



RODO podsumowanie roku 2021

Powoli staje się tradycją to, że jeden ze styczniowych artykułów na naszym blogu poświęcamy tematowi najważniejszych RODO-wydarzeń, które miały miejsce w roku poprzednim.

Jak pod tym kątem prezentował się rok 2021? Czy był on przełomowy? Czy przyniósł administratorom i podmiotom przetwarzającym więcej pytań czy, mimo wszystko, odpowiedzi?

Poniżej przedstawiamy nasz subiektywny ranking **5 najważniejszych wydarzeń z zakresu ochrony danych osobowych**, które miały miejsce w 2021 roku.

#1 COVID-19, czyli szczepienia i certyfikaty

Ten temat był przez nas wymieniany jako jedno z [najważniejszych wydarzeń roku 2020](#). Wszyscy po cichu liczyliśmy, że w roku 2021, nie będzie już potrzeby pisania o COVID-19. Tak się niestety nie stało. RODO zostało wciągnięte we wciąż toczący się spór antyszczepionkowców ze zwolennikami szczepień. Przepisy Rozporządzenia dostarczyły wielu argumentów przeciwnikom udostępniania informacji o szczepieniu czy wynikach testów na obecność koronawirusa.

RODO daje możliwość weryfikacji szczepienia czy testu np. przez pracodawcę. Jednak w takim przypadku powinny zostać wprowadzone specjalne przepisy o randze ustawowej. W wielu krajach (np. w Polsce) takie przepisy nie zostały jednak uchwalone do dzisiaj (stan na 18 stycznia 2022 r.). W związku z tym pracodawcy, którzy chcą weryfikować pracowników pod kątem COVID-19, wciąż nie wiedzą czy mogą robić to legalnie.

Brak pewności co do prawa w tym zakresie stwarza realne problemy i generuje konflikty. Wszyscy czekamy na ustawę, bądź jednoznaczną deklarację rządu, że taki akt prawny nie powstanie. Zdecydowanie więcej na ten temat napisaliśmy w jednym z [naszych artykułów](#).

Warta odnotowania jest rola Rozporządzenia w kontekście udostępniania informacji związanych z zapobieganiem COVID-19. W obrębie całego EOG, środki zapobiegawcze nie ingerują tak mocno w prywatność jednostek, jak np. w części państw azjatyckich.

#2 Cookies, czyli jak zjeść ciasteczko i mieć ciasteczko

Można odnieść wrażenie, że z każdym kolejnym miesiącem poprzedniego roku, temat cookies w kontekście przetwarzania danych osobowych wybrzmiewał coraz bardziej. Okazało się, że te niewielkie pliki tekstowe zapisywane przez przeglądarkę w pamięci urządzenia końcowego, potrafią sporo namieszać.

W szczególności temat cookies ożył wraz z [decyzją Prezesa UODO wydaną pod koniec roku 2021](#). Organ rozstrzygnął w niej, że użytkownik musi wyrazić zgodę na cookies w sposób aktywny. Nie może to być zgoda bierna udzielona jedynie poprzez ustawienie przeglądarki internetowej.





Co prawa aktywnej zgody w niektórych państwach Europy wymaga się już od kilku lat. W Polsce obowiązuje jednak art. 173 ust. 2 Prawa telekomunikacyjnego, który dopuszcza wyrażenie zgody na instalowanie plików cookies przez ustawienia przeglądarki. Prezes UODO w swojej decyzji powołał się jednak na warunki zgody wskazane w art. 4 pkt 11 RODO. Czy doszło zatem do pomieszczenia dwóch rodzajów zgód, tj. zgody na instalowanie plików cookies ze zgodą na przetwarzanie danych osobowych?

Czy pliki cookies w ogóle mogą być uznawane za dane osobowe? A jeżeli tak to przez kogo? Niestety, rok 2021 nie przyniósł jednoznacznej odpowiedzi na te pytania. Na pewno jednak jeszcze wyraźniej je oraz związane z nimi problemy zaakcentował.

Niestety, w zakresie funkcjonowania plików cookies w Polsce, wciąż mamy do czynienia z dwoma reżimami prawnymi (RODO i Prawo telekomunikacyjne). Wciąż również czekamy na e-Privacy, które ma kompleksowo uregulować kwestie m.in. pozyskiwania danych z urządzeń użytkowników (np. właśnie poprzez mechanizm cookies) i zastąpić obecne rozwiązania.

Pozostaje mieć nadzieję, że rok 2022 przyniesie nam w tym temacie więcej odpowiedzi.

#3 Nowe standardowe klauzule umowne, czyli lepiej późno niż wcale

Ponad trzy lata czekaliśmy na decyzję Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych do państw trzecich, która uwzględniałaby postanowienia RODO. Przez ten czas, administratorzy i podmioty przetwarzające musieli pracować na klauzulach, których treść odwoływała się do uchylonej przez RODO dyrektywy 95/46/WE.

[4 czerwca 2021 r. Komisja Europejska przyjęła, aż dwa zestawy standardowych klauzul umownych](#) (ang. *standard contractual clauses*, SCC) – [jeden do przekazywania danych osobowych do państw trzecich](#), a [drugi do stosowania pomiędzy administratorami a procesorami](#).

SCC w końcu zostały dostosowane do przepisów RODO, a także uwzględniają treść wyroku Trybunału Sprawiedliwości UE [w sprawie Schrems II](#). Poprzednie SCC nie mogą być już wykorzystywane dla nowych transferów danych. Natomiast przeniesienie transferów danych osobowych ze starych na nowe SCC powinno nastąpić do 27 grudnia 2022 r.

Pozostając jeszcze w temacie transferów danych do państw trzecich, warto odnotować fakt, że 28 czerwca 2021 r. Komisja Europejska przyjęła [decyzję wykonawczą stwierdzającą odpowiedni poziom ochrony danych osobowych w Wielkiej Brytanii](#).

Można zatem uznać, że rok 2021 w zakresie transferów danych do państw trzecich był dość łaskawy – administratorzy i podmioty przetwarzające otrzymały narzędzia, z których mogą korzystać przekazując dane poza EOG.

#4 Kary finansowe UODO, czyli co z tymi naruszeniami?

W 2021 roku, UODO wydał 12 decyzji, na mocy których nałożył kary finansowe na łączną kwotę prawie 0,5 mln EUR. W stosunku do roku 2020 mamy o jedną karę finansową więcej. Ich łączna





suma jest jednak dużo niższa (o ponad 300 tys. EUR). Być może taki trend (więcej kar, ale o mniejszej wysokości) utrzyma się w roku bieżącym.

Połowa z decyzji nakładających kary finansowe (równo 6) dotyczyła nieprawidłowości w wypełnianiu obowiązków związanych z zawiadomieniami o naruszeniu ochrony danych osobowych. Administratorzy nie kwapili się do zgłaszania naruszeń do UODO, jak również mieli wyraźny problem z informowaniem o nich osób, których dane dotyczą. Decyzje UODO w tym zakresie pokazały, że niejednokrotnie gorsze od samego naruszenia, jest jego zamieszczenie pod dywan.

Kary finansowe pojawiły się również w kontekście uchybienia obowiązkowi wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. W tych przypadkach, organ zwracał szczególną uwagę na tematy związane z Security IT i analizą ryzyka. Zdaniem UODO, zastosowanie środków technicznych bez dokonania uprzedniej analizy ryzyka dla procesu przetwarzania danych osobowych nie może dawać gwarancji, że zastosowane środki będą skuteczne i adekwatne.

Warto w tym miejscu wspomnieć również o decyzjach UODO, które co prawda nie wiązały się z karami finansowymi, ale wzbudziły wiele kontrowersji. Taką decyzję wskazaliśmy już w #2, natomiast drugą z nich jest decyzja, na mocy której [organ nałożył karę jednocześnie na administratora i procesora](#).

Sprawa dotyczyła sytuacji, w której pewna firma (administrator) zleciła innej firmie (procesorowi) działania windykacyjne w stosunku do swojego dłużnika. Poszukując kontaktu telefonicznego oraz e-mailowego, firma popełniła błąd i zaczęła nękać postronną osobę. Osoba ta złożyła skargę do UODO. UODO nałożył karę upomnienia zarówno na administratora, jak i procesora – za brak przesłanki przetwarzania danych osobowych. Na nic zdały się tłumaczenia procesora, że w jego przypadku taką podstawą była umowa zawarta z administratorem. Wielu ekspertów decyzję tę uznało za niebezpieczny precedens.

Pokazuje to, jak wiele aspektów stosowania RODO wciąż nie doczekało się jednoznacznej interpretacji.





Wsparcie przy RODO naruszeniu



Jeśli właśnie mierzysz się z trudną sytuacją, jaką jest RODO naruszenie, pomożemy Ci. Być może wyzwanie z którym się mierzysz, wcale nie jest tak poważne, jak Ci się wydaje. Albo odwrotnie, sytuacja, która wydaje się być błaha, wymaga szybkich i zdecydowanych działań z Twojej strony. Daj sobie pomóc. Nasz ekspert pozwoli Ci urealnić sytuację w której się znajdujesz.

W toku naszej pracy wspieraliśmy organizacje przy ponad 50 naruszeniach RODO.

Koszt konsultacji: 300 zł netto / h.

Wypełnij poniższy formularz i zgłoś potrzebę konsultacji przy naruszeniu (dyżurujemy również w weekendy, odpowiemy w ciągu maksymalnie 2 godzin).

FORMULARZ

#5 Wyroki WSA, czyli krótki przegląd orzecznictwa

Trzeba przyznać, że z każdym rokiem, liczba orzeczeń WSA odnoszących się do zagadnień związanych z przetwarzaniem danych osobowych, rośnie. Na pewno przyczynia się do tego sam UODO, wydając coraz więcej decyzji (nie tylko tych nakładających kary finansowe), od których wiele administratorów się odwołuje.

Które wyroki z roku 2021 zapadły nam w pamięć? Przede wszystkim te, w których WSA nie przyznaje racji organowi nadzorcemu. W 2021 roku WSA uchyliły decyzje UODO, nakładające kary na: Virgin Mobile, Cyfrowy Polsat oraz [ID Finance](#). W tym ostatnim przypadku, sąd wprost wskazał, że administrator danych nie zawsze jest winien wycieku danych osobowych.

Na uwagę zasługują również te wyroki WSA stojące w opozycji do przyjętej praktyki wyznaczenia terminów retencji danych osobowych w oparciu o okresy przedawnienia roszczeń. We wskazanych orzeczeniach, sąd zgodził się z argumentacją podniesioną w decyzjach UODO i za niedopuszczalne uznano przetwarzanie danych na podstawie art. 6 ust. 1 lit. f) RODO, w celu zabezpieczenia się przed ewentualnymi, niepewnymi roszczeniami. Zdaniem sądu nie ma potrzeby przechowywania danych „na zapas”, bowiem w razie ewentualnego sporu i tak dane te zostaną przekazane zainteresowanym stronom.

W zakresie tych wyroków zapraszamy do zapoznania się ze [stanowiskiem Związku Firm Ochrony Danych Osobowych](#).





Podsumowanie

Czy rok 2021 obfitował w wielkie, wręcz przełomowe wydarzenia na miarę rozpoczęcia stosowania RODO (rok 2018 r.) czy też wyroku Schrems II (rok 2020)? Niekoniecznie. Niemniej, z perspektywy branży ochrony danych osobowych, wydarzyło się dużo. Kolejne decyzje, kolejne wyroki i kolejne tematy rodzące wątpliwości interpretacyjne dostarczyły sporo pracy nie tylko branżowym ekspertom, ale przede wszystkim administratorom, procesorom i inspektorom ochrony danych.

A jakie są Wasze wrażenia w tym zakresie?

Autor artykułu:

Lex Artist

