P. Rezolu p. Sieny

Urząd Gminy Mielec
Data 04-11-2019
Nr 2634.2019.P

[redacted]

[redacted], dnia 23 października 2019 roku

W.P. Józef Piątek
Wójt Gminy Mielec
ul. Głowackiego 5
39-300 Mielec

25 maja 2018 roku zaczęła obowiązywać w Polsce ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz.U. 2018 poz. 1000), będąca konsekwencją wdrożenia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. „RODO".

Poprawne wdrożenie w **każdej** organizacji przepisów w/w ustawy wymaga dostosowania procedur ochrony danych osobowych na trzech poziomach funkcjonowania: **organizacyjnym, prawnym i informatycznym.**

Instytut Łączności w Warszawie Państwowy Instytut Badawczy dokonał w 2018 roku porównania dostępnych na rynku narzędzi kryptograficznych pod kątem spełnienia funkcji i ich przydatności w dostosowaniu podmiotów do wymagań RODO oraz możliwości zabezpieczenia danych osobowych od strony informatycznej, uznając jednocześnie szyfrowanie za **adekwatną** metodę zabezpieczania danych osobowych. Adekwatną, czyli również dającą skuteczną ochronę prawną użytkownikowi na gruncie sankcji wynikających z Ustawy i Kodeksu karnego.

Instytut wybrał 11 parametrów, które zdaniem badającego, wypełniają procedury zabezpieczenia danych osobowych i które powinny być podstawą analizy wdrożeniowej oprogramowania stosowanego w każdym podmiocie zobowiązanym do stosowania RODO, a są to:

- Możliwość szyfrowania plików
- Możliwość szyfrowania folderów
- Możliwość odzyskiwania plików
- Zaszyfrowane przesyłanie plików
- Szyfrowanie end to end
- Możliwość zabezpieczonego współdzielenia danych
- Możliwość szyfrowania plików zarchiwizowanych
- Możliwość szyfrowania back'up
- Możliwość śledzenia historii przetwarzania oraz rozliczania przez Administratora Danych Osobowych
- Brak możliwości dostępu do szyfrowanych danych przez producenta narzędzia szyfrującego

- Możliwość zablokowania dostępu do szyfrowanych danych administratorowi sieci IT

Na podstawie art. 2 ust. 1 i art. 10 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (j. t. Dz. U. z 2016 r. poz. 1764 ze zm.) proszę o udostępnienie informacji:

- *Który z w/w parametrów nie jest spełniony przez stosowane w Państwa jednostce informatyczne zabezpieczenie danych osobowych.*
- *Czy zleciliście Państwo obowiązki IODO nałożone na Państwa jednostkę przez Ustawę w formie usługi zewnętrznej i jeżeli tak, to komu?*
- *Czy w budżecie Państwa jednostki na 2020r. zostały zabezpieczone środki finansowe z przeznaczeniem na zakup usług i sprzętu IT, w tym zwiększającego bezpieczeństwo danych osobowych, którymi Państwo administrujecie? Jeżeli tak, to w jakiej wysokości? Jeżeli nie, to czy planujecie Państwo takie zadania na 2020 r.?*
- *Czy zapoznali się Państwo z raportem NIK, który oceniał stopień zabezpieczenia danych w JST i czy wnioski płynące z raportu zostały przeanalizowane przez osoby odpowiedzialne za bezpieczeństwo danych w organizacji ?*
- *Czy urząd i jego jednostki zależne wykonały w 2019 roku zobowiązanie jakie płynie z § 20 Rozporządzenia KRIO – coroczny audyt procesów IT ?*
- *Jakie stosujecie Państwo techniki zabezpieczania danych, w tym danych osobowych i wrażliwych w realizowanych transmisjach pomiędzy urzędem, a jednostkami zależnymi ?*
- *Jak realizujecie Państwo w praktyce wynikające z art. 17 ust 1. Rozporządzenia „RODO" – prawo do bycia zapomnianym"?*
- *Czy w okresie od wejścia w życie Ustawy z dnia 10 maja 2018 roku (Dz.U. 2018 poz. 1000), miały w Państwa jednostce miejsce sytuacje naruszenia przepisów ustawy? Czy zostały one należycie zgłoszone i jakie podjęto kroki celem eliminacji takich sytuacji w przyszłości ? Czy prowadzicie Państwo rejestr zdarzeń i incydentów, którego proadzenie nakłada na Państwa obowiązek ustawowy?*

Odpowiedź proszę kierować wyłącznie na adres poczty elektronicznej:

[redacted]

[redacted]