
LEX ARTIST

RODO - aktualności

19 kwietnia 2021 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 EROD m.in. o projektach decyzji stwierdzających odpowiedni stopień ochrony w Zjednoczonym Królestwie

02 Niemiecki komisarz ds. ochrony danych vs Whatsapp

03 Unia Europejska ureguluje zagadnienie dotyczące sztucznej inteligencji (AI)

04 Odciski palców na nowym dowodzie osobistym

05 Trwają prace nad przepisami o pracy zdalnej.. i końca nie widać

06 Prezes UODO – Media społecznościowe a bezpieczeństwo danych

01 EROD m.in. o projektach decyzji stwierdzających odpowiedni stopień ochrony w Zjednoczonym Królestwie

- 13 kwietnia 2021 r., podczas 48. posiedzenia plenarnego, Europejska Rada Ochrony Danych (EROD) przyjęła dwie opinie w sprawie projektów decyzji stwierdzających odpowiedni stopień ochrony w Zjednoczonym Królestwie
- pierwsza z nich (Opinia 14/2021) opiera się na przepisach RODO i ocenia zarówno ogólne aspekty ochrony danych, jak i rządowy dostęp do danych osobowych przekazywanych z EOG w celach egzekwowania prawa i bezpieczeństwa narodowego, uwzględnionych w projekcie decyzji stwierdzającej odpowiedni stopień ochrony. Ocena ta odnosi się do dokumentu Grupy Roboczej Art. 29 dotyczącego odpowiedniego stopnia ochrony przekazywanych danych osobowych
- z kolei druga opinia (Opinia 15/2021), oparta na dyrektywie 2016/680 („dyrektywie policyjnej"), analizuje projekt decyzji stwierdzającej odpowiedni stopień ochrony w świetle Zaleceń 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy 2016/680, jak również odpowiedniego orzecznictwa odzwierciedlonego w Zaleceniach 02/2020 w sprawie niezbędnych gwarancji europejskich dla środków nadzoru
- EROD zwróciła uwagę, że istnieją kluczowe obszary zbieżności między ramami ochrony danych UE i Zjednoczonego Królestwa w zakresie określonych podstawowych przepisów, dotyczących m.in.: podstawy dla zgodnego z prawem i rzetelnego przetwarzania danych osobowych dla prawnie uzasadnionych celów, ograniczenia celu, jakości i proporcjonalności danych, zatrzymywania danych, bezpieczeństwa i poufności czy przejrzystości. Jednak w swoich opiniach Rada wskazała także pewne kwestie, które Komisja Europejska powinna poddać dalszej ocenie lub ściśle monitorować

Źródło: https://uodo.gov.pl/pl/138/1998

02 Niemiecki komisarz ds. ochrony danych vs Whatsapp

- niemiecki komisarz ds. ochrony danych osobowych w Hamburgu chce przeciwdziałać przekazywaniu danych użytkowników Whatsapp Facebookowi i innym podmiotom trzecim
- Whatsapp to jeden z popularniejszych komunikatorów w Europie, który zmienia politykę prywatności. Nowa polityka prywatności wejdzie w życie 15 maja 2021 r.
- polityka ta spotkała się z falą krytyki – chodzi przede wszystkim zapis mówiący o możliwości przesyłania danych (np. numerów telefonów) do Facebooka oraz innych firm. Na skutek tego wielu użytkowników podjęło decyzję o przeniesieniu się do produktów konkurencji, np. Telegrama czy Signala
- komisarz stwierdził, że istnieją powody, by sądzić, że przepisy mówiące o rozszerzeniu udostępniania danych między komunikatorem a Facebookiem, będą „bezprawnie egzekwowane ze względu na brak dobrowolnej i świadomej zgody" użytkowników
- kontrowersyjne zmiany polityki prywatności WhatsAppa wywołały reakcję regulatorów innych państw. Jednym z nich jest włoski urząd ochrony danych osobowych, który zaangażował w sprawię także Europejską Radę Ochrony Danych (EROD). Sprawę monitoruje także Prezes UODO w ramach współpracy międzynarodowej, czekając na wytyczne EROD w tej sprawie

Źródło: https://cyberdefence24.pl/niemcy-reaguja-na-zmiane-polityki-whatsappa

03 Unia Europejska ureguluje zagadnienie dotyczące sztucznej inteligencji (AI)

- użycie sztucznej inteligencji dla systemów inwigilacji staje się coraz bardziej popularne, czego przykładem są Chiny, które na masową skalę korzystają z systemów monitoringu z funkcją rozpoznawania twarzy czy budowy systemu oceny społecznej (np. poprzez śledzenie zachowań użytkowników różnego rodzaju portali i wpływaniu na decyzje tych osób), co na pewno narusza prawo do prywatności
- by przeciwdziałać tego typu praktykom, Komisja Europejska ma zamiar wprowadzić regulacje w zakresie stosowania sztucznej inteligencji (AI), zakazując między innymi zaawansowanego monitoringu z rozpoznawaniem twarzy czy tworzenia systemów oceny społecznej. Mówi się także o zakazie użycia sztucznej inteligencji przy ocenie zdolności kredytowej
- takie rozwiązanie z pewnością spowoduje napięcie między Unią Europejską i amerykańskimi gigantami technologicznymi takimi jak Facebook, Google czy Microsoft i innymi firmami, które gromadzą ogromne ilości danych, zasilających zasoby sztucznej inteligencji
- informacje o projekcie podał portal Politico, z dokumentu wynika zakaz korzystania z systemów AI „wysokiego ryzyka", jeśli nie spełniają określonych kryteriów. Przewiduje się także wysokie kary za nie spełnianie tych wymogów (20 mln € lub do 4% światowego obrotu)

Źródło: https://ithardware.pl/aktualnosci/ue_wyda_regulacje_dotyczace_sztucznej_inteligencji_zakaz_monitoringu_ai_i_systemow_oceny_spolecznej-15789.html

04 Odciski palców na nowym dowodzie osobistym

- w sierpniu 2021 roku pojawią się nowe dowody osobiste (nowa warstwa graficzna i elektroniczna)
- jest to zmiana będąca implementacją rozporządzenia Parlamentu Europejskiego i Rady UE 2019/1157 z 20 czerwca 2019 r. w sprawie poprawy zabezpieczeń dowodów osobistych
- dowody będą zawierały odciski palców (dwa) oraz podpis posiadacza, które wnioskodawca będzie musiał złożyć osobiście w urzędzie. Zniknie zatem możliwość składania elektronicznego wniosku o nowy dowód osobisty. Wyjątkiem będą tu osoby poniżej 12 roku życia, dla których taka możliwość zostanie utrzymana. Odciski palców również nie będą pobierane od tych osób
- w nowym dowodzie będzie też kilka innych, dostrzegalnych na pierwszy rzut oka zmian – pojawi się m.in. oznaczenie państwa członkowskiego (na tle flagi Unii Europejskiej)
- zmiany mają głownie na celu ograniczenie ryzyka fałszowania dokumentów oraz przestępstw przeciwko wiarygodności dokumentów

Źródło: *https://www.gov.pl/web/cyfryzacja/nowe-dowody--jakie-zmiany*

05 Trwają prace nad przepisami o pracy zdalnej.. i końca nie widać

- od wielu miesięcy trwają prace, które mają przenieść regulacje dotyczące pracy zdalnej do Kodeksu pracy. Przyczyną tego jest oczywiście towarzysząca nam pandemia
- dziś pracodawcy wysyłają Pracowników na pracę zdalną na podstawie art. 3 ustawy z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, który obowiązuje w czasie stanu zagrożenia epidemicznego albo stanu epidemii, ogłoszonego z powodu COVID-19, oraz w okresie 3 miesięcy po ich odwołaniu
- obecnie trudno przewidzieć ile jeszcze potrwają wspólne ustalenia Ministerstwa Rozwoju, Pracy i Technologii, partnerów związkowych i pracodawców, choć regulacja wydaje się potrzebna i konieczna
- Główne założenia projektu to:

- praca zdalna będzie mogła być wykonywana całkowicie lub częściowo w miejscu zamieszkania pracownika lub w innym miejscu ustalonym przez pracownika i pracodawcę. Pracodawca będzie zobligowany dostarczyć sprzęt oraz pokryć koszty m.in. prądu i dostępu do Internetu.

Źródło: *https://www.prawo.pl/kadry/na-jakim-etapie-sa-prace-nad-przeniesieniem-przepisow-o-pracy,507729.html*

06 Prezes UODO – Media społecznościowe a bezpieczeństwo danych

- Prezes UODO zwrócił uwagę na bezpieczeństwo danych przetwarzanych w mediach społecznościowych. Troska Prezesa jest z pewnością spowodowana ostatnimi głośnymi sprawami, dotyczącymi „wycieków" danych osobowych z Facebooka czy Linkedina
- w przekazanej wiadomości zwrócono uwagę, by korzystając z serwisów społecznościowych zabezpieczać swoje dane poprzez:

- stosowanie silnego hasła,

- stosowanie dwuetapowego logowanie (login i hasło, następnie korzystanie z zewnętrznych tokenów),

- nie logowanie się na nieznanych urządzeniach,

- nie korzystanie z niezabezpieczonych publicznych hot-spotów,

- stosowanie różne haseł do różnych portali, korzystanie z managerów haseł,

- ograniczanie uprawnienia aplikacji do logowania za pomocą konta w portalu społecznościowym,

- W publikacji wskazano także co zrobić gdy do naruszenia dojdzie

Źródło: https://uodo.gov.pl/pl/138/1996