





RODO - aktualności

10 października 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

Mechanizm blokowania stron internetowych

02

Wyciekły dane żołnierzy służących na granicy z Białorusią

03

Szpitaly będą musiały zadbać o cyberbezpieczeństwo

04

Dane przypadkowych osób przechowywane w bazie Europolu

01 Mechanizm blokowania stron internetowych

- jeszcze w tym roku pojawić ma się ustawa, która stworzy mechanizm blokowania stron internetowych - celem jest ochrona małoletnich przed dostępem do pornografii
- póki co nie wiadomo jednak, jakie strony ma obejmować i jak ma wyglądać proces weryfikacji wieku użytkownika strony - za blokady ma być odpowiedzialny dostawca internetu
- wykonywanie obowiązków sprawdzi minister właściwy do spraw informatyzacji – Prezes Urzędu Komunikacji Elektronicznej zobowiązany będzie, na wniosek ministra właściwego do spraw informatyzacji, udzielić odpowiedniego wsparcia w prowadzonych przez ministra czynnościach kontrolnych, oraz do udzielenia ministrowi wszelkich informacji o dostawcach usługi dostępu do internetu koniecznych do wypełnienia obowiązków kontrolnych
- nie wiadomo, jak w szczególności będzie wyglądać proponowane rozwiązanie i czy nie stworzy możliwości do arbitralnego wpisywania stron internetowych na czarną listę oraz jak zostanie rozwiązana kwestia ochrony prywatności użytkownika
- są kraje, w których dostęp do stron pornograficznych wymaga wpisania specjalnego kodu - tak jest w Wielkiej Brytanii, gdzie jego uzyskanie wymaga przesłania zdjęcia i skanu dokumentu tożsamości
- kwestia prywatności rozwiązana jest w ten sposób, że dane o wieku gromadzone są w odrębnej bazie prowadzonej przez niezależny podmiot przydzielający tokeny - przekazuje on dostawcy usługi jedynie potwierdzenie, że osoba dysponująca kodem jest pełnoletnia

Źródło: <https://www.prawo.pl/oswiata/blokowanie-stron-internetowych-dostep-do-pornografii,517712.html>

02

Wyciekły dane żołnierzy służących na granicy z Białorusią

- doszło do wycieku danych kilkudziesięciu żołnierzy WOT, którzy służą na granicy z Białorusią w ramach operacji "Gryf"
- jak informuje Onet, dziennikarze portalu od kilku dni mają szczegółowe dane osobowe 58 żołnierzy Wojsk Obrony Terytorialnej – każda z ujawnionych pozycji zawiera stopień wojskowy, imię i nazwisko wojskowego, imię ojca oraz PESEL
- wyciek dotyczy żołnierzy 62. Batalionu Lekkiej Piechoty (62BLP) w Radomiu, który należy do 6. Mazowieckiej Brygady Obrony Terytorialnej (6MBOT)
- dane zostały umieszczone na publicznym komunikatorze internetowym WhatsApp
- do sprawy odniósł się rzecznik formacji kpt. Witold Sura – "Dowództwo nie komunikuje się w sprawie operacji 'Gryf' z żołnierzami poprzez ogólnodostępne komunikatory. Opisana przez Pana sytuacja nie jest wynikiem błędów systemowych, a jedynie przykładem jednostkowej działalności byłego żołnierza"
- portal twierdzi, że na wojskowej grupie na WhatsApp znajdowało się wielu żołnierzy, którzy wymieniali się tam informacjami dotyczącymi toczącej się na białoruskiej granicy operacji – łącznie 172 osoby
- niezależnie od portalu, dane żołnierzy WOT ma jeszcze co najmniej jeszcze jedna osoba - to reprezentujący ziemię radomską poseł PO Konrad Fryszak, a dane trafiły do jego skrzynki poselskiej

Źródło: https://www.rmfm24.pl/fakty/polska/news-onet-wyciekly-dane-zolnierzy-sluzacych-na-granicy-z-bialorus,nld,6333271#crp_state=1

03

Szpitala będą musiały zadbać o cyberbezpieczeństwo

- system ochrony zdrowia stanie się częścią krajowego systemu cyberbezpieczeństwa, co oznacza nowe obowiązki dla szpitali
- jednym z kontekstów debaty pt. „Bezpieczeństwo placówki i danych medycznych w cyberprzestrzeni” była Europejska Przestrzeń Danych Zdrowia (EHDS), czyli europejska sieć danych medycznych, która ma umożliwić wykorzystywanie danych dotyczących zdrowia w państwach członkowskich UE – system ten ma połączyć środowiska ochrony zdrowia: szpitali, przychodni, pacjentów z systemem innowacyjnym i badawczym
- dyrektor Pionu Eksploatacji i Bezpieczeństwa Systemów Teleinformatycznych w Centrum e-Zdrowia (CeZ) podkreślił, że placówki ochrony zdrowia są separowanymi jednostkami w zakresie cyberbezpieczeństwa – oznacza to, że szpitale budują własne systemy
- szpitali, które mają bardzo słaby stopień bezpieczeństwa jest 3 proc., 63 proc. szpitali wykazuje średni poziom bezpieczeństwa, a 20 proc. dobry lub bardzo dobry
- rozwiązania IT, które pozwalają na gromadzenie danych są już stosowane 97,3 proc. szpitali, i te szpitale zgłaszają gotowość do przetwarzania danych w postaci elektronicznej
- ponad 85 proc. szpitali posiada również stanowiska do tego, by dane te przetwarzać – jednocześnie jednak gotowość wymiany danych medycznych w ramach automatycznego systemu zgłasza jedynie 57,5 proc. szpitali. 57,2 proc. szpitali raportuje zdarzenia medyczne do systemu P1, a udział w wymianie tych danych bierze 30,5 proc.

Źródło: <https://www.prawo.pl/zdrowie/cyberbezpieczenstwo-szpitala-szykuja-sie-do-zmiany-przepisow,517740.html>

04

Dane przypadkowych osób przechowywane w bazie Europolu

- Europejski Inspektor Ochrony Danych wystąpił do Trybunału Sprawiedliwości Unii Europejskiej o stwierdzenie nieważności przepisów legalizujących bazę danych Europolu
- na początku 2023 r. EIOD wydał decyzję, w której nakazał Europolowi usunięcie danych starszych niż sześć miesięcy, o ile nie zostały one poddane kategoryzacji – agencja powinna filtrować napływające od służb poszczególnych państw informacje, odsiewać te, których dalsze przetwarzanie jest uzasadnione, bo da się je powiązać z przestępczością, a pozostałe kasować
- chodzi o zbiór danych o co najmniej 250 tys. osób, które służby poszczególnych państw w jakiś sposób wiązały z działalnością przestępczą – tyle że dotyczą one również osób przypadkowych
- Europol latami utrzymywał tę bazę, uznając, że zgromadzone w niej informacje kiedyś mogą okazać się przydatne
- po tej bezprecedensowej decyzji Parlament Europejski i Rada znowelizowały unijne rozporządzenie. Dodały też dwa przepisy, które legalizują z mocą wsteczną przetwarzanie danych bez stwierdzonego związku z działalnością przestępczą
- mówiąc wprost – nowe regulacje stanowią obejście decyzji EIOD i pozwalają dalej przetwarzać zakwestionowane dane
- zdaniem EIOD nowelizacja unijnego rozporządzenia stwarza niebezpieczny precedens próby niwelowania prawem skutków decyzji organu nadzorczego, jakim jest EIOD

Źródło: <https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/8554758,europol-przestepcy-dane-osobowe.html>

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