
LEX ARTIST

RODO - aktualności

[24.01.2024]

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 Ministerstwo Zdrowia: decyzja UODO powinna być skierowana do Adama Niedzielskiego

02 Mirosław Wróblewski nowym prezesem UODO, Senat poparł jego kandydaturę

03 Firma ma odrębne uprawnienia RODO jako pracodawca i przedsiębiorca

04 WSA o braku prawnie uzasadnionego interesu w pobieraniu i publikowaniu danych osobowych

05 Prezes UODO nałożył karę w wysokości 10 tys. zł na Sąd Okręgowy w Krakowie za niezgłoszenie naruszenia

06 Mamy pierwszy przypadek ransomware w banku w Polsce. Bank Spółdzielczy w Zambrowie ofiarą cyberataku

07 W 2023 r. nałożono "kary za RODO" na sumę 1,78 mld euro

01 Ministerstwo Zdrowia: decyzja UODO powinna być skierowana do Adama Niedzielskiego

- Były już minister zdrowia Adam Niedzielski, będąc administratorem danych przetwarzanych w elektronicznym systemie, pozyskał z niego dane, które opublikował w jednym z serwisów społecznościowych. Były to informacje na temat lekarza, który wystawił sobie receptę.
- PUODO w grudniu ub. roku poinformował, że wpis w mediach społecznościowych zawierał informację na temat lekarza, który wystawił sobie receptę na lek z grupy psychotropowych. - Tym samym minister zdrowia bezprawnie ujawnił dane o stanie zdrowia tej osoby - uznał UODO.
- W toku postępowania UODO ustalił, że administratorem ujawnionych danych jest Minister Zdrowia jako organ, bowiem to on został wyposażony w określone uprawnienia pozwalające mu na dostęp do danych przetwarzanych we wspomnianym systemie w ściśle zdefiniowanych przypadkach i w określonych celach. Dane lekarza zostały ujawnione z naruszeniem przepisów RODO oraz krajowych regulacji szczególnych, za przestrzeganie których odpowiedzialność ponosi administrator danych, czyli Minister Zdrowia - wskazał UODO.
- Po decyzji prezesa UODO część ekspertów podnosiła wątpliwości, czy w tej konkretnej sytuacji nie powinien odpowiadać Adam Niedzielski, który wówczas jako minister zdrowia piastował funkcję administratora danych, a nie Minister Zdrowia jako organ administrujący danymi.
- Według Ministerstwa Zdrowia decyzja prezesa Urzędu Ochrony Danych Osobowych o nałożeniu kary w wysokości 100 tys. zł powinna zostać skierowana do Adama Niedzielskiego, który naruszył przepisy o ochronie danych osobowych jako osoba fizyczna. Resort zdrowia zaskarżył decyzję prezesa UODO do Wojewódzkiego Sądu Administracyjnego z uwagi na skierowanie jej do podmiotu, który nie jest stroną w sprawie, tj. do Ministra Zdrowia.

Źródło: UODO nałożył karę na ujawnienie danych o zdrowiu lekarza (prawo.pl)

02 Mirosław Wróblewski nowym prezesem UODO, Senat poparł jego kandydaturę

- Senat zatwierdził decyzję Sejmu o wyborze Mirosława Wróblewskiego na prezesa Urzędu Ochrony Danych Osobowych.
- Mirosław Wróblewski jest radcą prawnym, dyrektorem Zespołu Prawa Konstytucyjnego, Międzynarodowego i Europejskiego Biura Rzecznika Praw Obywatelskich. Jest autorem ponad 50 artykułów i publikacji naukowych z zakresu prawa konstytucyjnego, międzynarodowego i europejskiego, w tym ochrony danych osobowych (jest m.in. współautorem komentarza do nowej ustawy o ochronie danych osobowych oraz poradnika i komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości). Jest wykładowcą m.in. na studiach podyplomowych „Prawo nowoczesnych technologii" oraz „Ochrona danych osobowych" w Akademii im. Leona Koźmińskiego.
- Przed senackim głosowaniem Mirosław Wróblewski mówił, że najważniejsza dla niego jako prezesa UODO będzie efektywna ochrona praw podmiotów danych osobowych, ale także egzekwowanie prawa i dbanie o spójność przepisów krajowych z europejskimi. Wyraził też opinię, że Urząd powinien "wykazywać większą mobilność", być bardziej obecny regionalnie i lokalnie, np. we współpracy z organizacjami pozarządowymi.
- Wcześniej zostały wycofane kandydatury Andrzeja Rybusa-Tołłoczko z rekomendacji Polski 2050 oraz Konrada Komornickiego zgłoszonego przez PSL.
- Zgodnie z przepisami, kadencja prezesa UODO trwa 4 lata, licząc od dnia złożenia ślubowania. Ta sama osoba nie może być Prezesem Urzędu więcej niż przez dwie kadencje.

Źródło: Mirosław Wróblewski nowym prezesem UODO (prawo.pl)

03 Firma ma odrębne uprawnienia RODO jako pracodawca i przedsiębiorca

- Pracodawca i przedsiębiorca to terminy często używane zamiennie, co może prowadzić do paradoksów prawnych, zwłaszcza w zakresie przepisów dotyczących ochrony danych pracowników.
- Ten sam podmiot prawny może pełnić różne role społeczne. Identyfikacja konkretnej roli jest istotna przy rozważaniach dotyczących przetwarzania danych osobowych. Przedsiębiorca to podmiot prowadzący działalność gospodarczą. Pracodawca – zatrudnia pracowników. Pracodawca nie musi być więc przedsiębiorcą.
- Rozróżnienie pojęciowe między pracodawcą a przedsiębiorcą ma znaczenie np. w przypadku stosowania legalnego monitoringu poczty elektronicznej, który jest uregulowany w kodeksie pracy, ale nie obejmuje kontroli w celu zapobiegania naruszaniu tajemnicy przedsiębiorstwa. Regulacje z Kodeksu pracy dotyczą jedynie monitoringu mającego na celu wykonanie zadań przez pracodawcę, a przedsiębiorca może wprowadzić monitoring w celu ochrony swoich interesów, spełniając jednocześnie wymogi RODO. Zatem przedsiębiorca, w obliczu zagrożenia dla swoich interesów, ma prawo monitorować pocztę nie tylko pracowników, ale także innych osób, które są kluczowe dla realizacji jego interesów.
- Przedsiębiorca może także nagrywać rozmowy pracowników z klientami w celu ochrony przed roszczeniami, a to nie jest kontrola pracownika, lecz utrwalenie sposobu wykonania usługi w kontekście ewentualnych roszczeń osób trzecich. Dopuszczalność nagrywania rozmów zależy od spełnienia wymogów zawartych w RODO.
- Podobnie jest w przypadku kontroli jakości produktu, gdzie przedsiębiorca może prowadzić monitoring wizyjny poza reżimem kodeksu pracy, jeśli wykaże, że ochrona przed roszczeniami kontrahentów dotyczącymi jakości produktu wymaga nagrania procesu produkcyjnego wraz z wizerunkiem pracownika.

Źródło: Firma ma odrębne uprawnienia RODO jako pracodawca i przedsiębiorca - GazetaPrawna.pl

04 WSA o braku prawnie uzasadnionego interesu w pobieraniu i publikowaniu danych osobowych

- W niedawno opublikowanym uzasadnieniu orzeczenia WSA w Warszawie poruszono – kolejny raz – kwestię pobierania danych osobowych z ogólnodostępnych, publicznych rejestrów oraz ich dalszego rozpowszechniania.
- Jak wskazał WSA w Warszawie "główna oś sporu w niniejszej sprawie dotyczy tego, czy Spółka, która pozyskała dane osobowe uczestniczki postępowania z ogólnopolskiego Rejestru Praktyk Zawodowych uprawniona była do ich przetwarzania na prowadzonym przez nią na ogólnodostępnym portalu internetowym w oparciu o przesłankę wskazaną w art. 6 ust. 1 lit f RODO.
- Sprawa ta rozpoczęła się od skargi fizjoterapeuty, którego dane osobowe w poniższym zakresie zostały pobrane przez administratora danych z Rejestru Praktyk Zawodowych "imienia, nazwiska, nr telefonu komórkowego, nr PWZ, NIP oraz adresu siedziby działalności gospodarczej, prowadzonej przez skarżącą".
- Spółka jako podstawę przetwarzania danych osobowych uczestniczki postępowania wskazała art. 6 ust. 1 lit f RODO, który to przepis stanowi, że przetwarzanie jest zgodne z prawem wyłącznie w przypadku, gdy – i w takim zakresie, w jakim przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.
- Zdaniem Sądu w niniejszej sprawie Spółka nie legitymuje się tak rozumianym “prawnie uzasadnionym interesem”. Spółka nie wykazała bowiem żeby między nią a uczestniczką postępowania istniały jakiekolwiek powiązania. Uczestniczka postępowania nie jest klientem Spółki. Nie miała ona zatem żadnych rozsądnych przesłanek aby spodziewać się że jej dane osobowe mogą być przetwarzane przez Spółkę.

Źródło: Judykatura.pl

05 Prezes UODO nałożył karę w wysokości 10 tys. zł na Sąd Okręgowy w Krakowie za niezgłoszenie naruszenia

- Prezes Urzędu Ochrony Danych Osobowych nałożył administracyjną karę pieniężną w wysokości 10 tys. zł na Sąd Okręgowy w Krakowie za brak zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych oraz niezawiadomienie o naruszeniu, bez zbędnej zwłoki osób, których dane dotyczą.
- Do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych osobowych złożone przez Ministra Spraw Zagranicznych (dalej również jako MSZ). Dotyczyło ono doręczenia przez operatora pocztowego adresatowi uszkodzonej i niekompletnej przesyłki. Prezes UODO został poinformowany nie przez administratora danych, a przez MSZ, któremu adresat zgłosił nieprawidłowości w jej dostarczeniu.
- W przedmiotowej sprawie doszło do naruszenia ochrony danych osobowych siedmiu osób, przy czym wobec czterech z nich powstało wysokie ryzyko naruszenia ich praw lub wolności z uwagi na zakres naruszonych danych osobowych. Naruszenie objęło numery PESEL, a także informacje o stanie zdrowia powódki oraz opinie psychologiczne dwójki dzieci. Informacje te powiązane z m.in. imionami i nazwiskami oraz kontekstem sprawy rozwodowej mogą powodować utratę kontroli nad danymi, zagrożenia związane z udostępnieniem numeru PESEL, ale również dyskryminację w środowisku tych osób czy naruszania ich dóbr osobistych.
- Zdaniem UODO, Administrator podejmując decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawił te osoby przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu ochrony danych osobowych i możliwości przeciwdziałania potencjalnym szkodom. Postępowanie organu wykazało też inne nieprawidłowości związane z naruszeniem. Inspektor ochrony danych Sądu błędnie ocenił poziom ryzyka naruszenia praw lub wolności osób fizycznych. Wskazał bowiem, że fakt, iż dokumenty zostały sporządzone w języku polskim, a wysłane do Wielkiej Brytanii, nie powoduje powstania wysokiego ryzyka w tym zakresie.

Źródło: Aktualności - UODO

06 Mamy pierwszy przypadek ransomware w banku w Polsce. Bank Spółdzielczy w Zambrowie został ofiarą cyberataku

- Jak donosi serwis Sekurak, usługi elektroniczne Banku Spółdzielczego w Zambrowie kilka dni temu przestały działać po tym, jak instytucja padła ofiarą cyberataku. Sekurak pisze, że prawdopodobną przyczyną incydentu było zainfekowanie systemu banku złośliwym oprogramowaniem, tzw. ransomware.
- Informację o poważnej awarii potwierdza oświadczenie BS w Zambrowie, jakie można znaleźć na jego stronie internetowej. Atak miał miejsce 16 stycznia. – Po dokonaniu analizy stwierdzono, iż dane klientów zostały zaszyfrowane. Niezwłocznie po zidentyfikowaniu incydentu bank zabezpieczył systemy informatyczne oraz rozpoczął pracę nad odtworzeniem funkcjonalności systemu oraz udostępnieniem klientom pełnego dostępu do usług.
- Konsekwencją opisanego wyżej naruszenia ochrony danych osobowych polegającego na zaszyfrowaniu danych jest czasowy brak dostępności do elektronicznych usług bankowych – realizowania płatności i dysponowania środkami zgromadzonymi na rachunkach bankowych.
- Z informacji na stronie BS w Zambrowie wynika, że obecnie zarówno jego internetowy serwis transakcyjny, jak i aplikacja mobilna działają obecnie poprawnie. Natomiast awaria wywołała obawy, iż atak może rozszerzyć się na inne banki zrzeszone w grupie BPS. Biuro prasowe tej instytucji zapewniło, że ryzyka takiego nie ma, gdyż systemy poszczególnych członków grupy nie są ze sobą połączone.

Źródło: Mamy pierwszy przypadek ransomware w banku w Polsce. Bank Spółdzielczy w Zambrowie został ofiarą cyberataku. (sekurak.pl); Cashless - Kłopoty Banku Spółdzielczego w Zambrowie. Instytucja padła ofiarą cyberataku

07 W 2023 r. nałożono "kary za RODO" na sumę 1,78 mld euro

- Jest już dostępny raport "DLA Piper GDPR fines and data breach survey: January 2024", poświęcony naruszeniom i administracyjnym karom pieniężnym, związanym z RODO.
- Kluczowe ustalenia:
  - w 2023 r. nałożono "kary za RODO" na sumę 1,78 mld euro,
  - na powyższą kwotę składa się w szczególności 1,2 mld euro - rekordowa administracyjna kara pieniężna, nałożona przez irlandzki organ nadzorczy na spółkę Meta
  - Niemcy, Holandia i Polska miały największą liczbę zgłoszonych naruszeń w okresie od stycznia 2023 do stycznia 2024: było ich odpowiednio 32.030, 20.235 i 14.167.

Źródło: 1706085545255 (licdn.com); https://www.linkedin.com/posts/adamklimowski_dla-piper-gdpr-fines-and-data-breach-survey-ugcPost-7155841541637341184-jhky?utm_source=share&utm_medium=member_desktop