
LEX ARTIST

RODO - aktualności

[12.02.2024]

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 ponownie karze Morele.net za wyciek danych klientów. Sklep zapłaci ponad 3,8 mln

02 Prokuratura zapłaci 20 tys. zł za udostępnienie niezanonimizowanych danych dziennikarzowi

03 NIL tworzy grupę roboczą dotyczącą bezpieczeństwa danych medycznych

04 OpenAI vs RODO – włoska odpowiedź na popularne rozwiązanie

05 Informacja o monitoringu pracowników jest odrębnym dokumentem. Stanowisko UODO

01 UODO ponownie karze Morele.net za wyciek danych klientów. Sklep zapłaci ponad 3,8 mln zł

- Po tym jak Naczelny Sąd Administracyjny 9 lutego 2023 r. uchylił decyzję Prezesa UODO, nakładającą karę na spółkę Morele.net, Prezes UODO jeszcze raz przeanalizował naruszenie przepisów RODO w Morele.net w związku z dużym wyciekiem danych i ponownie ukarał administratora.
- Postępowanie wykazało, że do naruszenia ochrony danych osobowych doszło przez brak zastosowania przez Spółkę odpowiednich zabezpieczeń, co doprowadziło do wycieku danych osobowych 2,2 mln osób.
- NSA podważył wcześniej kompetencje UODO dotyczące oceny zastosowanych przez administratora środków technicznych i organizacyjnych mających zabezpieczyć dane osobowe. Zdaniem sądu organ powinien uprawdopodobnić posiadanie wiedzy potrzebnej do przeprowadzenia takiej analizy zabezpieczeń. Z uzasadnienia wynikało, że Prezes UODO powinien był powołać biegłego albo wytworzyć wewnętrzny dokument stanowiący wnioski z analizy standardu środków bezpieczeństwa stosowanych przez spółkę, do którego administrator mógłby się odnieść w toku postępowania.
- W związku z tym UODO ponownie przeprowadził postępowanie administracyjne, które również wykazało, że spółka Morele.net stosowała niewystarczające zabezpieczenia techniczne do istniejącego ryzyka naruszenia ochrony danych. Zabrakło też wdrożenia odpowiednich procedur, które pozwoliłyby zareagować na nietypowe zachowania, takie jak zwiększony ruch sieciowy.
- Analiza wykazała, że administrator nie szyfrował części danych (do czego zresztą się przyznał), nie dysponował dwuskładnikowym uwierzytelnianiem, nie przeprowadził analizy ryzyka, która uwzględniałaby m.in. zagrożenia związane z możliwością logowania się do systemu z sieci publicznej. W efekcie dwukrotnie doszło do nieautoryzowanego dostępu z zewnątrz, na skutek którego osoba niepowołana weszła w posiadanie danych klientów spółki Morele.net. Zabrakło też rozwiązań technicznych i administracyjnych pozwalających monitorować ruch w sieci i reagować w przypadku wykrycia nieprawidłowych działań. Potwierdzają to ustalenia, z których wnika, że spółka nie miała pewności czy i jakie dane zostały wykradzione z jej zasobów.

Źródło: Kara UODO dla Morele.net (prawo.pl)

02 Prokuratura zapłaci 20 tys. zł za udostępnienie niezanonimizowanych danych dziennikarzowi

- WSA w Warszawie oddalił skargę Prokuratury Rejonowej w Gorlicach na decyzję Prezesa UODO, w której organ nadzorczy nałożył na administratora karę w wysokości 20 tys. zł. Prokuratura przekazała w trybie dostępu do informacji publicznej dane, które nie zostały uprzednio zanonimizowane.
- Powodem zastosowania sankcji przez Prezesa UODO było niezgłoszenie do organu nadzorczego naruszenia ochrony danych osobowych oraz niezawiadomienie osób, objętych tym incydentem.
- Naruszenie polegało na przekazaniu dziennikarzowi w trybie dostępu do informacji publicznej dokumentów, w których były dane trzech osób. Prezes UODO nie kwestionował samego udostępnienia dokumentacji w trybie dostępu do informacji publicznej, ale to, że przy jej udostępnieniu administrator nie zachował zasad z zakresu ochrony danych osobowych i nie zanonimizował przekazywanych dokumentów.
- Przed Sądem Prokuratura podnosiła argumenty, że naruszenie nie wiązało się z wysokim ryzykiem dla praw lub wolności osób (np. kradzież tożsamości), gdyż dotyczyło tylko trzech osób, a dane otrzymał tylko jeden dziennikarz, który sam je zanonimizował przed publikacją dokumentów. Zdaniem skarżącego działanie dziennikarza świadczyło o tym, że nie miał on zamiaru skorzystać z tych danych w celach przestępczych lub udostępniać ich innym osobom. Stąd zdaniem Prokuratury nie było konieczności zgłaszania naruszenia Prezesowi UODO, gdyż nie istniało wysokie ryzyko naruszenia praw i wolności dla osób, których dotyczyło naruszenie.
- Argumenty te nie przekonały WSA w Warszawie. Sąd uznał, że skarżący próbuje w ten sposób umniejszyć rozmiar naruszenia. Tymczasem zakres ujawnionych danych był szeroki i obejmował m.in. imiona, nazwiska, adresy, numery PESEL, numery dokumentów tożsamości. Wśród tych informacji były także dane małoletniego, w tym o jego stanie zdrowia.

Źródło: Dane udostępnione jako informacja publiczna a RODO (prawo.pl)

03 NIL tworzy Zespół ds. bezpieczeństwa danych medycznych

- 7 lutego 2024 r. w siedzibie Centralnego Ośrodku Badań, Innowacji i Kształcenia w Naczelnej Izbie Lekarskiej (COBIK NIL) odbyło się spotkanie inaugurujące powstanie Zespołu ds. bezpieczeństwa danych medycznych, zrzeszającego przedstawicieli sektora państwowego oraz specjalistów NIL. W wydarzeniu tym wzięli udział przedstawiciele Urzędu Ochrony Danych Osobowych: Jakub Groszkowski, Zastępca Prezesa UODO oraz Monika Krasińska – Dyrektor Departamentu Orzecznictwa i Legislacji.
- Uczestnicy spotkania dyskutowali na temat problematyki związanej z zarządzaniem danymi medycznymi i koniecznością podjęcia działań, które przyniosą korzyść pacjentom, środowisku medycznemu, ale też pracodawcom. Rozważali też możliwe działania, jakie Zespół ds. bezpieczeństwa danych medycznych mógłby podjąć, by wpłynąć na realne zmiany w istniejących regulacjach prawnych. Dalsze działania w tym zakresie powinny dotyczyć m.in. takich obszarów jak dostępność i jakość danych, ich bezpieczeństwo, rozwój i świadomość.
- Zaproponowano wyodrębnienie obszaru danych medycznych jako dedykowanego obszaru polityki publicznej w ochronie zdrowia, wyodrębnienie dedykowanego zespołu ds. danych medycznych, planu dalszego rozwoju systemu gromadzenia i wykorzystywania danych medycznych oraz przygotowanie projektu ustawy o danych medycznych.
- Podczas spotkania mówiono także o edukacji na temat ochrony danych osobowych w sektorze zdrowia oraz wykorzystania narzędzi sztucznej inteligencji do wsparcia, które mogą wspomagać lekarzy w diagnozowaniu chorób i terapii.

Źródło: Aktualności – UODO; NIL - NIL IN tworzy grupę roboczą dotyczącą bezpieczeństwa danych medycznych

04 OpenAI vs RODO – włoska odpowiedź na popularne rozwiązanie

- W niedawnej eskalacji między postępem technologicznym a ochroną prywatności, włoski krajowy organ ochrony danych, Garante, postawił w stan oskarżenia amerykańską firmę OpenAI, twórcę generatywnego chatbota ChatGPT. Zarzuty dotyczą naruszenia ogólnego rozporządzenia o ochronie danych (RODO), fundamentu prawnego Unii Europejskiej dotyczącego prywatności i ochrony danych osobowych.
- Garante rozpoczął swoje dochodzenie wobec ChatGPT w zeszłym roku, po tymczasowym zakazie działania usługi we Włoszech. Zakaz ten został nałożony w odpowiedzi na obawy dotyczące możliwości generowania przez system tekstów, obrazów, i dźwięków mogących naruszać prywatność użytkowników. Kluczowe punkty konfliktu obejmują niewystarczającą ochronę danych osobowych, brak systemu weryfikacji wieku użytkowników, a także ryzyko generowania przez system fałszywych informacji o osobach.
- OpenAI, z kolei, broni swojej pozycji, argumentując, że ich działania są zgodne z RODO i że firma podjęła dodatkowe kroki w celu ochrony danych i prywatności. Zobowiązali się również do ograniczenia ilości danych osobowych wykorzystywanych do szkolenia swoich algorytmów, podkreślając chęć poznawania świata, a nie indywidualnych użytkowników.
- Rosnąca popularność i możliwości generatywnych systemów AI, takich jak ChatGPT, przyciągają uwagę regulatorów na całym świecie. Od dochodzeń Federalnej Komisji Handlu w Stanach Zjednoczonych dotyczących relacji OpenAI z gigantami technologicznymi po europejskie i brytyjskie organy konkurencji badające inwestycje Microsoftu w OpenAI.
- W tle tych wszystkich wydarzeń trwa praca nad przełomową ustawą o sztucznej inteligencji w UE, która ma być pierwszym na świecie kompleksowym regulatorem dotyczącym AI. Przepisy te mają za zadanie nie tylko nadążać za szybkim rozwojem technologii, ale również zapewnić, że innowacje nie będą szły na koszt prywatności i bezpieczeństwa obywateli.

Źródło: OpenAI vs RODO - włoska odpowiedź na popularne rozwiązanie - Brandsit

05 Informacja o monitoringu pracowników jest odrębnym dokumentem. Stanowisko UODO

- Nie wystarczy, że nowo zatrudniana osoba zapoznała się z regulaminem pracy zawierającym zasady monitoringu. Tak uznał Urząd Ochrony Danych Osobowych w stanowisku wydanym dla DGP.
- DGP zwrócił się do UODO z szeregiem pytań, m.in.

1) Czy można przyjąć, że zapoznanie pracownika z regulaminem pracy przed dopuszczeniem do pracy będzie jednocześnie spełnieniem powyższego obowiązku i nie przekazywać odrębnej informacji o zasadach monitoringu?
2) Czy jest to zawsze odrębny obowiązek pracodawcy?

- W stanowisku UODO przyjęto wprost, że obowiązek poinformowania pracownika powinien być rozumiany jako odrębny obowiązek pracodawcy, co urząd uzasadnił dwoma argumentami, tj. umieszczeniem tego obowiązku w oddzielnej jednostce redakcyjnej art. 222 ustawy z 26 czerwca 1974 r. – Kodeks pracy oraz zasadą przejrzystości wynikającą z art. 5 RODO.
- Zgodnie ze stanowiskiem UODO obowiązki wynikające z art. 222 par. 6 i par. 8 k.p. to odrębne obowiązki. A dodatkowym argumentem – nieprzywołanym w stanowisku UODO – może być również konstrukcja rozporządzenia ministra rodziny, pracy i polityki społecznej z 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej, w którym w par. 3 pkt 2 lit. e i f również są wymienione dwa dokumenty, które powinny być przechowywane w części B akt osobowych, a mianowicie:

1) potwierdzenie zapoznania się przez pracownika z treścią regulaminu pracy (art. 1043 par. 2 k.p.) albo obwieszczenia (art. 150 par. 7 k.p.),
2) potwierdzenie poinformowania pracownika o celu, zakresie oraz sposobie zastosowania monitoringu (art. 222 par. 8 k.p.)

Źródło: Informacja o monitoringu pracowników jest odrębnym dokumentem. Stanowisko UODO - GazetaPrawna.pl