieranych z podmiotami (osobami prawnymi).

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

Obowiązki informacyjne udostępniane są osobom, których dane dotyczą poprzez umieszczenie m.in.:

- na wniosku (jeśli sprawa, z którą przychodzi osoba rozpatrywana jest w trybie wnioskowym) lub innej formie dokumentu, który wypełnia osoba, której dane dotyczą,
- w ogólnie dostępnym miejscu (tablica ogłoszeń, sekretariat) w tym na ścianie, tablicy,
- na stronie internetowej jednostki
- aplikacjach webowych (udostępnienie klauzuli w regulaminach, zakładkach, przy tworzeniu loginu itd.),
- mailowo i pocztowo (przy pierwszym kontakcie/w piśmie które kierowane jest 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.

Tak.