
LEX ARTIST

RODO - aktualności

27 luty 2023 r.

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 Kara UODO - Środki organizacyjne i techniczne powinny się uzupełniać

02 EROD publikuje trzy wytyczne po konsultacjach społecznych

03 Cała władza w ręce UODO. Rozporządzenie o ochronie danych osobowych (RODO), działa

04 Pacjent musi wyrazić jasną zgodę na udzielanie informacji o jego zdrowiu

05 Newsletter UODO

01 Kara UODO - Środki organizacyjne i techniczne powinny się uzupełniać

- Urząd Ochrony Danych Osobowych nałożył na Sąd Rejonowy Szczecin-Centrum w Szczecinie administracyjną karę pieniężną w wysokości 30 tys. zł. W decyzji zostało stwierdzone naruszenie przepisów RODO polegające na niewdrożeniu przez administratora odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci.
- Do Urzędu Ochrony Danych Osobowych 20 września 2020 r. wpłynęło zgłoszenie naruszenia ochrony danych osobowych złożone przez Sąd Rejonowy Szczecin-Centrum w Szczecinie. Do naruszenia doszło na skutek zagubienia trzech nośników danych typu pendrive: jednego służbowego – szyfrowanego oraz dwóch prywatnych – nieszyfrowanych. Na zagubionych nośnikach znajdowały się projekty orzeczeń i uzasadnień, zawierające dane osobowe (z okresu od grudnia 2004 r. do sierpnia 2020 r.).
- Podczas prowadzonego postępowania ustalono wieloletne korzystanie na służbowym sprzęcie komputerowym z prywatnych nośników, niezabezpieczonych i niezweryfikowanych przez dział IT szczecińskiego sądu. Okazało się również, że administrator pomimo istniejących procedur dotyczących zakazu użytkowania prywatnych nośników danych nie prowadził nadzoru nad tym, czy pracownicy sądu stosowali się do wewnętrznych uregulowań.
- Organ w toku postępowania stwierdził, że administrator nie wdrożył adekwatnych środków technicznych, np. blokady portów USB w celu uniemożliwienia korzystania z prywatnych nośników danych. Podkreślić należy, że administrator dopuszczający użytkowanie przenośnych nośników danych powinien zapewnić, aby były to nośniki służbowe zweryfikowane przez dział IT i zabezpieczane przed dostępem osób nieuprawnionych w przypadku ich zgubienia lub pozostawienia bez nadzoru.

- Wdrożenie przez administratora środków technicznych i organizacyjnych nie jest działaniem jednorazowym, ale powinno ono przybrać postać ciągłego procesu, w ramach którego administrator dokonuje przeglądu i w razie potrzeby uaktualnia przyjęte wcześniej zabezpieczenia. Regularna ocena zastosowanych środków bezpieczeństwa pozwoliłaby administratorowi na weryfikację, czy wprowadzona procedura określająca zakaz użytkowania prywatnych nośników danych jest przestrzegana, a więc i skuteczna. W ocenie organu, gdyby administrator zweryfikował sposób realizacji środka organizacyjnego w postaci zakazu użytkowania prywatnych nośników danych, to wówczas znacząco obniżyłby ryzyko wystąpienia naruszenia albo nawet doprowadziłby do całkowitego jego wyeliminowania.

Źródło: *https://www.uodo.gov.pl/pl/138/2639*

02 EROD publikuje trzy wytyczne po konsultacjach społecznych

Po przeprowadzeniu konsultacji publicznych EROD przyjęła w ostatecznej wersji trzy zestawy wytycznych:

- Wytyczne dotyczące zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO: Wytyczne wyjaśniają wzajemne zależności między terytorialnym zakresem stosowania RODO (art. 3) a przepisami dotyczącymi międzynarodowego przekazywania danych w rozdziale V. Mają one pomóc administratorom i podmiotom przetwarzającym w ustaleniu, czy operacja przetwarzania stanowi międzynarodowy transfer danych, oraz zapewnić wspólne rozumienie pojęcia międzynarodowego przekazywania danych.
- Wytyczne dotyczące certyfikacji jako narzędzia przekazywania danych: Głównym celem niniejszych wytycznych jest dalsze wyjaśnienie praktycznego zastosowania tego narzędzia transferu. Wytyczne składają się z czterech części, z których każda koncentruje się na konkretnych aspektach dotyczących certyfikacji jako narzędzia do transferów.
- Wytyczne dotyczące zwodniczych wzorców projektowych w interfejsach platform mediów społecznościowych: Wytyczne zawierają praktyczne zalecenia dla projektantów i użytkowników platform mediów społecznościowych dotyczące sposobu oceny i unikania wprowadzających w błąd wzorców projektowych w interfejsach mediów społecznościowych, które naruszają wymogi RODO.

Źródło: *https://edpb.europa.eu/news/news/2023/edpb-publishes-three-guidelines-following-public-consultation_en*

03 Cała władza w ręce UODO. Rozporządzenie o ochronie danych osobowych (RODO), działa

- Tylko za ubiegły rok sumaryczna wysokość wszystkich nałożonych kar przekroczyła 2 mld euro, z czego 1,3 mld w Irlandii. Polska pod tym względem znajduje się w środku rankingu z ponad 3,3 mln euro nałożonych grzywien. W całej Unii Europejskiej liczba zgłoszeń naruszenia ochrony danych przekroczyła 100 tys. W Polsce – 13 tys.
- Wiele wskazuje na to, że wysokość kar wzrośnie, podobnie jak dotkliwość ich egzekwowania. Zaostrzeniem bardzo zainteresowana jest Komisja Europejska. Niektórzy politycy uznali działanie systemu ochrony danych za punkt honoru, choćby nasz czołowy reprezentant w UE, europejski inspektor ochrony danych Wojciech Wiewiórowski. W KE i okolicach krążą pogłoski o nieuniknionym zaostrzeniu egzekwowania przepisów poprzez wdrożenie systemu umożliwiającego duże śledztwa i nakładanie naprawdę wysokich grzywien na dużych graczy.

Źródło: *https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8664379,cala-wladza-w-rece-uodo-rodo-rozporzadzenie-o-ochronie-danych-osobowych.html*

04 Pacjent musi wyrazić jasną zgodę na udzielanie informacji o jego zdrowiu

- Lekarz nie powinien się domyślać zgody pacjenta na przekazanie informacji o stanie zdrowia innym osobom – konieczne jest złożenia przez pacjenta jasnego oświadczenia w tym zakresie. Sama obecność innej osoby podczas rozmowy z pacjentem, nie oznacza automatycznie, że pacjent chce, aby w obecności tej osoby „opowiadać" o jego stanie zdrowia.
- Zasadą jest to, że lekarz może udzielić informacji o stanie zdrowia pacjenta innym osobom za zgodą pacjenta (lub jego przedstawiciela ustawowego). Lekarz jest zwolniony z obowiązku zachowania tajemnicy zawodowej, gdy przepisy konkretnych ustawy przewidują możliwość udzielenia informacji o stanie zdrowia pacjenta innym osobom lub instytucjom. Jednym z takich wyjątków jest upoważnienie pacjenta do udzielania informacji innej osobie.
- Pacjent może dokonać upoważnienia w dowolnej formie, zatem także ustnie, pisemnie, czy elektronicznie poprzez Internetowe Konto Pacjenta. Obecne przepisy nakazują, aby poinformować pacjenta przed złożeniem przez niego m.in. oświadczenia o upoważnieniu o możliwości złożenia go za pośrednictwem IKP, zaś oświadczenie złożone w inny sposób niż za pośrednictwem IKP należy zamieścić się w dokumentacji indywidualnej wewnętrznej. Powyższe oznacza, że w przypadku upoważnienia w drodze rozmowy należy sporządzić odpowiednią notatkę z przebiegu rozmowy, warto także poczynić stosowną adnotację w dokumentacji medycznej.

Źródło: *https://www.prawo.pl/kadry/ochrona-niezaleznosci-inspektora-ochrony-danych-wyroki-tsue,519828.html*

05 Newsletter UODO

W Newsletterze:

- Podstawa pozyskiwania szczególnych kategorii danych osobowych obywateli Ukrainy
- Pojazdy komunikacji miejskiej bez monitoringu fonicznego

Pracodawca w celu zapewnienia bezpieczeństwa pracowników lub ochrony mienia może zainstalować monitoring, ale powinien on umożliwiać jedynie rejestrację obrazu, a nie dźwięku. Nie ma więc podstaw prawnych, by w kabinie kierowcy w pojazdach komunikacji miejskiej montowane były kamery umożliwiające rejestrację dźwięku.

- Lepsza ochrona danych osobowych przy zgłaszaniu zdarzeń niepożądanych
- Finlandia: kara 230 tys. euro za naruszenie ochrony danych osobowych pracowników
- Hiszpańska branża reklamowa ma swój kodeks postępowania