





# RODO - aktualności

[05.04.2024]

# UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01

UODO ukarał dwa banki za brak zgłoszenia naruszenia ochrony danych osobowych

02

Ochrona danych jednym z celów rozporządzenia DSA. Prezes UODO poza systemem

03

Wyciek danych w DCG Centrum Medyczne we Wrocławiu

04

Prezes UODO wycofuje skargę kasacyjną w sprawie przekazania danych wyborców Poczcie Polskiej

05

Firmy nie mają planu na AI. Kto weźmie odpowiedzialność za algorytmy?

# 01 UODO ukarał dwa banki za brak zgłoszenia naruszenia ochrony danych osobowych

- Prezes UODO ukarał dwa banki za brak zgłoszenia naruszenia ochrony danych. Santander Bank Polska S.A. ma zapłacić karę w wysokości 1 mln zł 440 tys. zł, a Toyota Bank Polska S.A. - 78 tys. zł. W pierwszym wypadku chodziło o dokumenty z danymi klientów banku, które leżały na ulicy, w drugim - na wysłaniu przez bank danych osoby do nieuprawnionego odbiorcy.
- Prezes UODO o naruszeniu ochrony danych osobowych w Santander Bank Polska S.A. dowiedział się z mediów. Polegało ono na upublicznieniu dokumentów bankowych, znajdujących się w porzuconej na jednym z osiedli przesyłce, po tym jak została ona wcześniej skradziona firmie kurierskiej. W przesyłce były m.in. takie dane jak: imiona i nazwiska, daty urodzenia, numery rachunków bankowych, dane adresowe i kontaktowe, numery PESEL, nazwy użytkowników i hasła do banku, czy dane o zarobkach, seria i numery dowodu osobistego, informacje o produktach bankowych.
- Administrator danych tłumaczył, że nie zgłosił tego naruszenia, gdyż przesyłka została odnaleziona przez jedną zidentyfikowaną osobę w krótkim czasie, po jej utracie przez kuriera. Ponadto ustalono, że nie brakowało w niej żadnych dokumentów, a osoba, która znalazła dokumenty, zaniosiła je bezpośrednio na posterunek policji i oświadczyła, że nie kopiowała znalezionych dokumentów. Prezes UODO w toku postępowania uznał, że bez znaczenia jest to, że dane zostały udostępnione tylko jednej zidentyfikowanej osobie. Liczy się bowiem fakt, że przesyłka została odnaleziona przez tę osobę, a w przypadku wystąpienia naruszenia ochrony danych, oceny ryzyka naruszenia praw lub wolności osoby fizycznej powinno się dokonać przez pryzmat osoby zagrożonej, a nie interesów administratora.
- Prezes UODO ukarał także Toyota Bank Polska S.A. W tym przypadku kara wyniosła 78 tys. zł i została nałożona za niezgłoszenie prezesowi UODO naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Administrator zgłosił naruszenie ochrony danych półtora roku po jego wystąpieniu, w momencie gdy zwrócił się do niego organ nadzorczy po otrzymaniu skargi od osoby poszkodowanej tym naruszeniem.

## 02 Ochrona danych jednym z celów rozporządzenia DSA. Prezes UODO poza systemem

- Projekt nowelizacji ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw, który ma dostosować polskie przepisy do unijnego Aktu o usługach cyfrowych (Digital Services Act, w skrócie DSA), znajduje się obecnie na etapie konsultacji społecznych i opiniowania.
- Głównym celem unijnego rozporządzenia jest zwiększenie bezpieczeństwa użytkowników Internetu, m.in. poprzez wprowadzenie jednolitych kryteriów i procedur dotyczących usuwania nielegalnych treści i ich moderacji w państwach członkowskich UE. Wprowadza ono także nowe obowiązki dla platform internetowych i kładzie nacisk również na ochronę danych osobowych użytkowników, uzupełniając w tym zakresie przepisy RODO.
- Dzięki unijnym przepisom platformy internetowe nie mogą już legalnie wykorzystywać danych osób nieletnich i wrażliwych danych osobowych do profilowania w celach reklamowych, co – jak przypomina resort cyfryzacji – udało się w dużej mierze dzięki lobbingowi Polski.
- W projekcie przewidziano, że właściwymi organami w zakresie nadzoru realizacji zadań przewidzianych w DSA zostanie ustanowiony prezes Urzędu Komunikacji Elektronicznej (UKE) i prezes Urzędu Ochrony Konkurencji i Konsumentów (UOKiK). Ewentualne spory kompetencyjne ma z kolei rozwiązywać premier. I choć prawnicy co do zasady oceniają takie rozwiązanie jako sensowne, zwracają uwagę, że potencjalnym problemem może okazać się to, że nie wskazano wśród nich prezesa Urzędu Ochrony Danych Osobowych.
- Zdaniem projektodawcy PUODO nie został ustanowiony jednym z właściwych organów w rozumieniu rozporządzenia, ponieważ odpowiada już za nadzór nad stosowaniem RODO. Rezygnacja z wyznaczenia go jako dodatkowego organu czuwającego nad przestrzeganiem stosowania przepisów DSA ma pomóc utrzymać jednolite zasady przeprowadzania postępowania i pewności prawa, a także zapobiec potencjalnej dyskryminacji określonych podmiotów czy ich nierównemu traktowaniu. Poza tym, projekt przewiduje możliwość współpracy z prezesem UODO. Zakłada również przekazywanie mu informacji związane z przetwarzaniem danych osobowych – ale dopiero na jego wniosek.

# 03 Wyciek danych w DCG Centrum Medyczne we Wrocławiu

- Imię i nazwisko, PESEL, adres, nr telefonu itd., a być może także informacje na temat stanu zdrowia - wyciekły dane pacjentów DCG Centrum Medyczne (do niedawna Dolnośląskie Centrum Ginekologii i Zdrowia Rodziny) przy ul. Powstańców Śląskich we Wrocławiu. Informacja na ten temat pojawiła się w portalu niebezpiecznik.pl, DCG wydało oświadczenie w tej sprawie.
- O kradzieży danych przez hakerów oraz ujawnieniu ich na forum cyberprzestępczym DCG Centrum Medyczne poinformowało swoich pacjentów za pomocą SMS-a. Wydało także oświadczenie, a w nim m.in. informację od spółki Medily, która była dostawcą systemu medycznego, z którego korzystało DCG.
- Z oświadczenia wynika, że do wycieku danych pacjentów DCG doszło 19 marca 2024 w wyniku przestępstwa, na skutek złamania zabezpieczeń stosowanych przez dostawcę oprogramowania - firmę Medily sp. z o.o. Nie wiadomo na razie, kto go dokonał.
- Skradzione dane znalazły się na forum cyberprzestępczym dostępnym w sieci TOR. Po ok. czterech godzinach zostały stamtąd usunięte. Były to: dane osobowe pacjentów (imię i nazwisko, pesel, dane adresowe i dane kontaktowe), informacje o umówionych wizytach (dane pacjenta, dane lekarza wraz z jego specjalizacją oraz data i godzina rezerwacji), dane o stanie zdrowia pacjentów (recepty, skierowania, zwolnienia), dane użytkowników/pracowników (imię, nazwisko, dane kontaktowe).
- Sprawa wycieku danych pacjentów wrocławskiej kliniki DCG Centrum Medyczne jest znana Prezesowi UODO. Organ nadzorczy w związku z tymi wydarzeniami podejmie działania w ramach zadań i uprawnień, przysługujących mu na gruncie ogólnego rozporządzenia o ochronie danych (RODO) oraz przepisów krajowych.

Źródło: [Aktualności – UODO; Wyciek danych pacjentów DCG Centrum Medyczne we Wrocławiu \(www.wroclaw.pl\)](#)

# 04 Prezes UODO wycofuje skargę kasacyjną w sprawie przekazania danych wyborców Poczcie Polskiej

- Prezes UODO pismem procesowym z dnia 26 marca 2024 r. skierowanym do Naczelnego Sądu Administracyjnego cofnął skargę kasacyjną, jaką organ nadzorczy złożył od wyroku WSA w Warszawie uchylającego postanowienie Prezesa UODO o odmowie wszczęcia postępowania w sprawie ze skargi jednego z obywateli na Ministerstwo Cyfryzacji, które przekazało Poczcie Polskiej jego dane osobowe na potrzeby tzw. wyborów kopertowych. Jednocześnie Prezes UODO wniósł o umorzenie postępowania w tej sprawie przed NSA.
- Wskazany wyrok z dnia 13 marca 2024 r. NSA oddalił bowiem skargę kasacyjną Poczty Polskiej od wyroku WSA w Warszawie z dnia 26 lutego 2021 r. zapadłego w sprawie ze skargi Rzecznika Praw Obywatelskich na czynność Ministra Cyfryzacji w przedmiocie udostępnienia Poczcie Polskiej danych osobowych z rejestru PESEL.
- Wskutek powyższego rozstrzygnięcia NSA, ww. wyrok WSA, w którym sąd ten stwierdził bezskuteczność opisanej czynności Ministra Cyfryzacji jako naruszającej przepisy prawa obowiązujące w momencie jej dokonania, stał się prawomocny.
- W kontekście powyższego Prezes UODO nie może podtrzymać stanowiska zaprezentowanego tak w zaskarżonym postanowieniu, jak i w skardze kasacyjnej, gdzie wskazano, że z uwagi na istniejące w obrocie prawnym, w czasie przekazywania danych osobowych z rejestru PESEL, rozstrzygnięcie Prezesa Rady Ministrów z dnia 16 kwietnia 2020 r., nakładające na Poczta Polską obowiązek, o którym mowa w art. 99 ustawy z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2, dla realizacji którego potrzebne jest pozyskanie danych osobowych przez operatora pocztowego, istniała podstawa prawna do udostępnienia tych danych operatorowi pocztowemu i pozyskanie danych osobowych przez Poczta Polską miało oparcie w art. 6 ust. 1 lit. c) RODO.

Źródło: [Prezes UODO wycofuje skargę kasacyjną w sprawie przekazania danych wyborców Poczcie Polskiej \(ceo.com.pl\)](#); [Prezes UODO wycofuje skargę w sprawie przekazania danych Poczcie \(prawo.pl\)](#)



# 05 Firmy nie mają planu na AI. Kto weźmie odpowiedzialność za algorytmy?

- Najnowsze dane SAS wskazują, że co dziesiąta firma nie ma żadnego planu w zakresie dostosowania swoich technologii AI do przepisów. Chodzi m.in. zarówno o rozporządzenia o ochronie danych osobowych (RODO), jak i unijny AI Act. Analitycy twierdzą, iż w 44 proc. przypadków to brak zrozumienia zapowiadanych rozwiązań prawnych.
- Możliwości tej technologii w kontekście strategicznych decyzji dostrzega już 42% polskich menedżerów – wynika z najnowszych badań SAS. Kłopot stanowią jednak liczne wyzwania. Choć dominują te związane z obawami pracowników (40%) i brakami kompetencyjnymi w firmach (34%), to lekceważone nie mogą być też bariery natury regulacyjnej. Co trzeci badany zdaje sobie sprawę, że sytuacja prawna w kontekście AI jest niepewna.
- Na poziomie Unii Europejskiej sztuczną inteligencję w ramy prawne wzięł AI Act, przyjęty w marcu przez Parlament Europejski. Prace legislacyjne nad jego osadzeniem na polskim gruncie dopiero ruszają. W ramach pierwszego etapu konsultacji Ministerstwo Cyfryzacji (MC) zapyta m.in., czy powinien powstać nowy, przeznaczony temu obszarowi organ nadzoru rynku. Regulacja bazuje na podejściu opartym na ryzyku, „uzależniając obowiązki dostawców i podmiotów wdrażających modele i systemy AI od potencjalnego ryzyka wyrządzenia szkód obywatelom, społeczeństwom i gospodarkom”.
- Niestety podejście firm stosujących systemy AI nie napawa optymizmem. Eksperci SAS podkreślają, że ankietowani przedsiębiorcy wykazują się dużą dozą pewności w zakresie zgodności swoich rozwiązań z nowymi lub zapowiadanyymi przepisami. Prawie połowa respondentów wyraziła daleko idące przekonanie, że ich oprogramowanie wykorzystujące AI spełni wymogi prawa, a kolejne 36 proc. była o tym przekonana „do pewnego stopnia”. Dzieje się tak, gdyż firmy w dużej mierze oczekują, że zadba o to zewnętrzny dostawca technologii.
- Firmy i instytucje bardziej niż kiedykolwiek muszą więc zachować należytą staranność przy wyborze dostawcy.

Źródło: [Firmy nie mają planu na AI. Kto weźmie odpowiedzialność za algorytmy - rp.pl](https://www.lex-artist.pl/firmy-nie-maja-planu-na-ai-kto-wezmie-odpowiedzialnosc-za-algorytmy-rp-pl)

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,  
w szczególności rozpowszechniany i kopiowany.*