
LEX ARTIST

RODO - aktualności

24 sierpnia 2020 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 Czy pracodawca może korzystać z prywatnych danych kontaktowych do pracownika?

- Pracodawca, który dysponuje danymi kontaktowymi do pracownika pozyskanymi podczas rekrutacji, takimi jak np. adres prywatnej poczty elektronicznej czy numer prywatnego telefonu komórkowego, nie może ich wykorzystywać do kontaktów zawodowych z pracownikiem bez jego zgody.
- Kodeks pracy nie wskazuje zatem prywatnego adresu poczty elektronicznej i numeru prywatnego telefonu jako danych, których pracodawca ma prawo żądać od pracownika. W polskim systemie prawnym nie istnieje też żaden przepis, który zobowiązywałby osobę fizyczną do posiadania takich środków komunikacji. Dysponowanie adresem poczty elektronicznej i telefonem jest i powinno pozostać dobrowolne.
- Warto bowiem pamiętać, że zazwyczaj podczas rekrutacji, pozyskując dane, o których mowa w art. 221 § 1 Kodeksu pracy, a więc m.in. dane kontaktowe wskazane przez osobę ubiegającą się o zatrudnienie, pracodawca, spełniając obowiązek informacyjny deklaruje, że będzie je przetwarzał jedynie na potrzeby przeprowadzenia naboru. Zatem na ten nowy cel przetwarzania danych pracownika, jakim jest kontaktowanie się z nim w celach służbowych, musi pozyskać zgodę zatrudnionego.

Źródło: https://uodo.gov.pl/pl/138/1636

02 Smart TV narzędziem inwigilacji?

- Nowoczesne telewizory zbierają dane głosowe oraz materiały wideo, które mogą stać się elementem kampanii cyberszpiegowskich. W przypadku złośliwych działań wbudowane mikrofony oraz kamery stanowią zagrożenie dla prywatności użytkowników i ich otoczenia. Ryzyko związane z inwigilacją za pomocą „Smart TV" jest takie samo, jak w przypadku telefonów lub innych inteligentnych urządzeń.
- nowoczesne telewizory mogą „w sposób ciągły" zbierać dane na temat użytkowników i ich otoczenia. Mowa tu przede wszystkim o nagrywaniu dźwięków oraz materiałów wideo.
- Większość producentów inteligentnych telewizorów monitoruje bezpieczeństwo swoich produktów, lecz nie da się w pełni uniknąć zagrożenia, jakie występuje w sieci. „Smart TV może stać się celem cyberataku tak samo, jak komputer lub inne urządzenie" – podsumował Arseniy Shcheltsin w rozmowie z agencją Prime.

Źródło: https://cyberdefence24.pl/smart-tv-narzedziem-inwigilacji

03 Umowy z przedszkolem - jakich danych nie trzeba podawać

- Do UODO docierają pytania rodziców dotyczące zakresu pozyskiwanych danych w ramach umów o świadczenie usług przedszkolnych zarówno przez podmioty publiczne jak i niepubliczne. Zainteresowani sygnalizują zbieranie nie tylko danych koniecznych do zawarcia umowy jak imię i nazwisko rodziców dziecka, adres ich zamieszkania, ale i takich danych jak: numer PESEL rodziców, miejsce zatrudnienia rodziców, informacje o stanie zdrowia dziecka.
- ważne jest odpowiednie informowanie rodziców i uczniów o tym, kto jest ich administratorem danych, na jakiej podstawie dane są przetwarzane, w jakim celu i przez jaki okres.
- zgodnie z § 41 ust. 1 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach, o każdym wypadku zawiadamia się niezwłocznie m.in. rodziców (opiekunów) poszkodowanego. Dla wypełnienia powyższego obowiązku, przetwarzanie informacji o miejscu pracy rodzica może być niezbędne, w przypadku braku możliwości innej formy kontaktu z rodzicem.
- Niedopuszczalne jest przetwarzanie danych osobowych dzieci i rodziców dotyczących ich zdrowia, które nie wynikają wprost w przepisów prawa, chyba że rodzic bądź opiekun wyraził na to świadomą, dobrowolną i możliwą do wycofania zgodę. Przedszkole nie może pozyskiwać wyżej wymienionych danych, ponieważ nie są one warunkiem koniecznym przy rekrutacji

Źródło: https://uodo.gov.pl/pl/138/1637

04 Kary w Belgii i Hiszpani

- Belgijski organ ochrony danych nałożył grzywnę w wysokości 20 000 EUR na operatora telekomunikacyjnego Proximus za kilka naruszeń ochrony danych podczas przetwarzania danych osobowych w celu publikowania publicznych książek telefonicznych.
- Obywatel belgijski (powód) zwrócił się do Proximus, wydawcy publicznej książki telefonicznej, o wycofanie publikacji jego danych osobowych w publicznym katalogu Proximus, jak również o opublikowaniu danych osobowych w spisie innych wydawców. Proximus, jako wydawca własnego publicznego katalogu, potwierdził wobec powoda, że nie będzie już publikować danych osobowych, a także poinformuje innych wydawców o publicznym spisie numerów, aby nie publikowali danych osobowych powoda. Jednak kilka miesięcy później powód odkrył, że jego dane osobowe zostały opublikowane nie tylko w katalogu Proximus, ale także w innych wydawnictwach publicznej książki telefonicznej.
- Proximus nie wywiązał się (odpowiednio) ze swoich obowiązków jako administratora, w związku z czym naruszył art. 6 RODO w związku z art. 7 RODO oraz art. 24 i art. 5 ust. 2 RODO.
- Proximus nie udzielił osobie, której dane dotyczą, przejrzystych informacji w trakcie i po rozpatrzeniu jej żądania, ani nie ułatwił odpowiednio realizacji praw osoby, której dane dotyczą, w związku z czym naruszył art. 12 i 13 RODO.

Źródło: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu20000-fine-proximus-several-data-protection_en

04 Kary w Belgii i Hiszpani

- Hiszpański Urząd Ochrony Danych (AEPD) nałożył grzywnę w wysokości 75 000 EUR na VODAFONE ESPA.000A za przetwarzanie numeru telefonu wnioskodawcy w celach marketingowych po skorzystaniu przez niego z prawa do usunięcia w 2015 r., Pomimo tego, że osoba, której dane dotyczą, otrzymała SMS reklamowy. Kontroler stwierdził, że numer powoda, który był łatwy do zapamiętania, był używany przez jego pracowników jako „fikcyjny numer".
- AEPD uznał, że VODAFONE ESPAÑA naruszył art. 6 ust. 1 RODO, przetwarzając dane osobowe powoda bez podstawy prawnej.

Źródło: https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-75000-eur-vodafone_en

04 Kary w Belgii i Hiszpani

- Hiszpański Urząd Ochrony Danych (AEPD) nałożył grzywnę w wysokości 70 000 EUR na XFERA MOVILES za ujawnienie danych osobowych klienta stronie trzeciej.
- Powód został poinformowany przez innego klienta Masmovil, że z powodu błędu firmy został obciążony rachunkiem powoda, a tym samym miał dostęp do swoich danych osobowych (imię, nazwisko, numer dowodu osobistego i osobisty numer telefonu).
- AEPD uznał, że stanowi to naruszenie zasady poufności, określonej w art. 5 ust. 1 lit. f) RODO.

Źródło: https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-70000-eur-xfera-moviles_en

- Hiszpański Urząd Ochrony Danych (AEPD) nałożył na firmę grzywnę w wysokości 1.200 EUR za telefonowanie do osoby, której dane dotyczą, oferując jej ofertę dotyczącą hoteli, gdy były one objęte systemem wykluczania reklam.

Źródło: https://edpb.europa.eu/news/national-news/2020/spanish-data-protection-authority-aepd-imposes-fine-company-not-complying_en

05 Miliony użytkowników Instagrama, TikToka i YouTube'a poszkodowanych w wycieku danych

- Dane 235 mln użytkowników Instagrama, TikToka i YouTube'a wyciekły do sieci. Informacje znajdujące się w niezabezpieczonej bazie danych znaleźli specjaliści firmy Comparitech.
- Na podstawie analizy próbek odnalezionych w sieci danych Comparitech stwierdził, że jeden na pięć rekordów zawierał dane takie, jak numer telefonu i adres e-mail pokrzywdzonych w wyniku wycieku osób. Oprócz tego wszystkie rekordy składały się z informacji dotyczących imienia i nazwiska, nazwy profilu, zdjęcia profilowego, a także opisu konta użytkowników. Rekordy zawierały także dane o liczbie osób obserwujących dane konto, zaangażowaniu generowanym przez umieszczane na nim treści, a także tempie wzrostu popularności profilu. W bazie danych można było znaleźć również informacje na temat płci i wieku osób śledzących poszczególne profile oraz ich lokalizacji.
- Przedstawiciel firmy Comparitech Paul Bischoff ocenia, że dane tego typu stanowią największą wartość dla cyberprzestępców, którzy działają z użyciem techniki phishingu. Szczególną wartość ujawnionej bazie danych nadaje fakt, że informacje w niej zawarte są posegregowane w ramach wyróżnionych wcześniej kategorii, co sprawia, że są bardzo łatwe w użyciu dla botów, którymi posługują się hakerzy np. podczas rozsyłania SPAM-u.

Źródło: https://cyberdefence24.pl/miliony-uzytkownikow-instagrama-tiktoka-i-youtubea-poszkodowanych-w-wycieku-danych

06 Ochrona danych osobowych: Kolejne branże chcą się samoregulować

- Osiem kodeksów postępowania ws. ochrony danych osobowych czeka na zatwierdzenie prezesa Urzędu Ochrony Danych Osobowych. Kolejne branże pracują nad własnymi.
- Jak informuje UODO, wnioski o zatwierdzenie kodeksów dobrych praktyk złożyło do niego osiem organizacji branżowych: Porozumienie Zielonogórskie (ochrona zdrowia), Związek Banków Polskich, Federacja Polskich Szpitali, Związek Rewizyjny Spółdzielni Mieszkaniowych, Krajowa Izba Doradców Podatkowych, Związek Pracodawców Organizacja Firm Badania Opinii i Rynku, Polska Rada Centrów Handlowych oraz Stowarzyszenie Bibliotekarzy Polskich.

Źródło: https://biznes.gazetaprawna.pl/artykuly/1488700,dane-osobowe-rodo-zasady-w-branzach.html

07 Czy największa nałożona kara za naruszenie RODO była słuszna? Sąd oceni, czy zabezpieczenia Morele.net były wystarczające

- Sprawa sięga jesieni 2018 r., kiedy to klienci sklepów Grupy Morele.net zaczęli otrzymywać SMS-y wskazujące na konieczność dopłaty jednego złotego. Link z wiadomości prowadził do podstawionej bramki płatności elektronicznej, za pośrednictwem której oszust mógł zdobyć login i hasło do konta w banku i w ten sposób uzyskać dostęp do środków znajdujących się na rachunku.
- Zaraz po wykryciu kradzieży danych ze swej bazy Grupa Morele.net zgłosiła incydent Urzędowi Ochrony Danych Osobowych. Ten zaś wszczął kontrolę. W sumie chodziło o dane ponad 2,2 mln klientów: imię, nazwisko, adres poczty elektronicznej (e-mail), numer telefonu i adres do doręczeń.
- Zdaniem UODO Morele.net, przetwarzając dane osobowe ponad 2,2 mln klientów, czyli na dużą skalę, a także zważywszy zakres tych danych, powinna skuteczniej monitorować potencjalne zagrożenia. Zdaniem kontrolerów ukarana spółka jedynie częściowo wywiązywała się z tego obowiązku. Nie oceniała, czy środki techniczne i organizacyjne są adekwatne do istniejącego ryzyka. O tym, że były niewystarczające, świadczy zaś fakt, że doszło do wykradzenia bazy danych.
- Ogłoszenie orzeczenia WSA w Warszawie w tej sprawie (sygn. Akt II SA/Wa 2559/19) zostało odroczone do 3 września 2020 r.

Źródło: https://prawo.gazetaprawna.pl/artykuly/1488771,wyciek-danych-osobowych-oszust-kradziez-morele-net-rodo-zabezpieczenia.html

08 Co zrobić z zebranymi już zgodami na marketing i informacje handlowe

- Projekty prawa komunikacji elektronicznej (dalej: p.k.e.) oraz ustawy wprowadzającej p.k.e., które znajdują się w konsultacjach publicznych, m.in. porządkują kwestię uzyskiwania zgód na niezamówione informacje handlowe oraz marketing bezpośredni. Obie zgody, dziś ujęte w różnych przepisach, w przyszłości mają być uregulowane w jednym artykule – 360 p.k.e.
- Projekt p.k.e. łączy bowiem obowiązujący obecnie – szalenie kontrowersyjny – art. 172 ustawy z 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r. poz. 2460, ost. zm. Dz.U. z 2020 r. poz. 695) z art. 10 u.ś.u.d.e. – Do dziś nikt nie jest jednak do końca pewien, kiedy trzeba zebrać jedną zgodę, a kiedy drugą. Doktryna też tego nie rozstrzyga. Po zmianach ma być już tylko jedna zgoda, która – o ile spełni odpowiednie warunki – będzie tożsama w zakresie sposobu jej uzyskiwania z tą zgodą, którą znamy z RODO – wyjaśnia Piotr Liwszic.
- Jego zdaniem jedna zgoda z p.k.e. może obejmować wszelkie sposoby komunikacji elektronicznej z użytkownikami, a zatem także telefony, wiadomości SMS lub MMS oraz – coraz modniejsze – powiadomienia push z aplikacji na smartfony.

Źródło: https://prawo.gazetaprawna.pl/artykuly/1488596,rodo-zgoda-na-marketing-informcje-handlowe.html

09 UODO: Zgoda nie zawsze jest podstawą przetwarzania danych

- Zgoda może być podstawą przetwarzania danych tylko wtedy, gdy nie występują inne przesłanki legalizujące. Gdy jednak zgoda ma zastosowanie, to musi spełniać określone warunki, by rzeczywiście była podstawą przetwarzania.
- Wiele osób jest przekonanych, że jeśli nie wyraziło zgody na przetwarzanie swoich danych osobowych, to nie można tego robić. W praktyce jednak zgoda może być podstawą do przetwarzania naszych danych, gdy nie występują inne przesłanki legalizujące, które są określone w art. 6 ust. 1 RODO.
- Dopiero gdy nie mają zastosowania powyższe przesłanki, to podstawą do przetwarzania danych osobowych może być zgoda. Należy jednak pamiętać, że niedopuszczalne jest odbieranie zgody na przetwarzanie naszych danych osobowych w przypadku istnienia innej przesłanki legalizacyjnej upoważniającej administratora do przetwarzania danych osobowych w tym samym zakresie i celu.
- Szczególną czujnością kierujmy się, gdy mamy do czynienia z działaniami marketingowymi. O ile zgoda na marketing bezpośredni nie jest wymagana, o tyle sytuacja się zmienia, gdy taka forma komunikacji jest realizowana telefonicznie. Prawo telekomunikacyjne w art. 172 zakazuje wykonywania połączeń do celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na nie zgodę.

Źródło: https://uodo.gov.pl/pl/138/1638