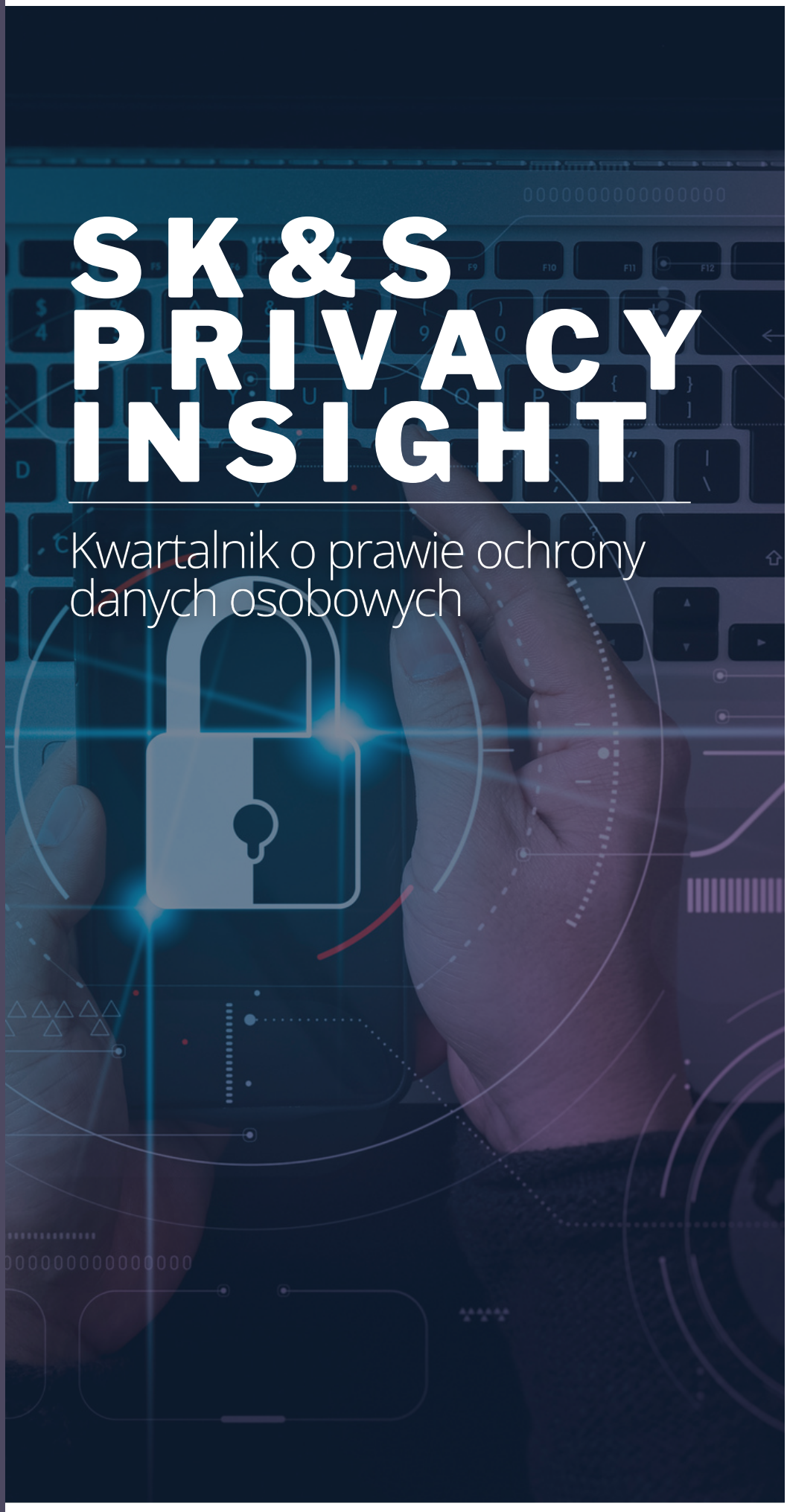


SK&S PRIVACY INSIGHT

Kwartalnik o prawie ochrony danych osobowych

SOŁTYSIŃSKI KAWECKI SZLĘZAK

W tym numerze

CZERWIEC 2023 | NUMER 4

Aktualizacja zasad przetwarzania danych osobowych w toku badania klinicznego

Katarzyna Wnuk
Prawnik, adwokat
katarzyna.wnuk@skslegal.pl
+48 602 151 178

W połowie kwietnia weszła w życie ustawa o badaniach klinicznych produktów leczniczych stosowanych u ludzi (dalej: „Ustawa"). Więcej informacji o ustawie pod kątem wymogów regulacyjnych znajduje się w podsumowaniu mec. Myszko oraz mec. Jakubiak dostępnym **tutaj**.

Poza zmianami regulacyjnymi, ustawa wprowadza zmiany w zakresie przetwarzania danych osobowych w toku badania klinicznego. Poniżej przedstawiamy najistotniejsze zmiany, o których należy pamiętać podczas zapewniania zgodności badania klinicznego z RODO. Oczywiście poza specyficznymi dla badań klinicznych przepisami dot. ochrony danych osobowych, wciąż należy stosować RODO i wynikające z niego obowiązki.

Czy w toku badań klinicznych trzeba realizować żądania osób, których dane dotyczą?

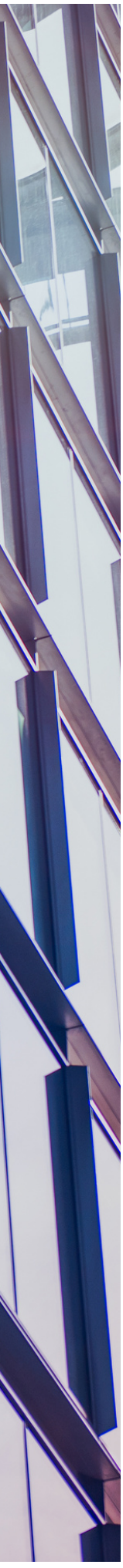
Zgodnie z RODO, osoby których dane są przetwarzane mogą realizować wynikające z rozporządzenia prawa dotyczące jego danych osobowych. Niemniej jednak, jak wynika z art. 8 ust. 1 -3 Ustawy, przy realizacji badań klinicznych będących badaniami naukowymi dopuszcza się ograniczenie wskazanych praw osób, których dane dotyczą, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację celów badania klinicznego będącego badaniem naukowym i jeżeli ograniczenie praw jest konieczne do realizacji tych celów. Przykład takiej sytuacji wskazuje uzasadnienie do Ustawy: *należy podkreślić ewentualne zmiany w danych osobowych uczestnika badania klinicznego, które mogłyby negatywnie wpłynąć na wynik badania klinicznego, jego uwiarygodnienie czy też niemożliwość publikacji wyników badania klinicznego. W konsekwencji produkty lecznicze opracowane w ramach badania klinicznego, których skuteczność została dowiedziona w ramach tego badania, nie będą mogły być kierowane do dalszych czynności skutkujących udostępnieniem ich w szerokim stosowaniu ogółowi populacji. W konsekwencji może to wpłynąć negatywnie na prawo innych osób do skutecznego leczenia. Dodatkowo należy podkreślić, że zmiany w danych osobowych uczestnika badania klinicznego skutkujące ww. niemożnością realizacji badania klinicznego będącego badaniem naukowym wpłyną negatywnie na prawa pozostałych osób biorących udział w badaniu.*

Prawa, które mogą być objęte ograniczeniem to:

- prawa dostępu do danych (art. 15 RODO), przy czym w tym przypadku ograniczenie można stosować do czasu zakończenia badania klinicznego
- prawa do sprostowania danych (art. 16 RODO) – można ograniczyć stosowanie tego prawa w trakcie badania klinicznego i po jego zakończeniu
- prawa do ograniczenia przetwarzania (art. 18 RODO) – zasady ograniczenia prawa są takie same jak dla prawa sprostowania danych
- prawa do sprzeciwu wobec przetwarzania (art. 21 RODO) – tak samo jak powyżej, zasady ograniczenia prawa są takie same jak dla prawa sprostowania danych

Opisane powyżej ograniczenie praw nie dotyczy poniższych danych (co oznacza, że można w stosunku do nich realizować ww. prawa dostępu, sprostowania, ograniczenia przetwarzania, sprzeciwu):

- imię i nazwisko
- numer PESEL, a w przypadku gdy nie nadano tego numeru – rodzaj i numer dokumentu potwierdzającego tożsamość oraz data urodzenia
- adres korespondencyjny
- numer telefonu lub adres poczty elektronicznej



Tym samym w przypadku otrzymania wniosku dot. praw wynikających z RODO od uczestnika badania podmiot prowadzący badania kliniczne powinien pamiętać, że nie musi w pełni odpowiadać na każdy wniosek i realizować jego żądań, jednakże:

- ustawa wprowadza OGRANICZENIE, a nie WYŁĄCZENIE praw
- administrator danych powinien móc WYKAZAĆ, ŻE SPEŁNIONE ZOSTAŁY PRZESŁANKI OGRANICZENIA wynikające z ustawy (tj. jest prawdopodobne że prawa uniemożliwią/poważnie utrudnią realizację celów badania klinicznego zgodnie z opisem na początku niniejszego punktu); mając na uwadze że RODO wymaga rozliczalności działań, ocena i analiza ją poprzedzająca powinna być UDOKUMENTOWANA
- należy pamiętać, że OGRANICZENIE NIE DOTYCZY WSZYSTKICH PRAW, KTÓRE RODO PRZYZNAJE OSOBOM KTÓRYCH DANE DOTYCZĄ (np. nie jest możliwe ograniczenie prawa do bycia zapomnianym, tj. prawa do usunięcia danych na podstawie art. 17 RODO)
- mimo ograniczenia, OBOWIĄZUJĄ PRZEPISY DOT. REALIZACJI PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ WYRAŻONE W ROZDZIALE III RODO (np. wciąż obowiązuje termin 1 miesiąca na odpowiedź na wniosek, a w przypadku nieuwzględnienia wniosku – w ciągu jednego miesiąca należy wytłumaczyć czemu żądanie nie zostanie zrealizowane)

Szczególnie istotne bezpieczeństwo danych

Art. 8 ust. 4 Ustawy podkreśla, że przy przetwarzaniu danych osobowych uzyskanych na potrzeby badania klinicznego oraz w trakcie tego badania administrator danych wdraża odpowiednie zabezpieczenia techniczne i organizacyjne, o których mowa w art. 32 ust. 1 RODO, mając w szczególności na względzie charakter danych osobowych przetwarzanych w badaniu klinicznym i ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane w związku z prowadzonym badaniem klinicznym.

Zapis ten podkreśla jak istotne jest prawidłowe zabezpieczenie danych osobowych przetwarzanych w toku badania klinicznego. Można argumentować, że wskazane w nim wymogi powielają obowiązki wynikające z RODO, niemniej jednak – niezależnie od rozstrzygnięcia powyższych wątpliwości - dla podmiotów organizujących badania kliniczne istotne powinno być odpowiednie zabezpieczenie danych, tak by nie doszło do naruszenia ich bezpieczeństwa (w tym np. niepożądanego dostępu osoby trzeciej lub utracenia dostępności danych przez administratora). Należy pamiętać, że zabezpieczenia mogą być zarówno techniczne (np. szyfrowanie danych) jak i organizacyjne (np. polityka dostępu do danych oparta na zasadzie minimalnego dostępu).

Jak wynika z RODO i praktyki Prezesa Urzędu Ochrony Danych Osobowych istotne jest nie tylko WDROŻENIE odpowiednich zabezpieczeń, ale i ZWERYFIKOWANIE ICH SKUTECZNOŚCI oraz REGULARNE ICH TESTOWANIE. Administrator danych powinien zapewnić bezpieczeństwo danych nie tylko w swoich systemach, a TAKŻE W SYSTEMACH SWOICH PODMIOTÓW PRZETWARZAJĄCYCH (za pomocą zapisów umowy z tym podmiotem, a także za pomocą regularnych kontroli bezpieczeństwa u tego podmiotu).

Co ze zgodą na przetwarzanie danych osobowych w toku badania klinicznego?

Ustawa uchyla podstawę dla dwóch rozporządzeń krajowych, które wskazywały na konieczność zbierania zgód na przetwarzanie danych osobowych w toku badania klinicznego (tj. zgód wynikających z RODO, niebędących zgodami na udział w badaniu klinicznym), czyli rozporządzenia Ministra Zdrowia z dnia 2 maja 2012 r. w sprawie Dobrej Praktyki Klinicznej oraz rozporządzenia Ministra Zdrowia z dnia 12 października 2018 r. w sprawie wzorów dokumentów przedkładanych w związku z badaniem klinicznym produktu leczniczego oraz opłat za złożenie wniosku o rozpoczęcie badania klinicznego. Rozporządzenia te są obecnie uznane za uchylone.

Powyższe oznacza, że za uchylone uznano przepisy wskazujące wprost, że dla przetwarzania danych w toku badania klinicznego konieczne jest zebranie odrębnej zgody na przetwarzanie danych osobowych. W konsekwencji, w toku badań klinicznych można rozważyć inne podstawy przetwarzania danych, niż zgoda, w tym oprzeć się na europejskich wytycznych w tym zakresie (np. na opinii Europejskiej Rady Ochrony Danych nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między RBK a RODO).

Stosowanie zgody jako podstawy przetwarzania danych osobowych w toku badań klinicznych nie wydaje się odpowiednie z wielu powodów. Przywołana powyżej opinia EROD wskazuje, że zgoda nie jest odpowiednią podstawą przetwarzania w przypadku każdego badania klinicznego ze względu na wątpliwości co do jej „dobrowolności". Podobne wątpliwości wyrażono w uzasadnieniu do Ustawy, gdzie wskazano, ze *pomimo że dotychczas przetwarzanie danych osobowych uczestników badania opierało się na ich wyraźnej zgodzie zarówno przepisy RODO, jak i wydana na ich podstawie opinia EROD, wskazują na możliwość zastosowania innych podstaw prawnych przetwarzania danych osobowych – w szczególności w postaci podstawy wskazanej w art. 9 ust. 2 lit. j rozporządzenia 2016/679 (przetwarzanie jest niezbędne do celów badań naukowych), które pozwalają na zachowanie większej spójności z zasadami prowadzenia badań klinicznych. Stosowanie podstawy prawnej dotyczącej niezbędności przetwarzania do celów badań naukowych, jako podstawy prawnej przetwarzania danych uczestników badania, wydaje się być właściwym stanowiskiem (...).* Wątpliwości budzi także fakt, że zgoda może być w każdym momencie wycofana, co tworzy ryzyko dla integralności bazy danych zgromadzonych w toku badania.

Ze wstępnych konsultacji z odpowiednimi organami wynika, że organy zatwierdzające dokumentację dot. badania klinicznego mogą wciąż wymagać zgód na przetwarzanie danych osobowych. Nie otrzymaliśmy jednak wiążących informacji w tym zakresie.

W naszej ocenie w świetle powyższej zmiany prawa, uzasadnione będzie rozważenie innych, oprócz zgody, podstaw przetwarzania danych osobowych wskazanych w art. 6 i 9 RODO.

Weryfikacja wieku nieletnich na platformach społecznościowych - teoria a praktyka. Możliwe zaostrzenie dotychczasowych wymagań na rynku europejskim, Francja prekursorem zmian.

Agnieszka Jurcewicz-Androsz
Prawnik, adwokat
agnieszka.jurcewicz-androsz@skslegal.pl
+48 600 782 823

Niebezpieczeństwo w sieci

Ochrona dzieci w świecie cyfrowym jest zagadnieniem budzącym ogromne zainteresowanie. Dostęp do sieci umożliwia nieletnim kontakt ze szkodliwymi i nielegalnymi treściami oraz zachowaniami, które mogą mieć wpływ na ich prawidłowy rozwój. Nękanie, nagabywanie do celów seksualnych czy też do samookaleczania się, promowanie postaw prowadzących do niebezpiecznych praktyk żywieniowych, wyłudzenia, kradzieże tożsamości, cyberbullying ze strony rówieśników, jak również możliwy dostęp do treści i produktów zarezerwowanych wyłącznie dla osób dorosłych - to nie wszystkie z zagrożeń świata cyfrowego czyhających na dzieci i młodzież.

Mając na uwadze powyższe oraz ogromną popularność platform społecznościowych takich jak TikTok, Facebook, Instagram czy też YouTube wśród nieletnich (zarówno poniżej 13 jak i 18 r.ż.) ważnym zagadnieniem na forum europejskim staje się skuteczne uregulowanie prawne, jak i faktyczne kwestii związanych z weryfikacją wieku dzieci rejestrujących się na tych platformach oraz ewentualną zgodą ich opiekunów na taką rejestrację. Wypracowane tutaj rozwiązanie będzie mogło być później zastosowane przez podmioty świadczące inne usługi w sieci.

Wymogi dotyczące wieku na platformach społecznościowych

Formalnie, użytkownikiem większości platform społecznościowych może zostać osoba, która ukończyła 13 lat. W zależności od platformy społecznościowej niektóre funkcje (np. możliwość wysyłanie bezpośrednich wiadomości, ustawienia prywatności profilu czy też możliwość robienia relacji „na żywo") i treści przeznaczone dla dorosłych są wyłączone dla osób pomiędzy 13 a 18 r.ż. Ma to na celu zapewnienie większego bezpieczeństwa dzieci w przestrzeni cyfrowej. Działanie tych funkcji uzależnione jest jednak od wskazanej przez użytkownika daty urodzenia lub wieku podanych w trakcie rejestracji.

Weryfikacja i przetwarzanie danych osobowych dzieci w sieci

Obowiązujące przepisy europejskie dotyczące przetwarzania danych osobowych dzieci, jeżeli podstawą przetwarzania jest zgoda, zezwalają na samodzielne udzielenie zgody na takie przetwarzanie w przypadku, gdy usługi społeczeństwa informacyjnego są oferowane bezpośrednio dziecku, które ukończyło 16 lat (państwa członkowskie mogą jednak przewidzieć niższą granicę wieku, ale musi ona wynosić co najmniej 13 lat). Jeżeli dziecko jest młodsze, przetwarzanie danych dziecka będzie zgodne z prawem wyłącznie, gdy opiekun prawny dziecka wyrazi na to zgodę (art. 8 pkt 1 RODO). W Polsce, w przypadku dzieci w wieku 13 - 16 lat powinny zostać złożone dwa oświadczenia zawierające zgodę na przetwarzanie danych osobowych – dziecka, jak i jego przedstawiciela ustawowego. Z kolei Dyrektywa o audiowizualnych usługach medialnych (2010/13/UE „Dyrektywa") implementowana w Polsce do ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji wymaga przyjęcia odpowiednich środków w celu ochrony dzieci przed szkodliwymi treściami online, w tym do stosowania narzędzi mających na celu przeprowadzenie weryfikacji wieku użytkowników platform udostępniających video w odniesieniu do treści, które mogą zaszkodzić fizycznemu, psychicznemu lub moralnemu rozwojowi małoletnich (art. 28b pkt 3 Dyrektywy).

Należy też wskazać, że art. 8 ust. 1 RODO, poprzez ustalenie granicy wieku, od którego dzieci mogą w niektórych przypadkach wyrazić zgodę na przetwarzanie własnych danych - w sposób dorozumiany - ustanawia potrzebę weryfikacji ich wieku (art. 8 pkt 2 RODO). Tym samym, dostawcy usług internetowych powinni skutecznie weryfikować wiek użytkowników aby ustalić czy dany użytkownik w ogóle może posiadać konto na określonej platformie społecznościowej (czy ma ukończone co najmniej 13 lat) a jeśli tak jakie ustawienia będą dla niego właściwe w związku z jego wiekiem (na niektórych platformach w Polsce zależeć będą one od tego czy ma 13-16 czy 16-18 lat). Ponadto, przetwarzając dane osobowe na podstawie zgody, w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, mają obowiązek sprawdzenia ich wieku a w razie konieczności – powinni także uzyskać zgodę ich opiekunów prawnych na przetwarzanie danych osobowych (np. w przypadku przetwarzania danych osobowych dziecka w celu przedstawienia mu spersonalizowanych reklam). Muszą w tym celu dołożyć rozsądnych starań, biorąc pod uwagę dostępne technologie na rynku.

Dzieci rejestrują się na platformach zawyżając swój wiek

Niestety, z badań przeprowadzonych w lipcu 2022 r. przez Ofcom (brytyjski organ państwowy kontrolujący i nadzorujący rynek mediów i telekomunikacji) wynika, że jedna trzecia dzieci w wieku od 8 do 17 lat, które mają profil w mediach społecznościowych rejestruje się z fałszywą datą urodzenia jako osoby pełnoletnie. Stwierdzono także, że większość dzieci w wieku od 8 do 17 lat (77%), które korzystają z mediów społecznościowych - gdzie minimalny wiek użytkownika to 13 lat - ma obecnie swój profil na co najmniej jednej z dużych platform. Co więcej, badania sugerują, że 60% dzieci w wieku od 8 do 12 lat, które korzystają z tych platform, rejestruje się za pomocą własnego profilu (co oznacza, że podają nieprawdziwe dane dotyczące wieku). Wśród tej grupy nieletnich prawie połowa założyła samodzielnie co najmniej jeden ze swoich profili, a pozostali korzystali z pomocy rodzica lub opiekuna. Wyniki sugerują również, że 47% dzieci w wieku od 8 do 15 lat z profilem w mediach społecznościowych deklaruje (poprzez zawyżenie wieku podczas rejestracji), że ma więcej niż 16 lat, a 32% dzieci w wieku od 8 do 17 lat nieprawdziwie deklaruje, że ma więcej niż 18 lat. Wśród młodszej grupy wiekowej, w wieku od 8 do 12 lat (czyli grupy, która teoretycznie w ogóle nie powinna mieć dostępu do takich usług), w badaniu oszacowano, że 39% ma profil wiekowy użytkownika 16+, a 23% - 18+, również wskutek podania zawyżonego wieku w trakcie rejestracji.

Przeprowadzone badanie wykazuje, że sposób weryfikacji wieku przez platformy społecznościowe, oparty na deklaracji użytkownika dotyczącej wieku (najczęściej przez podanie daty urodzenia) jest nieskuteczny. W rezultacie: (i) duża grupa dzieci poniżej 13 r.ż. ma własny profil na co najmniej jednej z platform społecznościowych wskutek podania fałszywych danych dotyczących wieku podczas rejestracji; (ii) dzieci są narażone na treści i ustawienia niedostosowane do ich prawdziwego wieku i osiągniętej dojrzałości - również wskutek zawyżenia wieku podczas rejestracji. Podobne wnioski zostały przedstawione przez Age Verification Providers Association (AVPA) we wrześniu 2021 r., która sygnalizowała, że faktyczna weryfikacja wieku użytkownika jest niewielka lub żadna w większości państw członkowskich UE w przypadku oferowania towarów, treści lub usług w sieci, a deklaracja własna jest nieskutecznym rozwiązaniem. Również w rekomendacjach nr 7 francuskiego organu ochrony danych Commission Nationale de l'Informatique et des Libertés („CNIL") z 9 sierpnia 2021 r., pojawia się informacja, że 44% dzieci w wieku 11-18 lat skłamało odnośnie wieku na swoich platformach społecznościowych.

Postępowania dot. ochrony danych dzieci

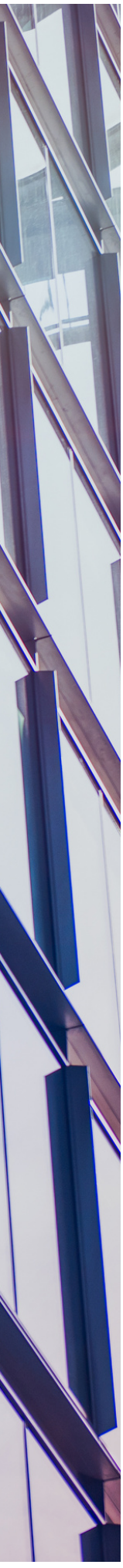
W tym miejscu należy wspomnieć o niektórych trwających i zakończonych postępowaniach dotyczących przetwarzania danych osobowych dzieci w sposób niezgodny z RODO w Internecie. We wrześniu 2022 r. irlandzki Data Protection Commission przedstawił wstępną decyzję innym organom nadzorczym na terenie UE, po przeprowadzonym postępowaniu badającym zgodność TikTok-a z ochroną danych RODO w fazie projektowania i domyślnymi wymaganiami dotyczącymi przetwarzania danych osobowych w kontekście ustawień platformy dla użytkowników poniżej 18 roku życia i środków weryfikacji wieku dla osób poniżej 13 roku życia. Czekamy na decyzję.

Information Commissioner Office wydał w dniu 4 kwietnia 2023 r. decyzję i nałożył na Tik Tok-a karę w wysokości 12,7 mln funtów. Organ wskazał, że Tik-Tok m.in.: przetwarzał dane osobowe dzieci poniżej 13 r.ż. (i) co jest sprzeczne z regulaminem Tik Tok-a oraz (ii) bez zgody opiekunów prawnych co jest niezgodne z RODO. Ponadto, spółka „nie zrobiła wystarczająco dużo" by sprawdzić kto korzysta z usług platformy społecznościowej i nie podjęła „wystarczających działań" by usunąć dane dzieci poniżej 13 r.ż.

Potencjalne rozwiązania

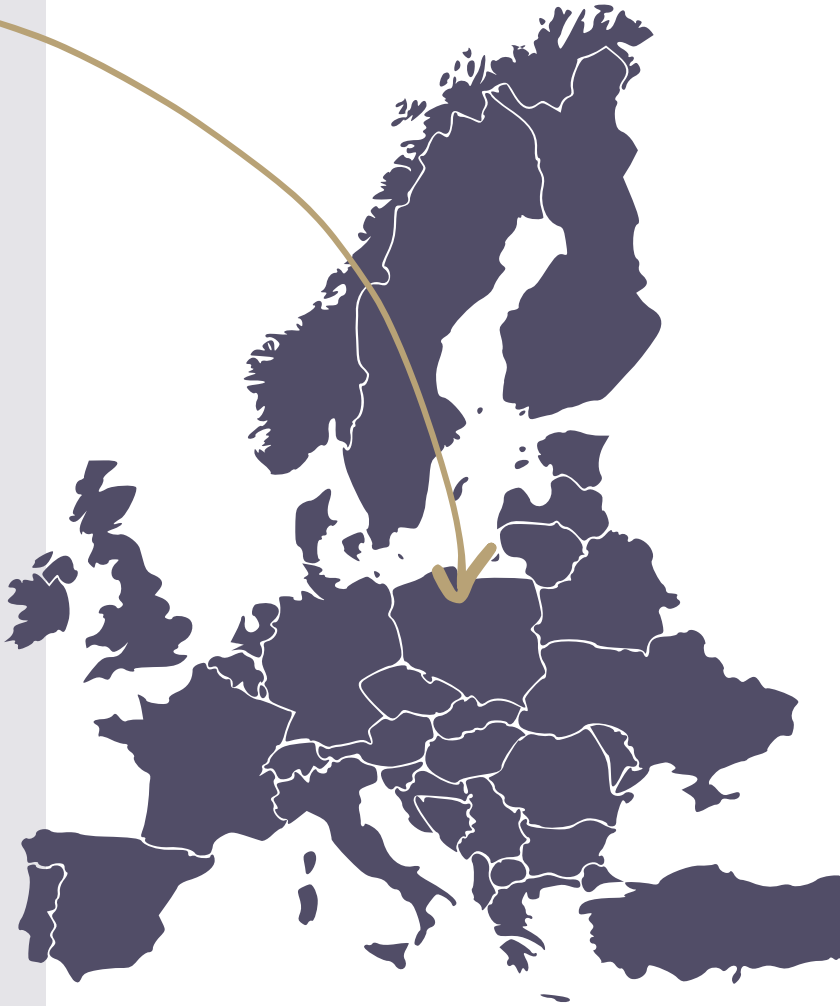
Powyższe wskazuje, że mechanizmy ustalania wieku stosowane przez platformy społecznościowe nie są efektywne. Z drugiej strony trudno jest znaleźć rozwiązania, które będą jednocześnie proste i adekwatne. Potwierdza to opinia CNIL z 22 września 2022 r., z której wynika, że aktualne systemy służące do weryfikacji wieku są albo (i) zbyt inwazyjne (np. te użyciem karty kredytowej czy też analizą twarzy; wskazano że jeżeli w ogóle miałyby być stosowane to powinny być używane z pośrednictwem zaufanego podmiotu trzeciego) albo (ii) bardzo łatwe do obejścia przez użytkownika jak np. deklaracja dotycząca wieku. W opinii wyraźnie wskazano, że weryfikacja wieku powinna gwarantować poufność informacji oraz należy przestrzegać zasady minimalizacji zbieranych danych. CNIL opracowuje program demo, który za pośrednictwem niezależnego podmiotu trzeciego i jego systemu miałby weryfikować wiek użytkownika z poszanowaniem tych zasad.

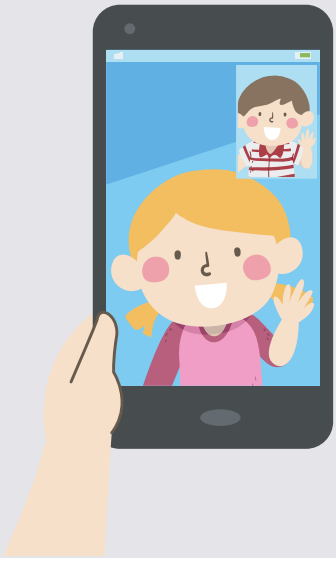
Administracja francuska podejmuje działania mające na celu zmuszenie właścicieli platform społecznościowych do wiarygodnego sprawdzania wieku swoich użytkowników. Przepisy przyjęte w maju przez francuski Parlament mają m.in. zmusić właścicieli platform społecznościowych (np. TikTok, Instagram czy też YouTube) do weryfikacji wieku użytkowników i żądania zgody rodzica lub rodziców w przypadku osób poniżej 15 r.ż. Rodzice mają też być uprawnieni do usunięcia konta społecznościowego dziecka, które nie ukończyło 15 lat. Przewidziano wysokie kary, w wysokości do 1 procenta rocznego globalnego obrotu firmy, w przypadku nieprzestrzegania ww. zasad. Rozwiązania techniczne - weryfikujące wiek użytkowników będą musiały być zatwierdzone przez ARCOM (*l'Autorité de régulation de la communication audiovisuelle et numérique* tj. organ regulacyjny ds. komunikacji audiowizualnej i cyfrowej) i CNIL. ARCOM byłby upoważniony również do pozywania dostawców usług nieprzestrzegających obowiązujących przepisów. Obecnie trwają prace obu izb francuskiego parlamentu nad wersją ustawy. Ponadto, we Francji testowany jest system podwójnej anonimowości. Użytkownicy weryfikują swój wiek lub tożsamość cyfrową na stronie lub platformie innej firmy, która generuje token. Następnie token jest używany na stronie internetowej, która wymaga weryfikacji wieku.



Sytuacja w Polsce

Teoretycznie, konto na większości platform społecznościowych mogą założyć dzieci od 13 r.ż., co wiąże się od razu z przetwarzaniem ich danych w celu realizacji umowy i często również na podstawie uzasadnionego prawnie interesu, bez konieczności wyrażania odrębnej zgody, a więc angażowania rodziców. Jak wynika ze wskazanych powyżej badań, dzieci standardowo zawyżają swój wiek. W rezultacie, mają dostęp do treści dla nich nieprzeznaczonych. Polski ustawodawca nie planuje obecnie działań podobnych to tych realizowanych we Francji, nie mniej należy założyć, że pośrednio regulacja francuska może mieć również wpływ na polski rynek wskazując realne sposoby umożliwiające weryfikację wieku użytkowników rejestrujących się na platformach społecznościowych.





Podsumowanie

Weryfikacja wieku użytkowników w sieci jest skomplikowana w szczególności z uwagi na brak skutecznych środków technicznych, które umożliwiałyby dokonanie skutecznej weryfikacji wieku z poszanowaniem poufności i minimalizacji danych. Aktualnie prowadzone testy nowych rozwiązań technicznych i planowane wytyczne techniczne francuskich organów regulacyjnych mogą wyznaczyć powszechny trend weryfikacji danych dzieci w Europie.

Prace nad nowym narzędziem dla transferu danych do USA

Maciej Jakubowski
Prawnik, radca prawny
maciej.jakubowski@skslegal.pl
+48 882 630 942

Od czasu wyroku TSUE w sprawie *Schrems II* transfer danych osobowych do Stanów Zjednoczonych nastręcza wiele trudności. Trwają prace nad rozwiązaniem tej sytuacji. Niedawno Europejska Rada Ochrony Danych wydała opinię na temat projektowanych rozwiązań.

Transfer danych na gruncie RODO

RODO określa zasady dotyczące transferu danych do państw trzecich tj. przekazywania danych osobowych do odbiorców zlokalizowanych poza Europejskim Obszarem Gospodarczym. Transfer z reguły będzie miał miejsce m.in. w sytuacjach udostępniania danych do administratora w państwie trzecim, czy przechowywania danych na serwerach zlokalizowanych poza EOG. Wielkość transferu czy jego częstotliwość nie ma znaczenia przy określaniu zasad na jakich transfer powinien się odbywać. Nadrzędnym celem przepisów rozporządzenia jest zapewnienie, że poziom ochrony gwarantowany przez RODO nie zostanie osłabiony, gdy dane osobowe dane są przekazywane do państw trzecich lub do organizacji międzynarodowych. Dlatego wprowadzono różne narzędzia służące do legalizacji transferu. Jedynym z nich jest tzw. decyzja o adekwatności wydawana przez Komisję Europejską. Na jej mocy państwo trzecie może zostać uznane za oferujące odpowiedni poziom ochrony, co oznacza, że dane mogą być przekazywane do innego podmiotu w tym państwie trzecim bez konieczności zapewnienia przez podmiot przekazujący dane dalszych zabezpieczeń lub obwarowania ich dodatkowymi warunkami.

Transfer danych do Stanów Zjednoczonych

Przez pewien czas transfer danych osobowych do Stanów Zjednoczonych był możliwy w oparciu o decyzję o adekwatności tzw. *Privacy Shield*. Sytuacja ulegała zmianie po wyroku Trybunału Sprawiedliwości UE (TSUE) w sprawie C-311/18 (Schrems II).

Trybunał w toku postępowania badał zakres stosowania RODO, zasady przekazywania danych do państw trzecich, kompetencje organów nadzorczych w tym dopuszczalność przekazywania danych osobowych do Stanów Zjednoczonych. Jednym z głównych rozstrzygnięć wyroku było uznanie poziomu ochrony zapewnianej przez *Privacy Shield* za nieadekwatny, co doprowadziło do unieważnienia decyzji. Od tego momentu transfer danych do Stanów wymaga podejmowania dodatkowych kroków po stronie podmiotów zainteresowanych zalegalizowania takiego transferu. Często działaniom tym towarzyszą koszty oraz duży nakład pracy.

Prace nad nową decyzją o poziomie adekwatności

Aktualnie obie strony, USA oraz UE, podejmują starania w celu wypracowania nowych rozwiązań, których zwieńczeniem miałaby być nowa decyzja o adekwatności dla USA. W lutym Europejska Rada Ochrony Danych wydała niewiążącą **Opinię 5/2023** na temat projektu decyzji KE. Z jednej strony z zadowoleniem przyjęto wprowadzone zmiany, w tym zasady konieczności i proporcjonalności gromadzenia danych przez służby wywiadowcze USA oraz nowy mechanizm dotyczący sądowych środków zaskarżenia dla osób w UE, których dane dotyczą. Z drugiej strony wyrażono zaniepokojenie m.in. w kwestiach praw podmiotów danych czy zbiorczego gromadzenia danych. Opinia EROD nie jest wiążąca. Komisja może wziąć ją pod uwagę, przygotowując ostateczny tekst swojej decyzji w sprawie odpowiedniego poziomu ochrony. Następnie projekt decyzji zostanie przedłożony do zatwierdzenia przez komitet złożony z przedstawicieli państw członkowskich. Oczekuje się, że Komisja przyjmie ostateczną decyzję w sprawie odpowiedniego poziomu ochrony w połowie 2023 r. Przyjęcie nowej decyzji o adekwatności powinno doprowadzić do ustabilizowania problematyki transferu danych do USA.

ORZECZNICTWO & DECYZJE

Zasady odpowiedzialności administratora w przypadku ataku hakerskiego – NSA uchyla decyzję PUODO ws. Morele.net

Druga co do wysokości (2.830.410 PLN, co stanowi równowartość 660 000 EUR) kara PUODO nałożona na Morele.net Sp. z o.o. została uchylona przez NSA. Sprawa wraca do PUODO.

Kara dotyczyła wycieku danych klientów sklepu internetowego, wskutek którego haker wysyłał SMSy mające na celu wyłudzenie danych dostępowych do konta w banku klientów tego sklepu. **PUODO ustalił, że administrator stosował niewystarczające zabezpieczenia podczas przetwarzania danych, które nie chroniły przed atakiem hakerskim, w tym m.in. stosował nieodpowiednie metody uwierzytelniania w celu uzyskania dostępu do danych.**

Decyzja PUODO była utrzymana przez Wojewódzki Sąd Administracyjny w Warszawie (wyrok z 3 września 2020 r., sygn. akt II SA/Wa 2559/19). Niemniej jednak, z PUODO i WSA nie zgodził się NSA.

Techniczne zabezpieczanie danych osobowych

Z wyroku NSA wynika istotna kwestia dot. odpowiedniego zabezpieczenia danych. NSA stwierdził, że administrator (przetwarzający) nie odpowiada za sam fakt nielegalnego działania osoby trzeciej (hakera), które doprowadziło do nieuprawnionego dostępu do danych, lecz za nieodpowiedni poziom stosowanych zabezpieczeń dopuszczający taki dostęp. Może bowiem dojść do niepożądanego dostępu do danych przez hakera nawet przy stosowaniu najwyższego poziomu zabezpieczeń. Tym samym, z **wyroku wynika, że obowiązek odpowiedniego zabezpieczenia danych ma charakter obowiązku starannego działania, nie zaś rezultatu.** Jak wskazuje NSA, *„o naruszeniu przepisu nie przesądza sama okoliczność nieuprawnionego dostępu do danych, ponieważ taki stan rzeczy jest potencjalnie możliwy do zaistnienia również przy dochowaniu najwyższego poziomu zabezpieczeń”*.

Jest to istotne, ponieważ z decyzji PUODO ws. Morele.net można było wywnioskować, że administrator będzie odpowiedzialny za każdy nieuprawniony dostęp do danych, mimo że RODO wymaga dopasowania zabezpieczeń do konkretnej sytuacji, w tym do ryzyka z jakim dla podmiotów danych wiąże się przetwarzanie ich danych. Spojrzenie wyrażone w wyroku NSA „racjonalizuje” wymagania wobec podmiotów przetwarzających dane i zwiększa ich pewność prawną. NSA wskazuje, również że wdrożenie środków technicznych powinno być oparte na podstawie przeprowadzonej oceny ryzyka i że ocena przyjętych środków bezpieczeństwa powinna być „dynamiczna”. Za odpowiednie należy uznać zabezpieczenia, których dochowanie mogło być w dacie i okolicznościach nieuprawnionego dostępu do danych obiektywnie wymagane od podmiotu (nie zaś środki skuteczne w każdym przypadku).

Organizacje przetwarzające dane powinny więc być pewne, że spełniają standardy organizacyjne i techniczne, które są dopasowane do aktualnych ryzyk. Ponadto, odpowiednia analiza ryzyka pomoże uzasadnić powyższe środki. Te działania będą silnymi argumentami w przypadku naruszeń ochrony danych osobowych, w tym ew. ataków hakerskich.

Zasady postępowania przed PUODO do weryfikacji?

NSA wskazał także, że pracownicy PUODO nie mieli kompetencji by w momencie wydawania decyzji oceniać środki bezpieczeństwa wdrożone przez administratora danych i że w toku postępowania należało przeprowadzić opinię z biegłego. PUODO nie uprawdopodobnił, że posiadał wiedzę, by ocenić środki techniczne w rozważanej, precedensowej sprawie. NSA podkreśla jednak, że wątpliwe jest czy w dotychczasowej praktyce prowadził sprawy podobne do omawianej i czy miał kompetencje by oceniać prawidłowość środków technicznych bez powołania biegłego. Ponadto, NSA wskazało że w momencie postępowania i wydania decyzji RODO było stosunkowo nową regulacją. Teza ta budzi kontrowersje, ponieważ wiedzy takiej teoretycznie należy oczekiwać od pracowników PUODO. Sam PUODO wniósł pismo w tej sprawie do NSA, wskazują, że „orzeczenie NSA w sposób niezaprzeczalny i precedensowy kwestionuje niezależność Prezesa UODO jako organu nadzorczego, jak i podważa jego kompetencje oraz kwalifikacje merytoryczne zatrudnionych w nim osób, niezbędne do wykonywania zadań, do których organ ten został powołany”.

NSA miał także wątpliwości co do obiektywizmu PUODO. Sąd wskazał, że organ powinien uwzględniać wnioski dowodowe strony dążące do wykazania korzystnych dla niej okoliczności faktycznych, jeżeli istnieją wątpliwości lub braki w zakresie niezbędnych informacji. Jest to także istotne z perspektywy prawa do obrony strony.

NSA wskazało także, że w analizowanej sprawie PUODO nie przedstawiło stronie wniosków wynikających z analizy środków bezpieczeństwa, uniemożliwiając jej czynne odniesienie się do nich i sprawiając, że stały się one znane stronie dopiero po wydaniu decyzji.

Powyższe zachęca do aktywnego uczestniczenia w postępowaniach przed PUODO i do wyrażania wątpliwości wobec podejścia PUODO do naruszenia poprzez składanie odpowiednich wniosków dowodowych mających podważyć niekorzystne rozumienie sytuacji.

Wyrok dostępny jest tutaj

Błędy pracowników nie mogą uzasadniać opóźnienia dokonania zawiadomienia o naruszeniu ochrony danych

Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę P4 sp. z o.o. na decyzję PUODO nakładającą na spółkę administracyjną karę pieniężną w wysokości 100.000,00 złotych za niezawiadomienie PUODO w terminie 24 godzin od stwierdzenia naruszenia ochrony danych osobowych.

P4 w postępowaniu przed PUODO wyjaśniła, że zawiadomienie PUODO o naruszeniu ochrony danych osobowych po upływie 24 godzin związane było z nieumyślnymi błędami pracowników kancelarii odpowiedzialnych za wysyłkę korespondencji. W ocenie PUODO, błędy pracowników nie mogą uzasadniać opóźnienia zawiadomienia organu nadzorczego. WSA przychylił się do tego stanowiska.

WSA potwierdził, że rzeczywiście P4 nie wywiązała się z obowiązku zawiadomienia o naruszeniu organu nadzorczego w terminie. WSA stwierdził również, że PUODO w sposób właściwy ustalił wysokość kary pieniężnej, która jest adekwatna do stwierdzonego naruszenia i spełnia zamierzone funkcje – represyjną i prewencyjną.

Wyrok dostępny jest tutaj

Zadośćuczynienie za naruszenie przepisów o ochronie danych osobowych

Zapadło kolejne orzeczenie dotyczące naruszenia dóbr osobistych z wątkiem danych osobowych w tle. Kwota zadośćuczynienia wyniosła w tym przypadku 20.000 złotych, czyli była stosunkowo wysoka dla tego typu spraw. Sąd Okręgowy w wyroku z 5 grudnia 2022 (XXV C 559/22) ustalił, że doszło do opublikowania w Internecie danych osobowych kobiety będącej asesorem komorniczym w sposób niezgodny z przepisami o ochronie danych osobowych. Chodzi o niezanonimizowany fragment orzeczenia Naczelnego Sądu Administracyjnego, który w okresie od 2016 do 2021 r. był powszechnie dostępny w Centralnej Bazie Orzeczeń Sądów Administracyjnych i dotyczy kwestii szczególnie drażliwej, bowiem jej postępowania dyscyplinarnego. Odkrycie to wywołało u kobiety poczucie strachu, bezsenność, brak apetytu i załamanie nerwowe. Osoba ta uświadomiła sobie, że każdy mógł dowiedzieć się o jej historii zawodowej zawierającej element postępowania dyscyplinarnego. Obok rozważań na gruncie dóbr osobistych sąd podkreślił, że brak odpowiedniej anonimizacji danych powódki, a następnie umieszczenie orzeczenia sądowego zawierającego niezanonimizowane dane w Centralnej Bazie Orzeczeń, stanowiło naruszenie przepisów RODO, które w art. 6 wymienia przypadki, w jakich przetwarzanie danych osobowych (a zatem również ich publikowanie) jest zgodne z prawem.

Wyrok dostępny jest tutaj

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

Interesujące decyzje PUODO w pierwszym kwartale 2023 r.

1. Decyzja w sprawie Kancelarii PIONIER – kara za przetwarzanie danych bez podstawy prawnej

Nie można przetwarzać danych osobowych, nie mając podstawy prawnej

W dniu 30 listopada 2022 r. PUODO nałożył na wspólników spółki cywilnej kancelarii PIONIER **karę pieniężną w wysokości 45.000,00 złotych** za naruszenie zasad przetwarzania danych osobowych poprzez przetwarzanie danych potencjalnych klientów administratora, w tym danych dotyczących zdrowia, bez podstawy prawnej, w szczególności bez uzyskania zgody na przetwarzania danych.

Działalność wspólników polega na świadczeniu pomocy prawnej w zakresie reprezentowania klientów poszkodowanych głównie w wypadkach komunikacyjnych przed towarzystwami ubezpieczeniowymi i sądami celem uzyskania na ich rzecz odszkodowań. Wspólnicy nawiązywali kontakt z potencjalnymi klientami na podstawie materiałów prasowych, informacji w mediach społecznościowych, itp. Podczas pierwszej rozmowy z potencjalnymi klientem pozyskiwano ustne zgody na przetwarzanie danych klientów do czasu zawarcia umowy. Wspólnicy w żaden sposób nie ewidencjonowali zgód pozyskanych w ustny sposób.

W ocenie PUODO administrator powinien być w stawnie wykazać podstawę prawną przetwarzania danych przed organem nadzorczym, w tym wyraźną zgody na przetwarzanie danych. W tym przypadku, wspólnicy nie byli w stanie przedstawić dowodu na uzyskanie takich zgód.

Decyzja dostępna jest tutaj

2. Decyzja w sprawie wspólnoty mieszkaniowej – kara za brak zgłoszenia naruszenia ochrony danych, brak zawiadomienia osób, których naruszenie dotyczyło, brak umowy powierzenia przetwarzania danych

W dniu 7 lutego 2023 r. PUODO nałożył na wspólnotę mieszkaniową **administracyjną karę pieniężną w wysokości 1.500,00 złotych** za kilka uchybień w działalności administratora, w tym brak zgłoszenia naruszenia ochrony danych, brak zawiadomienia osób, których naruszenie dotyczyło, brak umowy powierzenia przetwarzania danych osobowych członków wspólnoty mieszkaniowej.

W tym przypadku, w wyniku kradzieży kopii aktu notarialnego znajdującego się u zarządcy wspólnoty mieszkaniowej, doszło do naruszenia ochrony danych osobowych członków wspólnoty. Wspólnota mieszkaniowa nie zdecydowała się zawiadomić PUODO o naruszeniu. W ocenie PUODO administrator miał obowiązek dokonania zgłoszenia bowiem ryzyko wystąpienia negatywnych konsekwencji dla członków wspólnoty było wyższe niż znikome.

Co więcej, zdaniem PUODO administrator powinien również zawiadomić o zdarzeniu osoby, których dane znajdowały w skradzionym dokumencie celem umożliwienia im przeciwdziałania potencjalnym szkodom związanym z kradzieżą tego dokumentu. Brak podjęcia takich działań przez administratora był również powodem nałożenia kary na wspólnotę mieszkaniową.

Wspólnota nie zawarła też umowy powierzenia przetwarzania danych z zarządcą wspólnoty. Administrator nie dokonał również weryfikacji podmiotu przetwarzającego przed powierzeniem temu podmiotowi danych osobowych członków wspólnoty do przetwarzania.

Decyzja dostępna jest tutaj

3. Brak współpracy z organem nadzorczym naraża administratora/podmiot przetwarzający na karę finansową

Do zadań organu nadzorczego należy m.in. monitorowanie i egzekwowanie stosowania przepisów RODO na swoim terytorium. W celu realizacji tych zadań, organowi nadzorczemu przyznano wiele uprawnień, w tym prawo do uzyskania od administratora oraz podmiotu przetwarzającego dostępu do wszelkich danych i niezbędnych informacji, dostępu do pomieszczeń, sprzętu i środków służących do przetwarzania danych. Brak współpracy administratora/podmiotu przetwarzającego z organem nadzorczym podlega sankcjom finansowym, w sytuacji kiedy brak takiej współpracy utrudnia organowi szybkie i wnikliwe rozpatrzenie sprawy.

Brak współpracy z organem nadzorczym może przybierać różne formy, najczęściej jednak spotykane jest nieodbieranie kierowanej do administratora/podmiotu przetwarzającego korespondencji czy pozostawienie takiej korespondencji bez odpowiedzi.

Przykładowe decyzje, w których PUODO nałożył administracyjne kary finansowe w tym zakresie, dostępne są tutaj.:

- Decyzja
- Decyzja
- Decyzja

4. Prywatne nośniki wykorzystywane do przetwarzania danych u administratora danych

PUODO nałożył karę pieniężną w wysokości 30.000,00 złotych na Sąd Rejonowy Szczecin-Centrum w Szczecinie ze względu na niewdrożenie odpowiednich środków bezpieczeństwa do przetwarzania danych przy użyciu przenośnych pamięci.

W ww. Sądzie doszło do naruszenia ochrony danych w postaci zgubienia trzech nośników danych zawierających dane osobowe, w tym dwóch nośników prywatnych, które nie były zaszyfrowane.

Jak się okazało, pomimo istniejącego zakazu używania prywatnych nośników, administrator nie nadzorował przestrzegania zakazu przez pracowników oraz nie wdrożył odpowiadających zakazowi środków technicznych (np. blokady portów USB). Administrator powinien był zweryfikować sposób realizacji środka organizacyjnego w postaci zakazu użytkowania prywatnych nośników danych.

PUODO podkreślił, że nośniki danych powinny być weryfikowane przez dział IT i zabezpieczane przez nieuprawnionym dostępem osób trzecich (w szczególności w przypadku ich zgubienia).

Niewdrożenie powyższych środków doprowadziło do naruszenia ochrony danych osobowych.

Decyzja dostępna jest tutaj

CIEKAWOSTKI

Włoski organ nadzorczy pierwszy zajął się Chatem GPT

ChatGPT - komunikator opracowany przez firmę OpenAI, który jest zdolny odpowiadać na pytania, używając naturalnego, ludzkiego języka, a także może naśladować inne style pisania, korzystając z Internetu jako swojej bazy danych, bije kolejne rekordy popularności. Tymczasem Włochy stały się pierwszym państwem UE, który w marcu 2023 r. za skutkiem natychmiastowym zablokował jego funkcjonowanie na terenie swojego kraju.
Włoski organ ochrony danych stwierdził bowiem, że istniały obawy dotyczące prywatności związane z modelem działania ChatGPT w tym:

- Brak odpowiednich informacji wyjaśniających jakie dane są gromadzone przez OpenAI;
- Brak wystarczającej podstawy prawnej uzasadniającej masowe gromadzenie i przechowywanie danych osobowych w celu "szkolenia" algorytmów leżących u podstaw działania platformy;
- Mimo ze usługa jest skierowana do osób w wieku powyżej 13 lat, nie zastosowano żadnego narzędzia weryfikującego wiek użytkowników.

Tym samym organ nadzorczy wezwał OpenAI do podjęcia stosowanych działań naprawczych. Twórcy ChatGPT nie zwlekali z poprawkami. Wprowadzono m.in. nową politykę prywatności oraz tryb „incognito". Ponadto, użytkownicy są informowani, że aktywacja konwersacji oznacza potwierdzenie, że użytkownik ma ukończone 13 lat i posiada zgodę rodziców na korzystanie z usługi. Serwis wymaga również podania daty urodzenia podczas rejestracji.

Warto zwrócić uwagę, na zakres wprowadzonych ulepszeń w zakresie prywatności, współpracę z regulatorem oraz tempo prac. W rezultacie od 27 kwietnia 2023 r. ChatGPT został ponownie udostępniony we Włoszech. Z drugiej strony, powyższe pokazuje że nie zawsze wszystkie istotne kwestie są uwzględnianie na etapie projektowania rozwiązania zgodnie z zasadą privacy by design i zwłaszcza w tak istotnych przypadkach, szybka reakcja regulatora pozwoliła na szybkie wyeliminowanie nieprawidłowości.

Niezgodne z prawem przetwarzania danych dot. zdrowia pracowników – kara fińskiego organu nadzorczego

Fiński organ nadzorczy nałożył na spółkę Viking Line Oy Abp (spółkę zarządzającą promami pasażerskimi) administracyjną karę pieniężną w wysokości 230.000,00 euro za niezgodne z prawem przetwarzanie danych dotyczących zdrowia pracowników.

Postępowanie fińskiego organu nadzorczego zainicjowała skarga byłego pracownika, który wnioskował o dostęp do swoich danych osobowych, w tym informacji o jego zwolnieniach lekarskich i informacji diagnostycznych. Według byłego pracownika, administrator od 20 lat przechowywał jego dane dotyczące zdrowia w systemie kadrowym. Dodatkowo, według skarżącego niektóre zapisane informacje o diagnozach były nieprawidłowe, ponieważ nie było możliwe wprowadzenie do nich wszystkich kodów diagnoz. Skarżący, pomimo złożonego wniosku nie otrzymał wszystkich swoich danych osobowych przechowywanych w systemach byłego pracodawcy.

Zgodnie z fińską ustawą o ochronie danych osobowych, zapisywanie informacji o diagnozach w połączeniu z innymi danymi dotyczącymi zatrudnienia jest niezgodne z prawem.

W ocenie fińskiego organu nadzorczego administrator ma prawo przetwarzać w systemie kadrowym informacje o tym, kiedy i jak długo pracownik był nieobecny w pracy z powodu choroby (dopuszczalny powód, wypłata wynagrodzenia chorobowego). Jednak w powiązaniu z systemem kadrowym nie powinny być przechowywane informacje o przyczynie absencji chorobowej, np. choroby, urazy, informacje diagnostyczne. Informacje o stanie zdrowia muszą być przechowywane oddzielnie od innych danych osobowych dotyczących pracownika. Dane dotyczące zdrowia powinny być natychmiast usuwane, gdy ich przechowywanie przestało być już niezbędne. Fiński organ nadzorczy stwierdził, że nieprawidłowe informacje o diagnozach były przechowywane za długo i mogły stanowić zagrożenie dla ochrony prawnej osoby fizycznej. Administrator nie podjął działań, aby zapewnić, że przechowywane przez niego dane są dokładne i wolne od błędów. Dodatkowo, Viking Line Oy Abp nie poinformował swoich pracowników w odpowiedni sposób o przetwarzaniu ich danych osobowych.

Decyzja dostępna jest tutaj

Wysoka kara dla WhatsApp Ireland za naruszenie ochrony danych – irlandzki organ nadzorczy

Platforma WhatsApp Ireland została ukarana przez irlandzki organ nadzorczy (Data Protection Commission – DPC) administracyjną karą pieniężną w wysokości 5,5 mln euro w wyniku wiążącej decyzji Europejskiej Rady Ochrony Danych w sprawie rozstrzygania sporu z dnia 5 grudnia 2022 r.

Spór w niniejszej sprawie dotyczy przede wszystkim podstawy prawnej na jakiej oparł się WhatsApp Ireland przetwarzając dane osobowe użytkowników w następstwie aktualizacji warunków świadczenia usług przez tą platformę w 2018 r. W ocenie WhatsApp Ireland użytkownik akceptując zaktualizowane warunki świadczenia usług zawarł umowę z WhatsApp Ireland, a zatem podstawą prawną przetwarzania danych osobowych jest art. 6 ust. 1 lit. b) RODO. W ocenie skarżącego (użytkownika z Niemiec) WhatsApp Ireland opierał się na zgodzie jako podstawie przetwarzania danych osobowych (podczas aktualizacji warunków użytkownicy byli poproszeni o kliknięcie „Zgadzam się i kontynuuj").

W związku ze zgłoszeniem, przez kilka z zainteresowanych organów nadzorczych, sprzeciwu (na mocy art. 60 ust. 4 RODO) do projektu decyzji przedstawionej przez DPC w niniejszej sprawie – sprawa została przekazana do rozstrzygnięcia EROD (na mocy art. 65 RODO). EROD stwierdził, że WhatsApp Ireland generalnie nie może powołać się na umowę jako podstawę prawną dla przetwarzania danych osobowych. W konsekwencji EROD poleciła irlandzkiemu organowi nadzorczemu uwzględnić naruszenie art. 6 ust. 1 RODO oraz naruszenie zasady rzetelności z art. 5 ust. 1 lit. a) RODO.

Decyzja DPC oraz EROD dostępne są tutaj

Przetwarzanie danych w działalności reklamowej – hiszpański kodeks postępowania w branży reklamowej

Od 28 stycznia 2023 r. w Hiszpani obowiązuje kodeks postępowania dla podmiotów zajmujących się działalnością reklamową zatwierdzony przez hiszpański organ nadzorczy (Agencia Española de Protección de Datos – AEPD). Kodeks postępowania AUTOCONTROL (Association for the Self-Regulation of Commercial Communication) „Przetwarzanie danych w działalności reklamowej" koncentruje się przede wszystkim na rozpatrywaniu skarg podmiotów danych na działalność przedsiębiorców związaną z niezamówioną reklamą (spamem).

Jedną z najczęstszych podstaw skarg składanych do AEPD jest właśnie spam. Składanie skarg za pośrednictwem AUTOCONTROL pozwoli na szybsze rozpatrywanie skarg w ramach procedury mediacyjnej mającej zastosowanie do przetwarzania danych w celach reklamowych. W kodeksie przewidziano dobrowolną i bezpłatną mediację. Procedura mediacyjna ma trwać 30 dni. Przedstawiciel administratora ma 15 dni na przedstawienie rozwiązania ugodowego. W przypadku niepowodzenia procedury mediacyjnej skarga zostanie przekazana do organu nadzorczego.

Kodeks jest dostępny tutaj

Czy imię naszego psa stanowi nasze dane osobowe?

W większości przypadków – nie.

Niemniej jednak, brytyjski organ ochrony danych osobowych (Information Commissioner's Office, ICO) wydał decyzję, z której wynika że w określonych przypadkach imię zwierzęcia może stanowić dane osobowe właściciela.

Rozważania dotyczyły wniosku o udostępnienie danych psa policyjnego. Wniosek ten złożyła osoba poszkodowana przez tego psa i dotyczył on m.in. imienia psa oraz jego opiekuna oraz akta policyjne psa, dokumentacji z jego szkolenia itp.

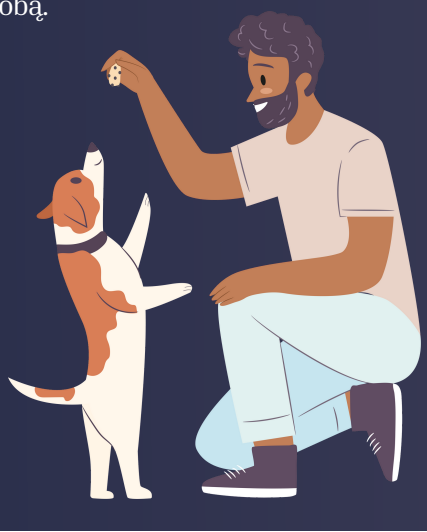
W rozważanej sprawie wpisanie imienia psa w wyszukiwarce internetowej ujawniało imię jego opiekuna psa (dane te były umieszczane w artykułach prasowych znajdujących się w sieci). Ze względu na możliwość zidentyfikowania w tym przypadku opiekuna przez dane psa, stwierdzono że imię to stanowi dane osobowe.

Organ stwierdził, że ocena byłaby taka sama w przypadku osób z pracy opiekuna którzy – nawet jeżeli ww. informacje nie byłyby publiczne – wiedzieliby kto posiada konkretnego psa po ujawnieniu im informacji o jego imieniu. W omawianych sytuacjach imię psa identyfikowało jego opiekuna pośrednio (dane osobowe to informacje pozwalające zarówno na bezpośrednią jak i pośrednią identyfikację osoby, której dane dotyczą).

Decyzja ta dotyczy jednak wyjątkowej sytuacji, w której dane psa i opiekuna były ujawnione online, a imię psa policyjnego wskazywało konkretnie jego przewodnika i umożliwiało jego zidentyfikowanie przez innych pracowników Policji. Należy także zauważyć, że inne informacje dotyczące psa nie pozwalały na zidentyfikowanie jego opiekuna, a zatem nie zakwalifikowano ich jako dane osobowe.

W naszej ocenie podejście to nie uzasadnia ogólnego przyjęcia że imię zwierzęcia będzie stanowiło dane osobowe jego właściciela czy opiekuna. W większości sytuacji dane zwierząt nie będą stanowiły danych osobowych właścicieli, gdyż nie pozwalają nawet na pośrednią identyfikację. Należy o tym pamiętać, ponieważ po wydaniu omawianej decyzji zaczęto rozpowszechniać uproszczone wnioski sugerujące iż wskutek ww. decyzji do wszystkich imion zwierząt należy również stosować przepisy o ochronie danych osobowych.

Omawiania decyzja podkreśla jak ważne jest uwzględnienie kontekstu konkretnej sprawy podczas oceny, czy konkretne informacje stanowią dane osobowe oraz jak bardzo skomplikowane może być stwierdzenie, czy dana informacja stanowi dane osobowe, czy nie. ICO nie stwierdził bowiem, że imię zwierzęcia jest zawsze danymi osobowymi jego właściciela/opiekuna. Konkretne okoliczności będą determinowały ocenę w tym zakresie. Taka sama zasada dotyczy oceniania wszystkich innych informacji, które mogą być powiązane z konkretną osobą.



AUTORZY:

Agata Szeliga
Partner, radca prawny
agata.szeliga@skslegal.pl
+48 698 660 648

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

Maciej Jakubowski
Prawnik, radca prawny
maciej.jakubowski@skslegal.pl
+48 882 630 942

Agnieszka Jurcewicz-Androsz
Prawnik, adwokat
agnieszka.jurcewicz-androsz@skslegal.pl
+48 600 782 823

Katarzyna Wnuk
Prawnik, adwokat
katarzyna.wnuk@skslegal.pl
+48 602 151 178

www.skslegal.pl