FUNDACJA „AKADEMIA ANTYKORUPCYJNA”

mgr Krzysztof Śnieżko

Szkoła Główna Gospodarstwa Wiejskiego w Warszawie

e-mail: krzysztof.sniezko/at/protonmail.com

ORCID: 0000-0003-2692-4351

KARY FINANSOWE ZA NARUSZENIE PRZEPISÓW RODO

Polskie regulacje prawne dotyczące ochrony danych osobowych w przypadku stwierdzenia przez PUODO naruszeń przepisów w tym zakresie przewidują możliwość nakładania wysokich kar finansowych (do 20 mln złotych) na podmioty, w których dopuszczono do tych naruszeń. Praktyka stosowania tych sankcji pokazuje jednak, że są one wymierzane w wysokości znacznie odbiegającej od maksymalnych limitów. Istotne jest aby wysokość kar była adekwatna do spowodowanego zagrożenia. Ważną rolę odgrywa także postawa podmiotu w zakresie podejmowanych czynności mających zminimalizować powstałe straty oraz jego współpraca z PUODO. Ważne są też podejmowane środki techniczne i osobowe w zakresie należytego zabezpieczenia danych oraz wpływ czynników zewnętrznych (cyberataki, włamania) na powstanie wycieku danych osobowych.

Słowa kluczowe: kary, naruszenia, RODO, cyberatak

W Polsce Prezes Urzędu Ochrony Danych Osobowych biorąc pod uwagę[1]

- rodzaj, charakter (umyślny , nieumyślny), czas trwania oraz jego wagę, a także kategorie danych osobowych, których dotyczyło naruszenie,
- odpowiedzialności administratora lub podmiotu przetwarzającego oraz ich działania podjęte w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą a także dotychczas wdrożone środki techniczne i organizacyjne,
- historię dotychczasowych naruszeń oraz współpracę z UODO w zakresie stosowania przepisów RODO oraz sposób powiadomienia UODO w stwierdzonym naruszeniu

nałożył dotychczas osiem kar, z czego aż w trzech przypadkach szczegóły naruszeń nie są publicznie dostępne a chodzi o[2]:

- karę w wysokości 1 973 zł (460 euro) dla wspólnoty mieszkaniowej,
- karę 8 148 zł (1 900 euro) dla spółka zarządzająca nieruchomościami,
- karę w wysokości 30 019, 5 zł (7 000 euro) dla agencja ochrony mienia.

Pozostałe kary pieniężne to:

1. prawie milion zł dla spółki Bisnode,
2. 56 tys. zł dla Dolnośląskiego Związku Piłki Nożnej[3],
3. 3 mln zł dla spółki z branży e-commerce morele.net za wyciek danych,
4. 201 tys. zł dla spółki z branży reklamowej ClickQuickNow,
5. 40 tys. zł dla burmistrza Aleksandrowa Kujawskiego.

Powyższe kary zostały nałożone za następujące naruszenia:

1. zasad ogólnych RODO w tym. zasady zgodności z prawem i zasady poufności,
2. brak zawarcia stosownych umów powierzenia przetwarzania danych osobowych,
3. obowiązku wdrożenia odpowiednich polityk dotyczących przetwarzania danych, w tym dot. retencji,
4. obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych w związku z przechowywaniem nagrań oraz naruszenia zasady integralności i poufności,

---

[1] Urząd Ochrony Danych Osobowych, Jak Prezes UODO nakłada administracyjne kary pieniężne? (online:) www.uodo.gov.pl/pl/138/1244 (dostęp: 15.12.2021).

[2] Jolanta Ojczyk, Europejczycy chętnie zgłaszają naruszenia RODO, urzędy nie boją się wymierzać wysokich kar (online:) www.prawo.pl/biznes/naruszenie-rodo-ile-zgloszen-jakie-kary-raport-dla-piper-2020,497501.html (dostęp:15.12.2021).

[3] Wróblewska Stawowy Kancelaria Prawna, RODO – odpowiedzialność za naruszenie przepisów, (online:) wskp.pl/blog/rodo-odpowiedzialnosc-za-naruszenie-przepisow (dostęp: 15.12.2021).

5. niewskazanie terminu usunięcia danych, naruszenie zasady rozliczalności i ograniczonego przetwarzania oraz nieprawidłowości w rejestrze czynności przetwarzania.

Większość powyższych kar była przede wszystkim spowodowana brakiem właściwych zabezpieczeń technicznych zastosowanych przez administratorów i związanymi z tym pośrednio lub bezpośrednio cyberatakami. W Polsce ofiarą cyberataku było morele.net, urząd miasta w Aleksandrowie Kujawskim, a pośrednio także spółka ClickQuickNow.

Mając na uwadze, iż regulacje RODO pozwalają na nałożenie maksymalnych kar pieniężnych nawet do wysokości 20 000 000 euro dla przedsiębiorstwa oraz do 100 000 złotych na jednostki sektora finansów publicznych, instytuty badawcze, czy Narodowy Bank Polski a także do 10 000 złotych na państwowe i samorządowe instytucje kultury[4] kary nakładane przez Prezesa UODO odbiegają od maksymalnych kar możliwych do nałożenia.

System kar i jego praktyczne stosowanie powinien z jednej strony pełnić funkcję restrykcyjną, mobilizującą podmioty, w których dochodziło do wycieku danych osobowych do ich lepszego zabezpieczenia a z drugiej strony nie powinien skutkować ukrywaniem faktu utraty danych osobowych, w obawie przed wysokimi grożącymi karami. Powinien być zachowany pewien kompromis adekwatności kary do stanu, poziomu naruszenia przepisów w zakresie ochrony danych osobowych w Polsce.

[4] GDPR - Portal Informacyjny, Ogólne warunki nakładania administracyjnych kar pieniężnych (online:) gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-83-ogolne-warunki-nakladania-administracyjnych-kar-pienieznych (dostęp: 15.12.2021).