Własność intelektualna, technologie informacyjne i ochrona danych

Wdrożenie i egzekwowanie RODO po upływie roku

Maj 2019 r.

Paneuropejska analiza porównawcza obejmująca m.in. naruszenia i sankcje

Jednym z najczęściej powtarzanych faktów dotyczących RODO jest wprowadzenie możliwości nałożenia surowych kar pieniężnych za naruszenie przepisów, sięgających 4 mln EUR lub 4% ogólnoświatowego obrotu ukaranego podmiotu. We współpracy z czołowymi ekspertami Andersen Global przedstawiamy krótką analizę porównawczą w zakresie nakładanych kar i sankcji w wybranych krajach europejskich w pierwszym roku obowiązywania RODO.

Francja

Francuski organ nadzorczy - *Commission Nationale de l'Informatique et des Libertés* (CNIL), decyzją nr SAN 2019-001 ze stycznia 2019 r. nałożył na Google LLC karę w wysokości 50 milionów euro. Była to pierwsza decyzja wydana na podstawie przepisów RODO i do chwili obecnej jest to najwyższa kara nałożona z tytułu naruszenia przepisów RODO.

CNIL uznał, że Google naruszyła wynikające z RODO zobowiązania, dotyczące przejrzystości informacji, gdyż podawane informacje były *„rozdzielone na kilka dokumentów"*, co uniemożliwiało użytkownikowi dogłębne zapoznanie się z ich treścią. CNIL stwierdził ponadto, że Google nie wywiązuje się z obowiązku wykazania podstawy prawnej do przetwarzania danych w zakresie personalizacji reklam oraz nie posiada prawidłowo uzyskanej zgody użytkowników.

Google odwołał się od decyzji , twierdząc między innymi, że CNIL nie ma jurysdykcji nad Google LLC. Google LLC uznaje, że centrala w Irlandii stanowi jego główną jednostkę w Europie i że jedynym właściwym organem jest irlandzka Komisja ds. ochrony danych. Sprawa jest nadal w toku.

Hiszpania

Od czasu wprowadzenia RODO w Hiszpanii odnotowano pewne zmiany. Nowa ustawa o ochronie danych osobowych (LOPDGDD), w której rozwinięto niektóre aspekty RODO, została przyjęta w grudniu 2018 r.

W 2018 r. liczba skarg wniesionych do hiszpańskiego organu nadzorczego przez osoby, których dane dotyczą, wzrosła o 33% w porównaniu z rokiem poprzednim. Zaangażowanie organu na rzecz zwiększania świadomości oraz ukierunkowania i wsparcia wdrożenia RODO było ogromne; udostępniono również narzędzia wspierające i wytyczne dotyczące przetwarzania danych osobowych.

Od chwili wejścia w życie przepisów RODO nie nałożono w Hiszpanii jakichkolwiek sankcji. Organ nadzorczy skupiał się raczej na analizie naruszeń i wysyłaniu ostrzeżeń do poszczególnych firm. Dotyczy to w szczególności dwóch decyzji, dotyczących szkół oraz danych osobowych i zdjęć uczniów. W tych przypadkach organ wziął pod uwagę starania obu szkół w zakresie środków ochrony danych podjętych przed wystąpieniem zdarzenia związanego z ochroną danych, jak i po jego wystąpieniu.

Niemcy

Od czasu wejścia w życie Europejskiego Ogólnego Rozporządzenia o Ochronie Danych (RODO) w maju 2018 r., niemieckie organy do spraw ochrony danych nałożyły 75 kar pieniężnych związanych z RODO. Łączna kwota tych kar wyniosła 449.000 EUR.

Najwyższa kara pieniężna w Niemczech wyniosła 80.000 EUR i została nałożona w wyniku wycieku danych dotyczących zdrowia na skutek nieodpowiednich mechanizmów kontroli wewnętrznej. W innym przypadku komisarz ochrony danych w Berlinie nałożył karę pieniężną w wysokości 50.000 EUR na bank, który przetwarzał dane byłych klientów, co do których nie uzyskał jednak zgody na przetwarzanie. W innej sprawie niemiecka sieć społecznościowa musiała zapłacić karę pieniężną w wysokości 20.000 EUR za przechowywanie niezaszyfrowanych danych użytkowników na starych serwerach.

Ogólnie rzecz biorąc, kary pieniężne mieściły się w granicach zdrowego rozsądku. Z drugiej strony można się spodziewać, że w 2019 r. nałożone zostaną kolejne sankcje. Niektóre organy ds. ochrony danych w Niemczech już zapowiedziały prowadzenie niezapowiedzianych kontroli oraz zwiększenie liczby pracowników uprawnionych do przeprowadzenia kontroli.

Dodatkowo, można potwierdzić, że świadomość na temat ochrony danych w Niemczech znacznie wzrosła. Firmy „uprzątnęły" swoje bazy danych, dokonały przeglądu swoich procesów ochrony danych oraz dostosowały te procesy do wymogów RODO.

Mniejsze niemieckie firmy i stowarzyszenia skarżą się jednak na wysoki poziom biurokracji, w szczególności w zakresie zobowiązań dotyczących informacji i dokumentacji. Nawet federalny komisarz ds. ochrony danych w Niemczech w swoim dorocznym raporcie podnosi tezę możliwości zmniejszenia wydatków administracyjnych dla małych przedsiębiorstw i stowarzyszeń.

Austria

Od czasu wdrożenia RODO w Austrii nastąpiły zauważalne, ale nie dramatyczne zmiany. Szybko wrosła liczba skarg w okresie od 2017 r. do 2018 r., gdyż ich ilość co najmniej potroiła się. Z drugiej strony najwyższa kara nałożona dotychczas w Austrii wyniosła 4800 EUR, i można ją określić mianem rozsądnej.

Ale uwaga! Chociaż wysokość kar nie zwala z nóg, można zauważyć zmianę w podejściu organu nadzorczego. Wymogi, jakie organ nakłada na administratorów danych, widocznie wzrosły, w szczególności w zakresie standardów bezpieczeństwa (zwłaszcza w branży opieki zdrowotnej), jak i wymogów informacyjnych oraz formalnych wymogów uzyskania zgody na przetwarzania danych i wykonywania nagrań wideo. W praktyce biznesowej setki nieważnych zgód mogą być bardziej

dolegliwe niż sama kara pieniężna, gdyż uniemożliwiają zgodne z prawem wykorzystywanie stosownych danych; ponadto osoby, których dane dotyczą mogą wystąpić z roszczeniami odszkodowawczymi. Ostatnie decyzje pokazują, że nie należy spodziewać się dalszego istnienia stosowanej dotychczas w Austrii praktyki „konsultacji zamiast kary", pierwotnie obiecywanej przez polityków. Obecny czas to ostatni dzwonek na zapewnienie zgodności z RODO.

Polska

Od czasu wejścia w życie RODO można zauważyć zwiększoną aktywność polskiego organu nadzorczego. W tym okresie organ (Prezes Urzędu Ochrony Danych Osobowych) opublikował obszerne wytyczne dla administratorów oraz ogłosił plan kontroli na 2019 rok. Plan obejmuje głównie podmioty publiczne, sektor finansowy oraz firmy telemarketingowe. Organ nadzorczy zapowiedział, że szczególną uwagę będzie zwracać na monitoring wideo oraz rekrutację pracowników.

Dotychczas w Polsce nałożono dwie kary pieniężne. Pierwsza, w wysokości niemal 1 mln PLN (ok. 230 tys. EUR), została nałożona na przedsiębiorstwo, które w swojej działalności wykorzystywało dane osobowe polskich przedsiębiorców. Dane były zbierane i prezentowane na stronie internetowej spółki, przy czym osoby, których dane dotyczą, nie były o tym informowane w sposób przewidziany w art. 14 RODO. Drugi przypadek dotyczył związku piłkarskiego, który na swojej stronie internetowej opublikował nazwiska, adresy oraz indywidualne numery identyfikacji 585 licencjonowanych sędziów. Kara pieniężna wyniosła 55 tys. PLN (ok. 13 tys. EUR) i o jej wysokości zdecydowała dobra współpraca z organem w trakcie kontroli, wykonanie zaleceń organu oraz fakt, że żaden z sędziów nie odniósł szkody. Nie były to jedyne naruszenia stwierdzone przez organ nadzorczy, jednak w przypadku pozostałych naruszeń nie nałożono kar.

W maju 2018 r. RODO wywołało wiele obaw pośród polskich przedsiębiorców. Jednocześnie znacznie zwiększyła się świadomość organów publicznych, przedsiębiorców i konsumentów na temat kwestii związanych z ochroną danych osobowych. RODO miało pozytywny wpływ na sektor MŚP – podmioty te podchodzą teraz ostrożniej do przetwarzania danych i dokładają większych starań, aby zapewnić zgodność z obowiązującymi przepisami.

W Polsce pojawiły się też skutki uboczne, przede wszystkim RODO-trolling. Pojawiają się Polskie żądania dotyczących danych osobowych, przesyłane przez osoby liczące na wykrycie naruszenia i znalezienie powodu do żądania wypłaty odszkodowania. Według naszej najlepszej wiedzy, dotychczas takie próby okazywały się nieskuteczne.

Włochy

We Włoszech upłynęło zaledwie kilkanaście dni od chwili pełnego stosowania nowego systemu kar przewidzianego przez RODO.

Chociaż RODO weszło w życie 25 maja 2018 r., Włochy zapewniły sobie „okres przejściowy" na podstawie art. 22 ust. 13 dekretu ustawodawczego nr 101/2018, zgodnie z którym w pierwszych ośmiu miesiącach, licząc od września 2018 r., włoski organ nadzorczy nie nałoży żadnych kar związanych z RODO. Ten „okres przejściowy" upłynął 19 maja.

W 2018 r. według raportu Prezesa włoskiego organu nadzorczego, praca organu skupiała się na kwestiach związanych ze szkodliwym oprogramowaniem, aspektami prawa pracy, cyberbezpieczeństwem, ochroną zdrowia, wystawianiem faktur elektronicznych i telemarketingiem.

Węgry

Od czasu wejścia RODO w życie, węgierski organ nadzorczy (NAIH) nałożył kary pieniężne w przedziale 500.000 - 1.000.000 HUF (ok. 1500 - 3000 EUR) oraz jedną karę w wysokości 11.000.000 HUF (ok. 34.000 EUR). Mniejsze kary dotyczyły naruszenia różnych wymogów w zakresie ochrony danych, m.in. nieudzielenia wystarczająco przejrzystych informacji na żądanie klienta (klient chciał wiedzieć, w jaki sposób jego dane przechowywane w kopiach zapasowych są przetwarzane i przez jaki okres), lub nieograniczenie przez administratora korzystania z numeru telefonu, gdy nowy właściciel numeru wskazał, że numer nie należy już do klienta, od którego został on pierwotnie uzyskany. W jednej decyzji wskazano, że – w kontekście pożyczki na finansowanie samochodu – używanie numeru telefonu na potrzeby egzekucji długu, czyli w celu innym niż wskazano osobie, której dane dotyczą w chwili otrzymania jej danych, stanowi rodzaj przetwarzania, o którym administrator powinien był powiadomić klienta, jak i jest przetwarzaniem, które powinno być poprzedzone testem równowagi przeprowadzonym specjalnie w tym celu. W ocenie organu ogólne nawiązanie do uzasadnionych interesów administratora jest niewystarczające (test równowagi musi zostać wykonany w odniesieniu do każdego celu). Z kolei przypadek, w którym NAIH nałożył karę 11.000.000 HUF (ok. 34.000 EUR) dotyczył naruszenia ochrony danych 6000 osób na stronie internetowej oraz wycieku danych na temat ich opinii w sprawach politycznych; ponadto administrator nie spełnił swojego obowiązku w zakresie powiadomienia organu nadzorczego.

Grecja

Do chwili obecnej grecki organ nadzorczy wydał niewielką liczbę decyzji na podstawie przepisów RODO. Decyzje były raczej łagodne, a organ wybierał raczej udzielenie nagany administratorom zamiast nakładania kar pieniężnych.

W trzech przypadkach dotyczących niespełnienia obowiązku powiadomienia o naruszeniu ochrony danych osobowych organ udzielił nagany, biorąc pod uwagę, że (a) RODO niedawno weszło w życie; (b) administratorzy zareagowali natychmiast i niezwłocznie oraz skutecznie zajęli się naruszeniem ochrony danych; (c) naruszenie ochrony danych dotyczyło bardzo niewielkiej liczby osób fizycznych; (d) atak hackerski, zgłoszony w jednym z przypadków, nastąpił z nieznanego źródła był bardzo zaawansowany.

W jednym przypadku dotyczącym niezgodności z obowiązkami dotyczącymi niechcianych komunikatów reklamowych organ udzielił nagany w związku z faktem, że tylko jedna osoba fizyczna złożyła skargę na otrzymywanie komunikatów reklamowych poprzez aplikację Viber bez udzielenia zgody na podstawie odpowiednich przepisów RODO. W opinii organu kluczowe znaczenie ma udzielenie osobom fizycznym odpowiednich informacji oraz jasne wskazanie celu przetwarzania danych, tj. czy prowadzone jest ono w celu wykonania umowy, czy ma charakter marketingowy.

Należy jednak zwrócić uwagę, że w porównaniu do przypadków rozstrzyganych według wcześniejszych ram legislacyjnych, wydaje się, że obecnie organ nadzorczy podejmuje bardziej surowe działania w zakresie nakładania kar pieniężnych – w pewnych sprawach osiągnęły one kwotę nawet 150.000 EUR.

Ponadto organ poinformował, że przeprowadził ponad 65 zdalnych postępowań wyjaśniających, dotyczących stron internetowych przedsiębiorstw z różnych sektorów gospodarki, których celem była weryfikacja zgodności z szeregiem zobowiązań wynikających z RODO. W wyniku kontroli organ nadzorczy wysłał zawiadomienia adresowane do administratorów, z żądaniem dostosowania operacji przetwarzania do postanowień RODO w określonym terminie, w niektórych przypadkach również poprzez podjęcie określonych działań proponowanych przez organ. W niektórych wypadkach organ zażądał również udzielenia mu dodatkowych informacji o operacjach przetwarzania danych osobowych.

Oprócz tego organ opublikował listę działań z zakresu przetwarzania danych, które w jego opinii powinny zostać poddane formalnej Ocenie Skutków dla Ochrony Danych (DPIA). Ponadto warto wspomnieć, że grecki organ ogłosił, iż od 25 maja 2018 r. do początku bieżącego roku (2019) otrzymał ponad 96.000 skarg od osób, których dane dotyczą, zarzucających naruszenie postanowień RODO. Po sprawdzeniu, jaka część z nich jest uzasadniona, organ nadzorczy wyda istotne decyzje w poszczególnych sprawach.

Na koniec należy wskazać, że Grecja nie przyjęła jeszcze przepisów obejmujących obszary pozostawione jurysdykcji Państw Członkowskich.

Rumunia

Od czasu wejścia RODO w życie w Rumunii zaszły zauważalne zmiany w zakresie ochrony prywatności danych. W 2018 r. rumuński parlament przyjął ustawę nr 190 dotyczącą niektórych z „otwartych" punktów RODO. Jednocześnie nastąpiła transpozycja dyrektyw 2016/680 i 2016/1148 do ustawodawstwa krajowego.

W zakresie prawodawstwa wtórnego / wytycznych co do najlepszych praktyk, zaangażowanie rumuńskiego organu nadzorczego jest dość niewielkie. Niektóre stowarzyszenia branżowe reprezentujące administratorów z sektora bankowości, telekomunikacji lub publikacji przedstawiły organowi do zatwierdzenia kodeksy postępowania, jednak, zgodnie z naszą wiedzą, żaden z tych kodeksów nie został jeszcze zatwierdzony. Zamiast tego organ postanowił zwiększać świadomość na poziomie nieformalnym, poprzez udział w wielu lokalnych konferencjach i wydarzeniach poświęconych RODO, organizowanych zarówno w sektorze publicznym, jak i prywatnym.

Postępowania kontrolne prowadzone przez organ ogólnie skupiały się na rozpatrywaniu skarg w związku z zarzucanymi naruszeniami prywatności danych, których ilość istotnie wzrosła od czasu wejścia RODO w życie. W 2018 r. liczba skarg złożonych po 25 maja była 2,5 razy wyższa niż liczba skarg wniesionych przed datą początkową obowiązywania RODO. Niezależnie od tego, rumuński organ wszczął również z urzędu szereg postępowań kontrolnych w wybranych sektorach gospodarki– przykładowo możemy wskazać, że tego typu postępowania toczą się już w sektorze bankowości. Ponadto organ zwraca szczególną uwagę na naruszenia bezpieczeństwa – kontrolami objęto już szereg naruszeń.

Nie wiemy jednak, jakie konkretne sankcje zostały nałożone przez organ w związku z naruszeniem przepisów RODO. Zgodnie z ogólną tendencją na poziomie UE, oczekuje się, że kary pieniężne oraz inne sankcje (w tym środki naprawcze) z tytułu niezgodności z RODO zostaną nałożone raczej wcześniej niż później.

Portugalia

Jedną z pierwszych sankcji, jaką po wejściu RODO w życie nałożono była ta, którą ukarano szpital publiczny w Barreiro, jeden z największych szpitali w regionie Lizbony. Naruszenie dotyczyło nieograniczonego dostępu do danych klinicznych. Sankcja była uzasadniona następującymi naruszeniami przepisów RODO: (a) zasady minimalizacji danych; z uwagi na to, że szpital umożliwiał nieograniczony dostęp do nadmiernej ilości danych specjalistom, którzy powinni mieć do nich wgląd jedynie w uzasadnionych przypadkach; (b) zasady integralności i poufności, z tytułu niewdrożenia środków organizacyjnych i technicznych w celu zapobieżenia nieuprawnionemu dostępowi do danych osobowych; (c) niezdolności szpitala do zapewnienia integralności, poufności, dostępności oraz stałej odporności systemów i procesów przetwarzania oraz (d) niewdrożenia właściwych środków organizacyjnych i technicznych w celu zapewnienia poziomu bezpieczeństwa stosownego do ryzyka, w szczególności środka polegającego na regularnym testowaniu, ocenie i kontroli skuteczności zabezpieczeń w przetwarzaniu danych. Portugalski organ ds. ochrony danych (CNPD) nałożył na szpital w Barreiro karę pieniężną w wysokości 400.000 EUR.

Andersen Tax & Legal | Service Line IP, IT & Data Protection

Specjalne podziękowania dla współpracowników:

> Hiszpania · Belén Arribas · belen.arribas@AndersenTaxLegal.es
> Niemcy · Dr Fritjof Börner · fritjof.boerner@AndersenTaxLegal.de
> Portugalia · Raquel Brízida Castro · raquel.castro@AndersenTaxLegal.pt
> Rumunia · Bogdan Halcu · bogdan.halcu@tuca.ro
> Grecja · Dr Themistoklis K. Giannakopoulos · themistoklis.giannakopoulos@AndersenLegal.gr
> Włochy · Francesco Inturri · francesco.inturri@andersentaxlegal.it
> Polska · Magdalena Patryas · magdalena.patryas@ksplegal.pl
> Austria · Katharina Raabe-Stuppnig · raabe@lansky.at
> Węgry · Tamás Szabó · tamas.szabo@sz-k-t.hu
> Francja · Angélique Vibert · angelique.vibert@AndersenTaxLegal.es