
LEX ARTIST

RODO - aktualności

24 stycznia 2022 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 Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania

02 RODO nie pozwala na ujawnienie danych hejtera

03 EROD: Wytyczne w sprawie prawa dostępu do danych

04 MEiN podaje dane o szczepieniach na uczelniach - pozyskanie prawnie wątpliwe

05 Styczniowy newsletter UODO

01 Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania (1)

- CERT Polska stworzył dokument skierowany do administratorów, twórców i projektantów systemów informatycznych wymagających kontroli dostępu użytkowników i pozwalających na uwierzytelnienie z użyciem hasła
- CERT Polska wskazuje, że system uwierzytelniający, m.in. :

1) POWINIEN stosować bezpieczny algorytm hashujący do przechowywania haseł
2) NIE POWINIEN wymuszać okresowej zmiany haseł użytkowników
3) NIE POWINIEN pozwalać na ustawienie hasła znajdującego się na liście słabych/często używanych haseł3
4) NIE POWINIEN pozwalać na ustawienie hasła zawierającego przewidywalne człony (np. nazwa firmy, usługi)
5) POWINIEN ustalać minimalną długość hasła na co najmniej 12 znaków
6) POWINIEN pozwalać na ustawienie hasła o długości co najmniej do 64 znaków
7) NIE POWINIEN wymagać dodatkowych kryteriów złożoności, np. znaków specjalnych, cyfr czy dużych liter
8) POWINIEN wymuszać zmianę hasła jeśli potwierdzono, bądź zachodzi podejrzenie, że aktualne hasło zostało przejęte lub upublicznione

01 Rekomendacje techniczne CERT Polska dla systemów uwierzytelniania (2)

- hasła jeśli potwierdzono, bądź zachodzi podejrzenie, że aktualne hasło zostało przejęte lub upublicznione

1) POWINIEN podawać dokładny powód w przypadku odrzucenia nowego hasła
2) NIE POWINIEN blokować wykorzystania funkcji “wklej” na polu hasła
3) ZALECA SIĘ wsparcie dla uwierzytelniania dwuskładnikowego
4) ZALECA SIĘ wyświetlanie użytkownikowi wskaźnika szacującego siłę nowego hasła

Źródło: https://cert.pl/posts/2022/01/rekomendacje-techniczne-systemow-uwierzytelniania/

02 RODO nie pozwala na ujawnienie danych hejtera (1)

- przepisy o ochronie danych osobowych nie dają Prezesowi UODO prawa do nakazywania administratorowi strony internetowej ujawnienia danych osobom trzecim, np. w celu wytoczenia powództwa – taka jest konkluzja wyroku WSA w Warszawie (sygn. II SA/Wa 989/20)
- bardzo trudno jest uzyskać dane osobowe pomawiającego kogoś w internecie – na pewno podstawą prawną nie jest RODO, o czym przekonała się spółka, która wystąpiła do Prezesa UODO o nakazanie administratorowi strony internetowej udostępnienia danych osobowych: imienia, nazwiska, adresu IP komputera osoby, która wysłała maila do Wojewódzkiej Stacji Sanitarno-Epidemiologicznej, że skarżąca spółka produkuje szkodliwe produkty kosmetyczne i lecznicze
- Prezes UODO umorzył postępowanie, a swoją decyzję tłumaczył tym, że nie ma uprawnienia do nakazania administratorowi lub podmiotowi przetwarzającemu ujawnienia danych osobowych osobie trzeciej, bo nie ma aktualnie żadnego przepisu, który dawałby mu takie kompetencje
- WSA oddalił skargę i wyjaśnił, że prezes UODO będąc podmiotem publicznym może podejmować wyłącznie takie działania, które znajdują swoje źródło w przepisach obowiązującego prawa – a tak w tym wypadku tak nie jest
- art. 15 RODO przyznaje prawo dostępu do danych osobowych wyłącznie tej osobie, której dane dotyczą

02 RODO nie pozwala na ujawnienie danych hejtera (2)

- jedynym celem RODO jest zagwarantowanie osobie fizycznej odpowiedniej ochrony jej danych osobowych a nie przyznawanie uprawnień informacyjnych innym podmiotom
- WSA tłumaczył, że w szczególności przepisy RODO nie dają uprawnień informacyjnych podmiotom, które zamierzają wytaczać powództwa osobom fizycznym, których dane osobowe objęte są ochroną
- przepisy analizowanej regulacji nie dają takich uprawnień także organowi nadzoru
- Prezes UODO nie może więc żądać od administratora danych osobowych ich ujawnienia osobie trzeciej, na potrzeby ewentualnego postępowania sądowego
- w obecnym stanie prawnym nie ma narzędzia – bez odwołania się do organów państwa – aby zażądać ujawnienia danych innej osoby, np. w związku z naruszeniem dóbr osobistych
- jest to nie problem RODO, ale polskiego państwa, które powinno stworzyć możliwość ochrony naruszonych praw, a tego nie robi, mimo że od lat wie o problemie – tym samym Polska narusza w ten sposób art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, co przesądził ETPCz w sprawie K.U. przeciwko Finlandii - wyrok ETPC z 2 grudnia 2008 r., skarga nr 2872/02, gdzie występował ten sam problem

Źródło: https://www.prawo.pl/biznes/dane-osobowe-rodo-nie-pozwala-na-ujawnienie-danych-hejtera,512901.html

03 EROD: Wytyczne w sprawie prawa dostępu do danych

- Europejska Rada Ochrony Danych, podczas 59. posiedzenia plenarnego, przyjęła Wytyczne w sprawie prawa dostępu do danych oraz pismo w sprawie zgody stosowania plików cookie
- Wytyczne przedstawiają różne aspekty prawa dostępu do danych i dostarczają bardziej precyzyjnych wskazówek co do tego, jak prawo dostępu powinno być realizowane w różnych sytuacjach
- dokument zawiera m.in. wyjaśnienia dotyczące zakresu prawa dostępu, informacji, które administrator musi przekazać osobie, której dane dotyczą, formatu wniosku o dostęp, głównych sposobów zapewnienia dostępu oraz pojęcia żądań ewidentnie nieuzasadnionych lub nadmiernych. Warto zauważyć, że stanowiska i opinie przedstawione podczas spotkania interesariuszy w listopadzie 2019, zostały uwzględnione w trakcie prac nad dokumentem
- EROD przyjęła pismo w odpowiedzi na pisma wzywające do jednolitej interpretacji zgody na stosowanie plików cookie
- w piśmie tym Rada podkreśla, że zależy jej na zapewnieniu zharmonizowanego stosowania zasad ochrony danych w całym Europejskim Obszarze Gospodarczym
- również w tym celu EROD powołała niedawno grupę zadaniową ds. banerów cookie, której rolą jest koordynowanie odpowiedzi na skargi dotyczące banerów cookie

Źródło: https://uodo.gov.pl/pl/138/2260

04 MEiN podaje dane o szczepieniach na uczelniach - pozyskanie prawnie wątpliwe

- środowisko akademickie jest jedną z najlepiej zaszczepionych przeciwko COVID-19 grup w Polsce - wynika z danych publikowanych przez resort edukacji i nauki – problemem może być natomiast to, skąd takie dane w ogóle pozyskano.
- zestawienie opracowano w oparciu o identyfikator, jakim jest numer PESEL - a precyzyjnie, numery PESEL wszystkich osób, których dane znajdują się w bazie POL-on
- tworząc zestawienie, powołano się na art. 342 ust. 4 PWSN – według prawników nie jest on podstawą do stworzenia takiego zestawienia - po pierwsze dla tego, że bazy nie powstały we wskazanych w przepisie celach, po drugie dlatego, że statystyk nie dało się stworzyć bez przetworzenia danych jednostkowych
- zgodnie z RODO podmioty sektora publicznego, w tym organy władzy publicznej powinny zawsze posiadać wyraźnie określony przepisem prawa cel przetwarzania danych osobowych oraz podstawę prawną do jego realizacji – w ich przypadku ani cel przetwarzania, ani jego podstawa nie mogą być określane dowolnie przez te podmioty
- jeśli przedmiotem analizy miałyby być dane o charakterze statystycznym, już na etapie udostępniania drugiemu podmiotowi należałoby zadbać o ich odpowiednie przygotowanie w taki sposób, aby nie było możliwe ustalenie tożsamości osób, których dotyczą
- tylko pod takim warunkiem informacje miałyby cechy danych statystycznych – w tym przypadku, jeżeli faktycznie oparto się na numerach PESEL - tak nie było

Źródło: https://www.prawo.pl/student/baza-danych-pol-on-a-dane-o-szczepieniach-rodo,512915.html

05 Styczniowy newsletter UODO (1)

- w styczniowym numerze newslettera Urzędu Ochrony Danych Osobowych dla IOD znajdziemy między innymi:

OGRANICZENIA W MONITORINGU WIZYJNYM PROWADZONYM PRZEZ GMINĘ

- gmina nie ma podstaw prawnych do prowadzenia monitoringu wizyjnego umożliwiającego dokonywanie pomiarów biometrycznych i identyfikowanie osób fizycznych oraz tablic rejestracyjnych pojazdów

ROLA OFERENTA PODCZAS WYCENY PORTFELA WIERZYTELNOŚCI

- oferent (przyszły cesjonariusz) jest samodzielnym administratorem, przetwarzającym udostępnione mu dane osobowe we własnym imieniu, we własnym interesie i na własne ryzyko

POZYSKIWANIE INFORMACJI O SYTUACJI OSOBY SKIEROWANEJ DO DPS

- dom pomocy społecznej informacje o sytuacji osoby skierowanej do umieszczenia w tej placówce w pierwszej kolejności powinien pozyskiwać, przeprowadzając wizytę domową oraz indywidualną rozmowę z osobą, której dane dotyczą i jej przedstawicielem ustawowym

BĘDZIE WŁAŚCIWA PODSTAWA PRZETWARZANIA DANYCH OSOBOWYCH W PORADNIACH PSYCHOLOGICZNO-PEDAGOGICZNYCH

- zgoda nie będzie już podstawą przetwarzania danych osobowych na potrzeby orzeczeń i opinii wydawanych przez zespoły orzekające działające w publicznych poradniach psychologicznopedagogicznych

05 Styczniowy newsletter UODO (2)

KARY

- Islandia: kara za niedostosowanie rządowej aplikacji do wymogów RODO

MIĘDZYNARODOWE

- Wytyczne w sprawie ochrony osób w związku z przetwarzaniem danych osobowych przez i na potrzeby kampanii politycznych

Źródło: Newsletter UODO dla IOD, archiwum Newslettera https://uodo.gov.pl/p/archiwum-newslettera-dla-iod

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

© Lex Artist Sp. z o.o., 2022