

Goszczanów , dn. 14.03.2017 r.

**Osoba Prawna**  
**Szulc-Efekt sp. z o. o.**  
**ul. Poligonowa 1**  
**04-051 Warszawa**  
**nr KRS: 0000059459**  
**Kapitał Zakładowy: 222.000,00 pln.**  
**www.gmina.pl [www.samorzad.pl](http://www.samorzad.pl)**

Na podstawie art. 14 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej w związku z wnioskiem o jej udostępnienie złożonym drogą elektroniczną w dniu 09.02.2017 r. (w zakresie w jakim stanowi wniosek o udostępnienie informacji publicznej) udzielam żądanej informacji:

*„Wnosimy o udzielenie informacji publicznej w przedmiocie czy Urząd (Gmina) ustanowiła i eksploatuje - System Zarządzania Bezpieczeństwem Informacji - scilicet - w rozumieniu dyspozycji §20 ust. 1 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. 2012.526) ? „*

Zarówno w §20 ust. 1 jak i w §20 ust 3 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, nie znajdują się wymagania dotyczące sporządzenia jednego dokumentu pn. „System Zarządzania Bezpieczeństwem Informacji”, w związku z powyższym nie dysponujemy takim dokumentem sporządzonym na podstawie tych przepisów.

W urzędzie funkcjonuje natomiast wiele dokumentów umożliwiających realizację i egzekwowanie zapisów §20 ust. 2 w/w rozporządzenia w zakresie zarządzania bezpieczeństwem informacji (Regulamin organizacyjny urzędu, Polityka bezpieczeństwa przetwarzania danych osobowych, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, systematycznie zmieniane i dostosowywane zakresy czynności pracowników, upoważnienia dla pracowników do wykonywania określonych czynności w tym do przetwarzania danych osobowych, plan ochrony informacji niejawnych, instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone” oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony, procedury bezpiecznej eksploatacji i szczególne wymagania bezpieczeństwa dla systemu do przetwarzania informacji niejawnych o klauzuli „zastrzeżone”, upoważnienia do przetwarzania informacji niejawnych, Wszystkie te dokumenty składają się w naszym urzędzie na „System Zarządzania Bezpieczeństwem Informacji”.

*Jeśli odpowiedź na powyższe pytanie jest twierdząca - w trybie wyżej powołanych przepisów - wnosimy o udzielenie informacji publicznej w przedmiocie - czy Urząd (Gmina) opracował wzmiankowany System Zarządzania Bezpieczeństwem Informacji na podstawie Polskiej Normy PN-ISO/IEC 27001 - stosownie do wymogów §20 ust. 3 cytowanego powyżej Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, (...) ?*

Urząd nie opracował systemu zarządzania bezpieczeństwem informacji na podstawie Polskiej Normy PN-ISO/IEC 27001. Należy przy tym zwrócić uwagę, że §20 ust. 3 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 nie nakazuje opracowania i wdrożenia systemu zarządzania bezpieczeństwem informacji w oparciu o normę PN-ISO/IEC 27001, a jedynie znajduje się w nim stwierdzenie, że wymagania w tym zakresie uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie tej normy. Można więc „budować” system zarządzania bezpieczeństwem informacji zarówno w oparciu o w/w normę, jak i w oparciu bezpośrednio o przepisy §20 ust. 1 i 2 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.

*W trybie wyżej powołanych przepisów - wnosimy o udzielenie informacji publicznej w przedmiocie - kiedy ostatni raz wykonano w Jednostce Samorządu Terytorialnego - okresowy audyt wewnętrzny w zakresie bezpieczeństwa informacji, w rozumieniu §20 ust. 2 pkt. 14 ww. Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności (...)?*

W 2016 r. przeprowadzaliśmy wewnętrzny audyt bezpieczeństwa informacji w zakresie danych osobowych. Nasza jednostka jest małą jednostką w związku z czym przegląd procedur związanych z zapewnieniem bezpieczeństwa informacji odbywa się w zasadzie w sposób ciągły.