Odpowiedź na zapytanie w trybie informacji publicznej

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 Szkole i nieposiadającego obecnie wsparcia producenta - interwali: Windows XP, Windows Vista, etc,

W chwili obecnej w naszej szkole nie są użytkowane komputery z oprogramowaniem nieposiadającym wsparcia producenta. Oprogramowanie używane to Windows 10 oraz Windows 11

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.

Szkoła dysponuje całościową polityką bezpieczeństwa informacji. Zawiera ona między innymi wykaz pomieszczeń lub ich części, budynków, w których dane osobowe są przetwarzane, sposób, w jaki przepływają dane między systemami, wykaz programów, które używane są do przetwarzania danych oraz zestawienie zbiorów danych, określenie środków organizacyjnych, jak i technicznych, które niezbędne są do zapewnienia integralności, rozliczalności i poufności danych, które są przetwarzane.

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

Audyt bezpieczeństwa informacji został przeprowadzony w listopadzie 2021 r.

4) Na mocy wyżej wzmiankowanych przepisów wnosimy o udzielenie informacji publicznej w przedmiocie, czy Szkoła 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 posiadamy stosowną umowę. Jej pełna treść w załączniku stanowi jednocześnie odpowiedź na pytanie 19 niniejszego zapytania.

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..

W szkole brak jest pracownika spełniającego powyższe zadania.

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

Zadania administratora wskazane w raporcie NIK są realizowane na bieżąco.

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 posiadamy stosowną umowę powierzenia danych osobowych Podmiotowi przetwarzającemu dane osobowe do przetwarzania, w trybie art. 28 ogólnego rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz.UE.L Nr 119, str. 1) (zwanego w dalszej części Umowy „Rozporządzeniem”), na zasadach, w zakresie i w celu określonym w niniejszej Umowie.

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

Nie wpłynęło żadne żądanie.

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. Jako dyrektor szkoły konsultowałem z organem prowadzącym zasadność wprowadzenia monitoringu wizyjnego. Gmina ubiegała się również o dofinansowanie monitoringu w szkole w ramach programu rządowego.

10) *C*zy 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)

nie prowadzono szkoleń ze względu na niewielką aktywność w przedmiotowych obszarach.

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".

Czy w związku z powyższym czy IOD podjął działania realne w tym zakresie? Czy zostały opracowane odpowiednie procedury? Jeśli tak to jakie?

Użytkownicy systemu /nauczyciele/ zostali przeszkoleni w zakresie bezpieczeństwa, uwierzytelniania i kontroli dostępu w obsługiwanym systemie . W przedmiotowych sprawach są wdrożone odpowiednie procedury. Regulamin korzystania z dziennika elektronicznego jest elementem prawa wewnątrzszkolnego. Przedstawiono w nim zasady bezpiecznego korzystania. Jego przestrzeganie zapewnia ochronę przed nieuprawnionym dostępem – do tej pory nie stwierdzono takiego przypadku.

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?

Tak mamy stosowną umowę powierzenia danych osobowych z organem prowadzącym a konkretnie z ZEAS-em, który obsługuje nas w zakresie m.in. księgowym

13) Wnosimy o informację w zakresie:

danych Inspektora Ochrony Danych (IOD)/ewentualnie zastępcy IOD

Grzegorz Bojanek, iodo@pilica.pl

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

1. identyfikacja i aktualizacji zbiorów danych osobowych;
2. przeprowadzenie oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych oraz monitorowanie jej wykonania;

3. weryfikacja klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązków informacyjnych, a w razie potrzeby przygotowanie niezbędnych zmian lub opracowanie właściwych dokumentów i klauzul;
4. analiza stosowanych przez Zleceniodawcę techniczno-organizacyjnych środków ochrony, bezpieczeństwa fizycznego oraz informatycznego związanych z przetwarzaniem danych osobowych;
5. prowadzenie rejestru czynności przetwarzania danych osobowych;
6. zarządzanie upoważnieniami do przetwarzania danych osobowych;
7. zarządzanie ewidencją osób upoważnionych do przetwarzania danych osobowych;
8. prowadzenie korespondencji z organem nadzorczym;
9. opiniowanie wzorów dokumentów dotyczących ochrony danych osobowych, klauzul zgód na przetwarzanie danych osobowych oraz klauzul obowiązków informacyjnych;
10. prowadzenie szkoleń dla pracowników z zakresu ochrony danych osobowych;
11. wspieranie pracy audytorów zewnętrznych w zakresie ochrony danych osobowych;
12. udział w kontrolach organu nadzorczego oraz współpraca z organem nadzorczym;
13. udział w kontrolach prowadzonych u Zleceniodawcy przez innych administratorów danych;
14. prowadzenie audytów podmiotów, którym Zleceniodawca powierzył przetwarzanie danych osobowych;
15. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Wyznaczenie i zawiadomienie odbyło się zgodnie z obowiązującym prawem. Wyznaczenie w drodze zarządzenia oraz podpisania stosowanej umowy – załącznik – powołanie IODO zawiadomienie PUODO z wykorzystaniem komunikacji elektronicznej.

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

Nie

· informacje dotyczące szkoleń, podnoszenia kwalifikacji przez IOD.

Osoba pełniąca funkcję IODO nie jest zobowiązana do składania takich informacji ADO ze względu na formę zatrudnienia.

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

· 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)

Inspektor ochrony danych Grzegorz Bojanek na bieżąco szkoli pracowników szkoły. Ostatnie szkolenie w zakresie ochrony danych osobowych odbyło się w styczniu 2022 r. W załączeniu Upoważnienie wraz z potwierdzeniem odbycia ostatniego szkolenia.

· rejestr czynności przetwarzania danych osobowych oraz jego zmiany. –

w załączeniu

· rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

brak

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

W załączeniu

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

Posiadamy klauzule informacyjne dla rodziców dzieci ubiegających się o przyjęcie do szkoły i odrębne klauzule dla doraźnych projektów**.** W załączeniu klauzula przyjęcia do szkoły, klauzula uczestnictwa w konkursie szkolnym, oraz ogólna klauzula informacyjna.

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

Do dnia dzisiejszego nie wystąpiła konieczność informowania osób o pozyskaniu danych osobowych w trybie art. 14 RODO

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

Z przepisów RODO nie wynika wprost obowiązek przeprowadzania audytu. To ADO decyduje w jaki sposób będzie realizował te obowiązki i zapewni zgodność z RODO. Może być to zatem stała, wyrywkowa kontrola, lub cykliczna całościowa, jak audyt. Dlatego na żądanie administratora inspektor ochrony danych osobowych prowadzi kontrolę RODO

14. Czy istnieje konflikt interesów przy pełnieniu funkcji IOD?

Brak konfliktu

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 jakiejkolwiek 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.

15. Czy istnieje dokumentacja z zakresu realizacji zadań IOD?

tak w zakresie prowadzonych kontroli i szkoleń

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

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

Nie dotyczy

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

Nie dotyczy

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

Nie

19. Skan umowy powierzenia na prowadzenie poczty elektronicznej???
Pomimo, że nie wnioskujemy o informację przetworzoną w zakresie wymagającym znacznych nakładów pracy, uzasadniamy nasze pytania stosownie do brzmienia art. 3 ust. 1 pkt. 1 Ustawy o dostępie do informacji publicznej – tym, że przedmiotowa informacja oraz ewentualna późniejsza próba optymalizacji tego obszaru wydaje się

szczególnie istotna z punktu widzenia Interesu Społecznego - o czym świadczy powołany protokół NIK.

Załącznik