Ruszcza, 17.12.2023r.

Zespół Placówek
Oświatowych w Ruszczy
ul. Szkolna 2
28-230 Połaniec

Nie otrzymałam odpowiedzi. Ponawiam wniosek.

Czy w roku 2023 w podmiocie był przeprowadzany Audyt bezpieczeństwa informacji wynikającego z Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j. z dnia 2017.12.05); na zgodność z § 20 ust.2 pkt 14 KRI?

Odp. Audyt został przeprowadzony w dniach: 12-14 grudnia 2023 roku.

Czy został opracowany raport z audytu dt. Zarządzania Bezpieczeństwem Informacji w obszarach zabezpieczeń organizacyjnych, technicznych i fizycznych. Ocena ta powinna opierać się na wymaganiach stawianych jednostkom publicznym, zgodnie z zapisami Rozdziału 5 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, oraz § 20 ust. 1 i 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności.

Odp. Po przeprowadzonym audycie zostanie dostarczony raport.

Taki obowiązek spoczywa na każdym podmiocie publicznym! Odpowiedzialność ponosi Dyrektor.

Czy w roku 2023 Inspektor Ochrony Danych opracował audyty z RODO (art. 39 ust.1 lit b RODO)?

Proszę wskazać kwalifikację i wiedzę prawniczą IOD? Czy IOD jest prawnikiem?

Odp. IOD nie ma wiedzy prawniczej oto kompetencje IOD:
Ukończone studia podyplomowe w zakresie „Ochrona danych osobowych w administracji i biznesie.

Audytor wiodący normy ISO 27001 – zarządzanie systemem bezpieczeństwa informacji.
Audytor wiodący normy ISO 22301 – zarządzanie ciągłością działania.
Skończone liczne kursy związane z ochroną i bezpieczeństwem danych osobowych oraz z cyberbezpieczeństwa.

Pytanie: Czy każda szkoła i przedszkole samorządowe są zobowiązane do przeprowadzenia Jednolitej Analizy Kontrolnej Krajowych Ram Operacyjnych?

Odp. Tak

Odpowiedź: **Tak.** Obowiązkiem podmiotu publicznego jest zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok..

Jak zarządzać bezpieczeństwem informacji

Zgodnie z rozporządzeniem Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych wprowadzone zostały nowe obowiązkowe wymagania dla:

rejestrów publicznych,wymiany informacji w postaci elektronicznej,systemów teleinformatycznych.

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (§ 20 ust. 1 rozporządzenia).

Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

- zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

- utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
- przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
- bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
- zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji;
- zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;
- ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
- ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych;
- bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
- **zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji**

, nie rzadziej niż raz na rok.

Rozwiązanie to dotyczy również jednostek budżetowych realizujących zadania publiczne, w tym również szkół.

Kiedy przeprowadzić audyt

Zarządzanie bezpieczeństwem informacji realizowane jest przez zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, **nie rzadziej niż raz na rok**.

Rozporządzenie nakazuje zatem przeprowadzenie audytu, ale co istotne, **nie musi to być audyt przeprowadzany akurat w maju**, bowiem przywołany przepis wskazuje jedynie, aby zapewnić audyt coroczny.

- Rozporządzenie Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tekst jedn.: Dz.U. z 2017 r., poz. 2247 ze zm.).

https://www.portaloswiatowy.pl/artykuly-i-porady/jednolita-analiza-kontrolna-krajowym-ram-operacyjnych-w-jednostce-oswiaty-18037.html

Mimo wielu problemów z jawnością życia publicznego, jakich doświadczamy w Polsce, sama procedura wnioskowania o jest bardzo prosta: wystarczy wskazać przedmiot żądania (czyli informację, o którą wnioskujemy), formę udostępnienia (np. skan na dany adres e-mail), no i podmiot, od którego domagamy się informacji. Nie trzeba wypełniać żadnych formularzy, przynosić żadnych zaświadczeń ani przedstawiać jakichkolwiek wyjaśnień; nie trzeba nawet podpisu! Wniosek może być jednozdaniowy, anonimowy (organ może wezwać wnioskodawcę do podpisu wniosku tylko wtedy, gdy planuje wydać decyzję administracyjną w sprawie), i wysłany z adresu e-mail o wdzięcznej nazwie „kwiatuszek72" tudzież „koziolek_matolek". Organ musi go rozpatrzyć dokładnie tak samo, jak każdy inny.

Spełnienie powyższych, niewygórowanych wymogów, pozwala na skuteczne korzystanie z prawa do informacji. Wśród nich nie ma podstawy prawnej. Nie musi być przytoczona w ramach wniosku. Jak słusznie wskazał WSA w Rzeszowie w wyroku z 6 października 2021 r. (sygn. akt II SAB/Rz 88/21):

Rzeczą organu, do którego wpływa wniosek o udostępnienie informacji publicznej, jest załatwienie go w przepisany sposób, czyli udostępnienie informacji jeśli ją wytworzył bądź jest w jej posiadaniu, albo odmowa lub umorzenie postępowania z przyczyn uregulowanych u.d.i.p., albo wreszcie poinformowanie, że żądane dane nie stanowią informacji publicznej w rozumieniu tej ustawy.

Zatem nawet ktoś, kto nie wie o istnieniu ustawy o dostępie do informacji publicznej, może złożyć wniosek.

Wszystko to wydawało nam się oczywiste. Okazuje się jednak, że nie jest to oczywiste dla wszystkich: w odpowiedzi na jeden z naszych wniosków, zostaliśmy wezwani do... wskazania trybu, w jakim pismo (przedmiot naszego wniosku) ma być udostępnione. W ramach wniosku odwołaliśmy się co prawda do Konstytucji RP, ale, w ocenie organu „samo odwołanie się do ww. przepisu jest w tym kontekście niewystarczające, albowiem samo unormowanie zawarte w art. 61 Konstytucji RP wyraża jedynie publiczne prawo podmiotowe obywatela dostępu do informacji, którego realizacja następuje na zasadach określonych w ustawach szczególnych".

Autor tej odpowiedzi „stawia wóz przed koniem". Prawa wynikają z samych ustaw, a nie z powołania się na ich przepisy (Co do zasady. Wyjątkiem jest choćby skarga kasacyjna). Wniosek o informację nie staje się takim wnioskiem dlatego, że powołujemy się na u.d.i.p. – to u.d.i.p. jedynie organizuje procedurę rozpatrzenia wniosku. Ustawa „działa", nawet jeśli jej nie przywołamy w treści wniosku.

Co więcej, trzeba pamiętać, że to na organie ciąży obowiązek prawidłowego zakwalifikowania wniosku i rozpoznania go we właściwym trybie (tak WSA w Kielcach w wyroku z 15 września 2021 r., sygn. akt II SAB/Ke 103/21). Nie może on delegować tego obowiązku na wnioskodawcę. Wbrew powiedzeniu, nieznajomość prawa nie zawsze szkodzi – a przynajmniej nie w tym przypadku. Zgodnie z art. 9 Kodeksu postępowania administracyjnego, organy administracji publicznej są obowiązane do należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania administracyjnego.

Organy czuwają nad tym, aby strony i inne osoby uczestniczące w postępowaniu nie poniosły szkody z powodu nieznajomości prawa, i w tym celu udzielają im niezbędnych wyjaśnień i wskazówek. Tym samym to organy mają obowiązek znać prawo i procedury, a nie wnioskodawcy. Wezwanie jest więc bezpodstawne i świadczy o całkowitym niezrozumieniu podstawowych zasad postępowania administracyjnego.

Monika Majecka

Łódź

Chrońmy dane