OR.1431.29.201

Temat: wniosek o udzielenie inf publicznej - Tom Kowalski
Nadawca: Violetta Miniuk <vminiuk@powiat.hajnowka.pl>
Data: 04.07.2019, 10:39
Adresat: "wpietruczuk@powiat.hajnowka.pl" <wpietruczuk@powiat.hajnowka.pl>

przesyłam wniosek i odpowiedź

--- Treść przekazanej wiadomości ---
Temat: Fwd: Starostwo Powiat hajnowski
Data: Mon, 1 Jul 2019 08:03:56 +0200
Nadawca: Sekretariat Starostwa Powiatowego w Hajnówce <starostwo@powiat.hajnowka.pl>
Adresat: Violetta Miniuk <biuro.rady@powiat.hajnowka.pl>

--- Treść przekazanej wiadomości ---
Temat: Starostwo Powiat hajnowski
Data: Mon, 1 Jul 2019 00:11:33 +0200
Nadawca: [redacted]
Adresat:sekretariat@powiat.hajnowka.pl

WNIOSEK

O UDOSTĘPNIENIE INFORMACJI PUBLICZNEJ

Na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz. U. Nr 112, poz. 1198) zwracam się z prośbą o udostępnienie informacji w następującym zakresie:

1. Czy wyznaczono Inspektora Ochrony Danych (IOD) zgodnie z art 37 RODO?

2. Czy IOD jest pracownikiem urzędu, czy też IOD jest zewnętrzną firmą?

3. W przypadku zewnętrznego IOD proszę podać: firmę i kwotę za obsługę (np. w formie - zł brutto /miesiąc).

4. W przypadku zewnętrznego IOD proszę podać czas obowiązywania umowy (data nawiązania i data wygaśnięcia umowy).

5. Czy urząd (zgodnie z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności), zapewnił okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok. Kto go ewentualnie wykonywał. Proszę o podanie kosztów audytu.

6. Czy urząd (zgodnie z rozporządzeniem w sprawie Krajowych Ram Interoperacyjności) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b)skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c)stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7. Czy urząd, zgodnie ze standardami kontroli zarządczej, dokonuje nie rzadziej niż raz w roku identyfikacji ryzyka w odniesieniu do celów i zadań. Czy zgodnie ze wskazanymi standardami, identyfikacja ryzyka następuje także wobec celów i zadań jednostek podległych lub nadzorowanych?

8. Czy jednostka zrealizowała obowiązki wynikające z rozdziału 5 (art 21-25) Obowiązki podmiotów publicznych - ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa?

- wyznaczono osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

- zapewniono zarządzanie incydentem w podmiocie publicznym

-zapewniono osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami,
w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

-wprowadził dokumentację dotyczącą cyberbezpieczeństwa

FORMA PRZEKAZANIA INFORMACJI:

Przesłanie informacji pocztą elektroniczną na adres e-mail.

Załączniki:

[redacted]docx 13,6 KB