
LEX ARTIST

RODO - aktualności

[10.04.2024]

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 Z ZUS wyciekły dane prawie 300 płatników

02 62% Polaków obawia się o bezpieczeństwo danych bardziej niż przed RODO

03 Włochy: czerwone światło dla biometrycznej kryptowaluty

04 Wyciek danych klientów znanego e-sklepu (DeeZee)

05 Zadośćuczynienie za niechciany spam pożyczkowy (wyrok)

01 Z ZUS wyciekły dane prawie 300 płatników

- Z ZUS wyciekły dane ok. 300 osób fizycznych w postaci imion, nazwisk, dat i miejsc urodzenia, adresu zamieszkania, numeru PESEL, numeru dowodu osobistego oraz numeru rachunku bankowego.
- Za wyciek odpowiada pracownik ZUS będący członkiem jednego ze związków zawodowych działających w Zakładzie, który drogą mailową wysłał je na prywatny adres mailowy wiceprzewodniczącego związku zawodowego, który już nie jest pracownikiem ZUS (a wcześniej, gdy pracował jeszcze w ZUS, był przewodniczącym związku na poziomie zakładowym).
- Fakt, że doszło do takiej sytuacji potwierdził serwisowi Prawo.pl Paweł Żebrowski, rzecznik prasowy ZUS. - System bezpieczeństwa w Zakładzie Ubezpieczeń Społecznych wykrył incydent związany z naruszeniem danych osobowych przez pracownika. Sprawa została zgłoszona m.in. do Prezesa Urzędu Ochrony Danych Osobowych. ZUS złożył również zawiadomienia do prokuratury. Zgodnie z przepisami Zakład poinformuje o incydencie osoby, których ta sprawa dotyczy. Wobec pracownika ZUS zostały wyciągnięte konsekwencje służbowe.
- Jak podkreśla jeden z ekspertów, w tego rodzaju sytuacjach odróżnia się, czy w posiadanie danych osoba weszła przy pełnieniu funkcji związkowej, czy przy okazji wykonywania pracy. Zgodnie bowiem z art. 28 ustawy o związkach zawodowych związki mogą żądać informacji niezbędnej do działalności związkowej. Ta informacja nie spełnia tego wymogu, ponieważ to jest informacja poufna dotycząca klientów ZUS.
- Wyciek będzie poddany zbadaniu. UODO może, ale nie musi nałożyć na ZUS karę finansową w związku z ewentualnym naruszeniem przepisów. Nawet wtedy, gdy doszło do tego nieświadomie, co nie jest okolicznością łagodzącą. Osoby, których dotyczy wyciek danych, powinny zweryfikować informacje otrzymane z ZUS-u i ewentualnie podjąć środki zaradcze, w tym związane z zastrzeżeniem numeru PESEL, gdyż może to grozić jego wykorzystaniem.

Źródło: Wyciek danych ZUS (prawo.pl); Wyciek danych z ZUS-u. Imiona, nazwiska, numery PESEL i adresy - Geekweek w INTERIA.PL

02 62% Polaków obawia się o bezpieczeństwo danych bardziej niż przed RODO

- Z raportu KPMG pt. „European Privacy Market Research 2023” wynika, że 62% polskich respondentów obecnie obawia się o bezpieczeństwo swoich danych osobowych bardziej niż pięć lat temu, a obawy te są nieco większe niż w pozostałych europejskich krajach (59%), zaś 60% respondentów z Polski uważa, że ochrona prywatności ich danych w kraju nie jest nadmierna, podczas gdy przeciętnie w Europie takie zdanie ma 48% społeczeństwa.
- W publikacji KPMG zebrano opinie mieszkańców osiemnastu krajów UE, w tym Polski.
- Niepokój wywołują m.in. algorytmy uczące się preferencji osób przeglądających treści w serwisach społecznościowych. Takie mechanizmy budzą obawy u 59% ankietowanych z Polski i 66% z Europy. Dodatkowo, treści typu deepfake zostały uznane za niepokojące przez 76% badanych Polaków oraz przez 80% pozostałych Europejczyków. Ponadto, 71% respondentów badania KPMG czuje dyskomfort związany z podsłuchiwaniem przez asystentów głosowych, podano.
- Raport wskazuje też, że w opinii respondentów z UE właściwe przetwarzanie danych osobowych powinno być głównie zadaniem banków (23%), instytucji państwowych (19%) oraz policji i sądów (19%). Jednak 13% respondentów wykazuje, że obdarza instytucje państwowe największym zaufaniem w tym zakresie. Europejczycy wykazują największe zaufanie do banków oraz policji i sądownictwa (po 24% wskazań). Dostawcy usług opieki zdrowotnej zostali wymienieni przez 15% respondentów jako godni zaufania, podczas gdy sprzedawcy detaliczni (2%) i media społecznościowe (3%) zajmują najniższe pozycje w rankingu.
- Według KPMG niewiele ponad połowa uczestników badania KPMG twierdzi, że zachowuje ostrożność przy wprowadzaniu danych do chatbotów, takich jak ChatGPT, z obawy, że ich dane mogą być przechowywane i wykorzystywane do nieznanych celów. 80% respondentów obawia się dyskryminacji i nadużywania danych osobowych przez AI.

Źródło: 62% Polaków obawia się o bezpieczeństwo danych bardziej niż przed RODO – Inwestycje.pl

03 Włochy: Czerwone światło dla biometrycznej kryptowaluty

- Włoski organ ochrony danych osobowych (Garante) skierował do Fundacji Worldcoin ostrzeżenie, że jej projekt obejmujący weryfikację tożsamości użytkowników na podstawie skanowania tęczówki oka najprawdopodobniej narusza RODO.
- Włoski urząd zajął się sprawą, mimo że kryptowaluta przydzielana uczestnikom programu w zamian za ich dane biometryczne nie jest jeszcze w tym kraju oficjalnie dostępna. „Obywatele Włoch mogą już pobrać aplikację World App ze sklepów z aplikacjami, podać swoje dane osobowe i zarezerwować bezpłatne tokeny WLD" – uzasadnia organ ochrony danych.
- Kryptowaluta worldcoin (WLD) została stworzona przez start-up technologiczny Tools for Humanity, którego współzałożycielem jest Sam Altman, dyrektor generalny OpenAI (spółki stojącej za ChatGPT). Projekt obejmuje narzędzie do skanowania tęczówek Orb, elektroniczną tożsamość World ID oraz aplikację World App. Całością zarządza Fundacja Worldcoin, która na swojej stronie internetowej zapewnia o pełnej zgodności z RODO, która zapewnia, że dane użytkowników zbierane są tylko za ich zgodą.
- Garante uważa jednak, że przetwarzanie danych biometrycznych w oparciu o zgodę uczestników projektu wydaną na podstawie niewystarczających informacji nie może być uznane za ważną podstawę prawną – stosownie do wymogów RODO.
- Pod koniec marca także portugalski organ (CNPD) nakazał tymczasowo projektowi Worldcoin zaprzestanie gromadzenia danych biometrycznych na 90 dni. Na początku marca podobny zakaz wydał organ w Hiszpanii.

Źródło: Czerwone światło dla biometrycznej kryptowaluty - GazetaPrawna.pl

04 Wyciek danych klientów znanego e-sklepu (DeeZee)

- Sklep internetowy DeeZee poinformował klientów o wycieku danych. Zaleca im zmianę hasła do swojego konta oraz zachowanie ostrożności w przypadku podejrzanych wiadomości.
- Do wycieku miało dojść w połowie marca. AtomStore, platforma e-commerce współpracująca z DeeZee, poinformowała o możliwym wycieku adresów mailowych, hash haseł (zakodowanych, zabezpieczonych haseł) oraz informacji o ilości i wartości zamówień. Sklep twierdzi, że baza objęta atakiem nie zawierała danych adresowych.
- Sklep internetowy DeeZee poinformował o natychmiastowo podjętych krokach: zablokowaniu dostępu osobom trzecim do sklepie, zabezpieczeniu infrastruktury IT, zgłoszeniu incydentu do odpowiednich organów, w tym Urzędu Ochrony Danych Osobowych, wszczęciu wewnętrznej procedury ws. naruszenia danych, przeprowadzeniu audytu zabezpieczeń danych osobowych.
- Atak hakerski na sklep DeeZee to kolejny alarmujący incydent, który podkreśla znaczenie bezpieczeństwa danych osobowych w świecie internetowym. Apel o zmianę haseł stanowi ważne ostrzeżenie dla klientów, aby podjąć środki ostrożnościowe w celu ochrony swoich danych.

Źródło: Wyciek danych klientów e-sklepu DeeZee. Lepiej zmienić hasło - rp.pl

05 Zadośćuczynienie za niechciany spam pożyczkowy (nieprawomocny wyrok)

- Powód otrzymywał od pozwanego na swój adres e-mail niechcianą korespondencję mailową w łącznej liczbie 41 w okresie od 6 lutego 2020 r. do dnia 15 lutego 2020 r. Korespondencja ta dotyczyła możliwości uzyskania pożyczki czy kredytu tzw. informacje handlowe dotyczące marketingu i reklamy. Korespondencja przychodziła do powoda o różnych porach dnia, nierzadko kilka razy dziennie. Głównie poranne godziny przesyłanych maili były dotkliwe dla powoda, ponieważ wybudzały go one ze snu.
- Pozwany podniósł, iż wszedł legalnie w posiadanie adresu e-mail powoda od innego podmiotu, który z kolei otrzymał zgodę na jego wykorzystanie przez powoda. Zdaniem pozwanego powód miał możliwość zapoznania się z klauzulą informacyjną zamieszczoną na stronie internetowej pozwanego, gdzie opisane są cele przetwarzania danych osobowych, czas ich przetwarzania, dane kontaktowe pozwanej spółki oraz uprawnienia osób których dane osobowe są przetwarzane. Z uprawnień tych powód skorzystał i wiadomości mailowe nie zostały do niego wysyłane.
- Jak stwierdził SO w Warszawie, powód nigdy nie współpracował z pozwaną spółką i nie udzielał jej zgody na przetwarzanie swoich danych osobowych. Z zebranego w sprawie materiału dowodowego wynika, że pozwany dysponował adresem e-mail powoda, na który przesyłał treści reklamowe i marketingowe, bez zgody powoda.
- Pozwany próbował się bronić i wskazał, że nie mają zastosowania przepisy prawa telekomunikacyjnego ponieważ pomiędzy stronami nie doszło do żadnej rozmowy telefonicznej, a spółka nie prowadziła żadnych działań telemarketingowych w stosunku do powoda.
- Sąd jednak wskazał, że naruszone zostało prawo telekomunikacyjne, UŚUDE i RODO, niewątpliwie doszło do naruszenia dóbr osobistych i przyznał powodowi 2 tyś. zł za otrzymanie niechcianego spamu dot. pożyczek i kredytów.

Źródło: Zadośćuczynienie za niechciany spam pożyczkowy (wyrok) | LinkedIn