apytanie

P. Dziuk
15.09. 2020.

Temat: Zapytanie
Nadawca: [redacted]
Data: 08.09.2020, 09:03
Adresat: sekretariat@kondratowice.pl

URZĄD GMINY
KONDRATOWICE
WPŁYNĘŁO - WYSŁANO
dnia 08.09.2020 r.
L.dz. 4164 zał.

p. Sekretarz
prot o dwóch

Szanowni Państwo

w załączeniu przesyłam wniosek o udzielenie informacji publicznej.
Proszę o zwrotną odpowiedź na wniosek przesłać na adres mailowy.

Pozdrawiam
[redacted]

Załączniki:

Zapytanie.pdf 120 KB

[redacted]

Przysieki, dnia 7 września 2020 roku

Szanowni Państwo,

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[1] 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

[1] **Instytut Łączności - Państwowy Instytut Badawczy** jest niezależną, narodową instytucją badawczo-rozwojową w dziedzinie telekomunikacji i technik informacyjnych. Prowadzi prace w zakresie rozwoju sieci telekomunikacyjnej państwa, normalizacji i standaryzacji systemów oraz urządzeń telekomunikacyjnych. Służy rozwojowi społeczeństwa informacyjnego i gospodarce opartej na wiedzy. Zapewnia wsparcie naukowe, badawcze i techniczne instytucjom państwa. Realizuje prace wykorzystywane w praktyce przez podmioty działające na rynku. Współpracuje z organizacjami i instytucjami badawczymi, przyczyniając się w ten sposób do integracji środowiska naukowego. Aktywnie uczestniczymy w budowaniu Europejskiej Przestrzeni Badawczej (European Research Area). Działalność badawcza jest ukierunkowana na rozwój nauki i praktyczne zastosowania wyników badań. Instytut jest jednostką naukową kategorii B.

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:

1. *Który z w/w parametrów nie jest spełniony przez stosowane w Państwa jednostce informatyczne zabezpieczenie danych osobowych.*
2. *Czy zleciliście Państwo obowiązki IODO nałożone na Państwa jednostkę przez Ustawę w formie usługi zewnętrznej i jeżeli tak, to komu?*
3. *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.?*
4. *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?*
5. *Czy urząd i jego jednostki zależne wykonały w 2019 roku zobowiązanie jakie płynie z § 20 Rozporządzenia KRIO[2] – coroczny audyt procesów IT?*
6. *Jakie stosujecie Państwo techniki zabezpieczania danych, w tym danych osobowych i wrażliwych w realizowanych transmisjach pomiędzy urzędem, a jednostkami zależnymi?*
7. *Jak realizujecie Państwo w praktyce wynikające z art. 17 ust 1. Rozporządzenia „RODO" – prawo do bycia zapomnianym"?*
8. *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 prowadzenie nakłada na Państwa obowiązek ustawowy?*

Odpowiedź proszę kierować wyłącznie na adres poczty elektronicznej:
mfilus.kancelaria@gmail.com

[2] 2 Rozporządzenie rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.