Stworzyć, skontrolować, wypromować - skuteczny rozwój biznesu na wiosnę

W TYM WYDANIU:

LexDigital

www.lexdigital.pl

Natalia Dzieciuchowicz

Jak się przygotować do kontroli z Urzędu Ochrony Danych Osobowych?

Zgodnie z przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych i Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, (RODO) Prezes Urzędu Ochrony Danych Osobowych (PUODO) jest organem uprawnionym do przeprowadzania kontroli zgodności z przepisami o ochronie danych osobowych.

Uprawnienia przysługujące Prezesowi zostały wskazane przede wszystkim w art. 58 RODO i należą do nich m.in.:

- nałożenie administracyjnej kary pieniężnej (w wysokości do 20 milionów euro lub do 4% rocznego światowego obrotu),
- wprowadzenie czasowego lub całkowitego zakazu przetwarzania danych osobowych,
- nakazanie usunięcia danych,
- wydanie upomnienia,
- nakazanie poinformowania osoby, której dane dotyczą, o naruszeniu ochrony jej danych,
- zawiadomienie administratora lub podmiotu przetwarzającego o podejrzeniu naruszenia RODO.

Uprawnienia Prezesa Urzędu do przeprowadzenia kontroli wynikają też z art. 78 ust. 1 ustawy o ochronie danych osobowych.

Co wpływa na decyzję Urzędu o przeprowadzeniu kontroli?

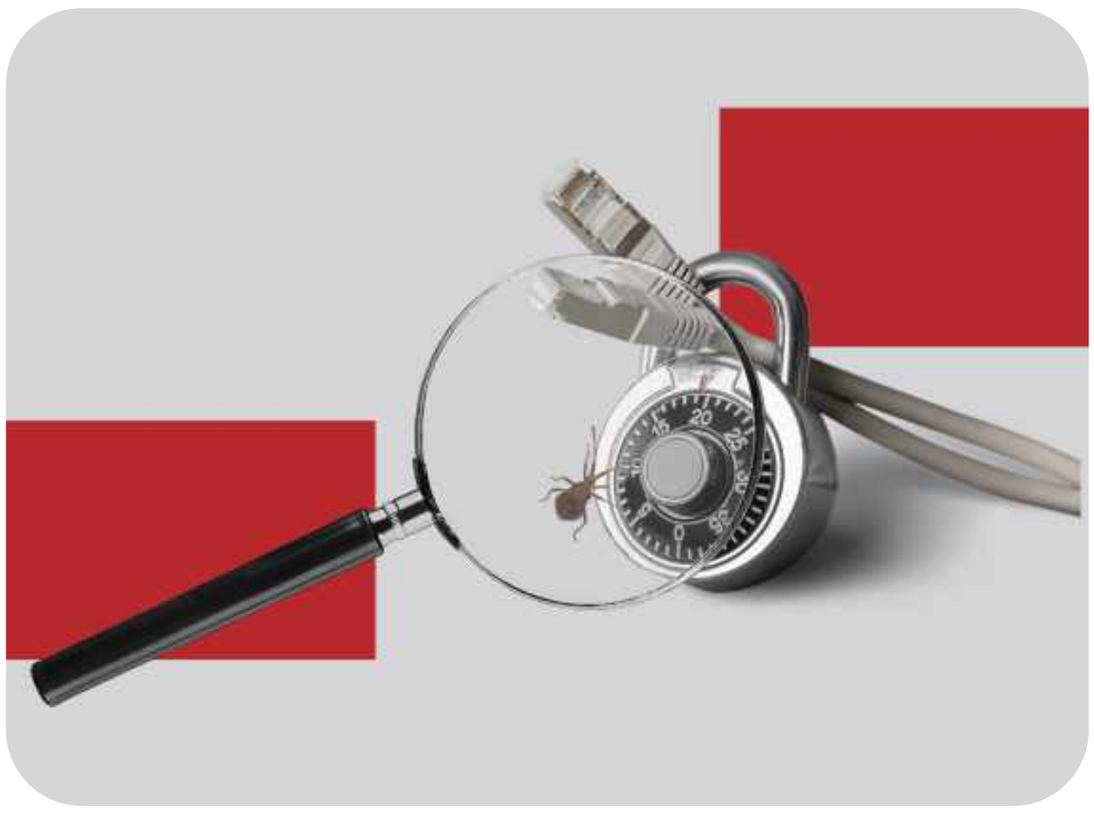
Kontrolowany podmiot może prowadzić działalność czy też wykorzystywać narzędzia, które poddawane są kontroli zgodnie z rocznym planem kontroli sektorowych Urzędu Ochrony Danych Osobowych udostępnianym na stronie www.uodo.gov.pl. (kontrola planowa);

Prezes Urzędu pozyskał określone informacje, które wpłynęły na decyzje o podjęciu działań kontrolnych (kontrola doraźna). Mogą to być np.

- skarga zgłoszona przez osobę fizyczną na niezgodne z prawem przetwarzanie danych osobowych przez administratora,
- informacja pozyskana od sygnalisty,
- inicjatywa innych organów, którym przepisy nadają uprawnienia kontrolne (sądów, prokuratur)
- informacje medialne,
- analiza zgłaszanych przez administratora naruszeń, w wyniku której Urząd podejmuje decyzję o konieczności dalszego postępowania (np. w wyniku nieprawidłowości w procesie zgłaszania naruszeń),
- kontrola wdrożonych przez administratora zaleceń Urzędu, jeżeli takie zostały wcześniej przez Urząd wydane,
- i inne.

Prezes decyduje o przeprowadzeniu kontroli wyrywkowej, zgodnie ze swoim swobodnym wyborem. Jest ona przeprowadzana w ramach spoczywającego na UODO obowiązku monitorowania przestrzegania stosowania przepisów RODO.

Z powyższych informacji wynika, że nawet jeżeli w rocznym planie kontroli przygotowanym i zatwierdzonym przez Prezesa UODO nie wymienia się działalności, którą prowadzimy, nie oznacza to, że kontrola nas ominie.



Podstawowe informacje dotyczące samej kontroli

Poniżej przedstawiamy informacje dotyczące tego, w jaki sposób, w praktyce, Urząd przeprowadza kontrole, czego spodziewać się po urzędnikach przeprowadzających kontrole, jakie zagadnienia będą ich najbardziej interesować, jak długo będzie trwała kontrola, jakie dokumenty przygotować i jak powinni być do kontroli przygotowani nasi pracownicy.

Zawiadomienie o kontroli i uprawnienia kontrolerów

Kwestią budzącą wątpliwości może być to, czy organ powinien wcześniej zawiadomić o kontroli. Przepisy ustawy o ochronie danych osobowych, jak również RODO nie regulują tej kwestii wprost. W tym kontekście można spotkać dwa podejścia. Wg pierwszego, Prezes UODO działając w stosunku do przedsiębiorców powinien zastosować przepisy ustawy - Prawo przedsiębiorców i zgodnie z jej art. 48 ust. 1 zawiadomić przedsiębiorcę o planowanej kontroli. Natomiast w przypadku, gdy podmiotem kontrolowanym nie jest przedsiębiorca, powinien zastosować tylko przepisy ustawy o ochronie danych osobowych (czyli w praktyce wystarczy okazanie upoważnienia). Drugie podejście zakłada natomiast, że kontrola prowadzona przez Prezesa UODO nie musi być poprzedzona zawiadomieniem. Wniosek ten jest oparty o treść art. 48 ust. 11 Prawa przedsiębiorców, zgodnie z którym zawiadomienia o zamiarze wszczęcia kontroli nie dokonuje się, w przypadku gdy kontrola ma zostać przeprowadzona na podstawie ratyfikowanej umowy międzynarodowej albo bezpośrednio stosowanych przepisów prawa Unii Europejskiej.

Należy pamiętać, że Inspektorzy UODO posiadają legitymacje służbowe i powinni przedstawić imienne upoważnienie do przeprowadzenia kontroli. Zdarzało się już, że podszywano się pod urzędników celem uzyskania dostępu do informacji przedsiębiorcy, starannie zatem należy zweryfikować tożsamość kontrolera. Wspomniana wyżej legitymacja powinna zawierać m.in. informacje o imieniu, nazwisku, stanowisku służbowym oraz fotografię kontrolera.

W ramach prowadzonych czynności kontrolnych kontrolujący mają prawo (na podstawie art. 84 ust. 1 ustawy o ochronie danych osobowych):

- wstępu od 6:00 do 22:00 na teren organizacji oraz do jej budynków, lokali i innych pomieszczeń,
- wglądu do dokumentów mających bezpośredni związek z przedmiotem kontroli (zakres kontroli najczęściej jest wskazany w treści zawiadomienia o kontroli i nie może on wykraczać poza wskazany w upoważnieniu),
- przeprowadzenia oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych,
- żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania świadków (np. pracowników kontrolowanego),
- zlecania sporządzenia ekspertyz i opinii.

> **Nawet jeżeli w rocznym planie kontroli przygotowanym i zatwierdzonym przez Prezesa UODO nie wymienia się działalności, którą prowadzimy, nie oznacza to, że kontrola nas ominie.**

Typowa kontrola najczęściej obejmuje weryfikację:

- podstaw prawnych przetwarzania danych osobowych,
- celów, w jakich dane są przetwarzane,
- źródeł pozyskiwania tych danych,
- kategorii osób, których dane dotyczą oraz kategorii przetwarzanych danych osobowych,
- odbiorców, którym dane są ujawniane,
- sposobu realizacji praw osób, których dane dotyczą, w tym treści klauzul informacyjnych kierowanych do poszczególnych kategorii podmiotów danych,
- zasad powierzenia przetwarzania,

- trybu nadawania upoważnień do przetwarzania danych i ich treści,
- wdrożenia polityk i procedur ochrony danych,
- czy wyznaczono inspektora ochrony danych, a jeżeli nie – przedstawienia dokumentacji argumentującej brak obowiązku powołania inspektora,
- czasu retencji danych - czy dane osobowe nie są przechowywane przez zbyt długi okres,
- zasad minimalizacji danych – czy zakres przetwarzanych danych jest adekwatny do celów przetwarzania,

- czy wdrożono środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa danych, na podstawie przeprowadzanej analiz ryzyka,
- dokumentacji potwierdzającej cykliczne przeprowadzanie analizy ryzyka (również oceny skutków dla ochrony danych) oraz stosowanie zasady Privacy by design i Privacy by default,
- czy prowadzony jest rejestr czynności przetwarzania oraz rejestr wszystkich kategorii czynności przetwarzania (jeżeli ten drugi rejestr dotyczy kontrolowanego, a więc gdy występuje on w roli podmiotu przetwarzającego dane na zlecenie innego administratora),

- czy odpowiednio dokumentowane są wszystkie naruszenia ochrony danych,
- czy pracownicy dopuszczeni do przetwarzania danych przeszli odpowiednie szkolenie w tym zakresie,
- treści zawartych umów powierzenia (jeżeli do takiego powierzenia dochodzi) i weryfikacji podmiotu przetwarzającego na zgodność przetwarzania danych z przepisami i wymaganiami administratora,
- zasad przekazywania danych do państwa trzecich i organizacji międzynarodowych.

LexDigital

Sugerujemy, aby przed rozpoczęciem kontroli skontaktować się z urzędnikiem, który będzie ją przeprowadzał, a którego dane powinny być umieszczone w treści zawiadomienia, aby pozyskać więcej informacji w przedmiocie kontroli.

Kontrola nie powinna trwać dłużej niż 30 dni i w praktyce najczęściej w siedzibie kontrolowanego trwa do kilku dni, a pozostałe czynności odbywają się już telefonicznie, mailowo i korespondencyjnie.

Jakie dokumenty przygotować przed kontrolą i kto, z ramienia organizacji, powinien w niej uczestniczyć?

Jeżeli w organizacji powołano Inspektora ochrony danych, konieczne jest zawiadomienie go o planowanej kontroli. Jeżeli organizacja nie powołała Inspektora, powinna zawiadomić inną osobę odpowiedzialną w obszarze ochrony danych osobowych. Będą to osoby najbardziej odpowiednie do wsparcia w zakresie kontroli i najlepiej zorientowane w kwestiach, których kontrola będzie dotyczyć.

Kontrolujący nie pominą najpewniej obszaru IT, warto wyznaczyć osobę odpowiedzialną za udzielanie informacji kontrolerom w tym zakresie. Kontrolerzy mogą pytać o sposoby zabezpieczenie systemów, zasady nadawania uprawnień do systemów, reakcji na incydenty, lokalizację serwerów, weryfikację dostawców usług IT i inne.

Jakub Pawłowski

Compliance: jak prowadzić marketing wobec przedsiębiorców?

Marketing z reguły kojarzy się z działaniami prowadzonymi wobec konsumentów. Świadomość organizacji w tym zakresie jest również dosyć wysoka, a działy marketingu, które w praktyce są odpowiedzialne za ten obszar, wiedzą, że legalna komunikacja z odbiorcą musi spełniać określone wymogi prawne. Co jednak z działaniami prowadzonymi wobec przedsiębiorców? Czy komunikacja marketingowa w tym zakresie musi spełniać te same wymogi co wobec konsumentów?

Akty prawne regulujące działania marketingowe

Działania marketingowe są regulowane głównie przez 3 akty prawne, tj.:

1. rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (dalej jako „**RODO**”);
2. ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (dalej jako „**UŚUDE**”);

ustawę z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (dalej jako „**PT**”).

Ogólne rozporządzenie o ochronie danych

Sprawa wygląda najprościej z punktu widzenia RODO. Jak wiadomo, przetwarzanie danych osobowych w jakimkolwiek celu, a więc również w celu prowadzenia działań marketingowych wymaga ustalenia odpowiedniej podstawy prawnej. Przykładowo, taką podstawą może być konkretny przepis prawa albo zgoda osoby, której dane dotyczą. Jedną z podstaw prawnych przetwarzania danych osobowych może być również prawnie uzasadniony interes administratora, który w praktyce oznacza możliwość przetwarzanie danych osobowych bez zgody osoby, której dane dotyczą.

I ten prawnie uzasadniony interes administratora może być właśnie podstawą działań marketingowych. Wniosek ten wynika z motywu 47 RODO, który wprost wskazuje, że: „Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego”..” I choć motywy rozporządzeń unijnych teoretycznie są jedynie wskazówkami interpretacyjnymi, a nie przepisami prawa sensu stricto, to w praktyce w istotny sposób wpływają na legalność konkretnych działań. Nie inaczej jest w przypadku bezpośrednich działań

marketingowych, które w świetle motywu 47 RODO powszechnie uznaje się za dopuszczalne w oparciu o prawnie uzasadniony interes administratora (tj. bez zgody).

Oczywiście powstaje pytanie, czy w kontekście wymogów RODO każdy rodzaj działań marketingowych i wobec każdej grupy odbiorców może być prowadzony w oparciu o prawnie uzasadniony interes? Motyw 47 wskazuje jedynie na marketing bezpośredni, który sam w sobie nie ma definicji legalnej. Wydaje się, że w kontekście RODO oparcie wszystkich możliwych działań na prawnie uzasadnionym interesie administratora jest zbyt daleko idącym uproszczeniem.

Ww. rozważania jednak wyczerpują tylko jeden aspekt prowadzenia działań marketingowych, którym jest przetwarzanie danych osobowych odbiorców.

Ustawa o świadczeniu usług drogą elektroniczną i Prawo telekomunikacyjne

Sprawę diametralnie zmieniają i utrudniają przepisy UŚUDE i PT, które, mówiąc najogólniej, wymagają zgody na prowadzenie działań marketingowych.

Zgodnie bowiem z art. 10 ust. 1 UŚUDE: „Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy będącego osobą fizyczną za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej".

Natomiast zgodnie z art. 172 ust. 1 PT: „Zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego lub przesyłania niezamówionej informacji handlowej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę".

Co ciekawe obie regulacje są powiązane z RODO, bowiem art. 4 UŚUDE i art. 174 PT wskazują, że do uzyskania uzyskanie zgody na marketing stosuje się przepisy o ochronie danych osobowych. To odniesienie oznacza, że uzyskując zgodę na działania marketingowe, należy przestrzegać wymogów art. 7 RODO w zakresie zbierania zgód. Zgoda zatem musi być rozliczalna, dobrowolna, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Ponadto, wycofanie zgody musi równie łatwe, jak jej wyrażenie.

Podsumowując powyższe, można powiedzieć, że przepisy RODO z jednej strony oraz przepisy UŚUDE i PT z drugiej strony są od siebie niezależne. Innymi słowy, to, że przepisy RODO dopuszczają przetwarzanie danych osobowych w celach marketingowych na podstawie prawnie uzasadnionego interesu administratora (tj. bez zgody osoby, której dane dotyczą), nie oznacza, że taka sama praktyka będzie dopuszczalna na gruncie UŚUDE i PT. Te przepisy nie dają bowiem żadnej możliwości działania bez zgody osoby, do której kierowane są informacje marketingowe.

Co z przedsiębiorcami?

Działalność gospodarcza może być prowadzona w różnych formach. Jedną z takich form jest prowadzenie jednoosobowej działalności gospodarczej przez osoby fizyczne (tzw. JDG), podlegające wpisowi do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG).

Patrząc od strony RODO, prowadzenie działalności gospodarczej przez osoby fizyczne w żaden sposób nie wpływa na prawa i wolności takiej osoby fizycznej, a w szczególności nie uszczupla w jakikolwiek sposób praw, jakie przysługują każdej osobie fizycznej w związku z przetwarzaniem jej danych osobowych. Żaden przepis RODO, a w szczególności przepisy art. 1 i 2, które regulują

przedmiot i materialny zakres stosowania RODO, w żaden sposób nie różnicują sytuacji osoby fizycznej, która jest przedsiębiorcą od sytuacji osoby, która nie jest przedsiębiorcą. Tym samym, działania marketingowe wobec przedsiębiorców również muszą być prowadzone w oparciu o odpowiednią podstawę prawną. Taką podstawą oczywiście może być wspomniany powyżej prawnie uzasadniony interes. W każdym razie to, że dane osobowe przedsiębiorców są gromadzone w publicznym rejestrze, nie oznacza, że mogą być wykorzystywane w dowolnych celach bez uwzględnienia podstawy prawnej.

Potrzebujesz poradnika "Jak ogarnąć marketing zgodnie z prawem?" Kliknij i sprawdź!

Jeżeli chodzi o UŚUDE, to przywołany powyżej art. 10 ust. 1, podobnie jak RODO, w żaden sposób nie różnicuje sytuacji osoby fizycznej, która jest przedsiębiorcą od sytuacji osoby, która nie jest przedsiębiorcą. Tym samym, jeżeli informacja handlowa ma być skierowana do osoby fizycznej, będącej przedsiębiorcą, konieczne jest uzyskanie zgody.

Na gruncie przepisów PT sprawa wygląda o tyle inaczej, że art. 172 ust. 1 PT nie posługuje się pojęciem osoby fizycznej, lecz abonenta oraz użytkownika końcowego, którymi odpowiednio są:

1. podmiot, który jest stroną umowy o świadczenie usług telekomunikacyjnych zawartej z dostawcą publicznie dostępnych usług telekomunikacyjnych (abonent),
2. podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi, dla zaspokojenia własnych potrzeb (użytkownik końcowy).

Patrząc na obie ww. kategorie, stwierdzić należy, że są one znacznie szersze, niż ma to miejsce w przypadku osoby fizycznej, o której mowa w art. 10 ust. 1 UŚUDE. Regulacja dotyczy abonentów i użytkowników końcowych, niezależnie od tego, czy są osobami fizycznymi, czy osobami prawnymi lub jednostkami organizacyjnymi. Ponadto, co jest najistotniejsze dla niniejszych rozważań, regulacja dotyczy abonentów i użytkowników końcowych niezależnie od tego, czy są konsumentami, czy są przedsiębiorcami. Wniosek jest zatem taki, że również przepisy PT wymagają zgody na prowadzenie działań marketingowych wobec osoby fizycznej będącej przedsiębiorcą.

Czy relacja B2B coś zmienia?

W powyższym kontekście można się zastanawiać, czy status nadawcy komunikatu marketingowego cokolwiek zmienia. Czy to, że informacja handlowa zostanie przesłana przez przedsiębiorcę do innego przedsiębiorcy, będącego osobą fizyczną, cokolwiek zmienia?

Na tak postawione pytanie odpowiedź brzmi: nie. Tak jak przepisy RODO, UŚUDE i PT nie różnicują sytuacji osoby fizycznej będącej przedsiębiorcą, tak też nie zmienia tej sytuacji fakt, że również status przedsiębiorcy jest po stronie nadawcy. Innymi słowy, relacja B2B w żaden sposób nie zmienia sytuacji – nadal konieczne jest uzyskanie zgody na działania marketingowe.

Podejście organów nadzorczych

Czy powyższe rozważania mają charakter wyłącznie akademicki?. Bynajmniej. Organy nadzorcze, które mogą kontrolować działania marketingowe to Prezes Urzędu Ochrony Konkurencji i Konsumentów, Prezes Urzędu Komunikacji Elektronicznej, czy Prezes Urzędu Ochrony Danych Osobowych i dotychczasowe decyzje pokazują, że działania marketingowe powinny uwzględniać również przedsiębiorców jako odbiorców.

W jednej ze swoich decyzji Prezes Urzędu Komunikacji Elektronicznej nałożył karę w wysokości 80.000 zł na firmę, która zleciła wykonanie połączeń telefonicznych właśnie do przedsiębiorców (i tylko do nich) nie posiadając stosownych zgód marketingowych. To pokazuje, że w praktyce nie tylko działania marketingowe wobec konsumentów wymagają odpowiedniego zaprojektowania i zabezpieczenia. Działania wobec osób fizycznych będących przedsiębiorcami również powinny być traktowane z należytą uwagą.

Podsumowanie

Podsumowując, prowadzenie działań marketingowych wobec przedsiębiorców wymaga ścisłego przestrzegania przepisów prawa, zarówno tych regulujących ochronę danych osobowych, jak i tych dotyczących świadczenia usług drogą elektroniczną oraz telekomunikacji. Pomimo że RODO dopuszcza możliwość przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu administratora, przepisy UŚUDE i PT wymagają uzyskania zgody na działania marketingowe, co oznacza konieczność zachowania ostrożności i zabezpieczenia się przed ewentualnymi sankcjami organów nadzorczych. Warto zauważyć, że brak zgody może skutkować nałożeniem kar finansowych, jak miało to miejsce ww. opisanym przypadku. Dlatego też należy podchodzić do prowadzenia działań marketingowych wobec przedsiębiorców z należytą uwagą i świadomością obowiązujących przepisów, co ma kluczowe znaczenie dla zachowania legalności i skuteczności tych działań.

Komisja Europejska nałożyła na Apple grzywnę w wysokości ponad 1,8 miliarda euro

Komisja Europejska nałożyła na Apple karę finansową w wysokości ponad 1,8 miliarda euro za nadużycie dominującej pozycji na rynku dystrybucji aplikacji do strumieniowania muzyki dla użytkowników iPhone'ów i iPadów za pośrednictwem App Store. Decyzja Komisji wynika z naruszenia przez firmę przepisów antymonopolowych UE, dokładniej chodzi o "anti-steering provisions". Działania Apple zostały uznane za niezgodne z zasadami uczciwej konkurencji i w efekcie naruszenie Artykułu 102(a) Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

Badanie Komisji wykazało, że Apple kontroluje każdy aspekt użytkowania iOS oraz ustala warunki, jakie deweloperzy muszą spełniać, aby być obecnymi w App Store i dotrzeć do użytkowników iOS w Europejskim Obszarze Gospodarczym (EOG). W szczególności, Apple zakazało deweloperom aplikacji muzycznych w pełni informowania użytkowników iOS o alternatywnych i tańszych usługach subskrypcji dostępnych poza aplikacją oraz uniemożliwiło udostępnianie instrukcji, jak z nich skorzystać. Ograniczenia te obejmują m.in. zakaz informowania użytkowników o cenach subskrypcji dostępnych poza aplikacją, zakaz informowania o różnicach cen pomiędzy subskrypcjami wewnętrznymi, a tymi dostępnymi gdzie indziej oraz uniemożliwienie deweloperom umieszczania linków prowadzących użytkowników iOS na ich strony internetowe, gdzie mogliby zakupić alternatywne subskrypcje.

Kara nałożona na Apple została ustalona na podstawie Wytycznych Komisji z 2006 roku dotyczących kar. Pod uwagę wzięto m.in. czas trwania i powaga naruszenia, obroty i kapitalizacja rynkowa Apple, oraz fakt, że firma przekazała nieprawdziwe informacje w trakcie postępowania administracyjnego. W celu zapewnienia skutecznej prewencji, Komisja zdecydowała się na dodanie do kary podstawowej dodatkowej kwoty w wysokości 1,8 miliarda euro. Całkowita kwota kary została uznana za proporcjonalną w stosunku do globalnych dochodów Apple i konieczną dla osiągnięcia prewencji.

Ponadto, Komisja nakazała Apple usunięcie restrykcyjnych przepisów "anti-steering" oraz zaniechanie powtarzania naruszenia lub stosowania praktyk o podobnym charakterze w przyszłości. Postępowanie to rozpoczęło się w czerwcu 2020 roku, gdy Komisja otworzyła formalne postępowanie w sprawie zasad Apple dla deweloperów aplikacji w App Store. Komisja zakończyła postępowanie, wydając decyzję nakładającą karę na Apple oraz wydając zalecenia dotyczące usunięcia niezgodnych z prawem przepisów.

Źródło: https://bit.ly/3T6ILgX

Wyciekły dane pracowników najpopularniejszych serwisów dostawy w Polsce

Nieuprawniony dostęp do danych dostawców usług takich jak Bolt, Glovo, Uber czy Wolta, korzystających z aplikacji AppJobs.Work, spowodował potencjalne zagrożenie dla tysięcy użytkowników. Dane osobowe, włączając w to imiona, nazwiska, numery PESEL,

adresy zamieszkania czy dane finansowe, zostały naruszone. Incydent wynika prawdopodobnie z działań byłego pracownika AppJobs, który miał wcześniej autoryzowany dostęp do systemów firmy. Choć nie doszło do zewnętrznego ataku, dziesiątki tysięcy użytkowników są narażone na ryzyko wykorzystania ich danych w oszustwach finansowych. AppJobs podjęło działania mające na celu zwiększenie ochrony danych i poinformowało użytkowników o incydencie, sugerując zmianę haseł i zwiększenie świadomości dotyczącej phishingu. Mimo że firma twierdzi, że nie doszło do zewnętrznego wycieku danych, groźba phishingu i oszustw finansowych jest realna.

Źródło: https://bit.ly/4c7EBy7

NSA pozwala na przechowywanie CV kandydatów po zakończeniu rekrutacji. Jak wygląda stanowisko?

Naczelny Sąd Administracyjny orzekł, że pracodawcy mogą przechowywać CV kandydatów nawet po zakończonej rekrutacji, mając na uwadze ewentualne zarzuty dyskryminacji. Decyzja ta wynika z interesu zarówno pracodawców, jak i potencjalnych pracowników, i jest istotna dla firm zatrudniających personel. W toku sprawy, która dotyczyła kandydatki do pracy, organ nadzoru nakazał usunięcie danych po rekrutacji, jednak NSA uznał, że przechowywanie danych jest uzasadnione, szczególnie w kontekście ewentualnych zarzutów dyskryminacji. Wyrok ten stanowi ważny precedens, dający pracodawcom pewność prawną, że mogą przechowywać dokumenty rekrutacyjne w celach obrony przed potencjalnymi roszczeniami, przynajmniej do momentu przedawnienia. Ostatecznie, sąd podkreślił, że decyzja o przechowywaniu danych musi być zgodna z przepisami o ochronie danych osobowych i uzasadniona konkretą potrzebą obrony przed ewentualnymi roszczeniami.

Źródło: https://bit.ly/49FW6Eb

Włoski Urząd Ochrony Danych znowu zakazuje ChatGPT

Włoska agencja ochrony danych, Garante, poinformowała, że aplikacja sztucznej inteligencji ChatGPT opracowana przez OpenAI narusza przepisy dotyczące ochrony danych osobowych. W zeszłym roku Garante zakazał działania ChatGPT z powodu rzekomego naruszenia unijnych przepisów o prywatności. Mimo reaktywacji usługi po rozwiązaniu niektórych problemów, regulator kontynuuje śledztwo, wskazując na potencjalne naruszenia prywatności. OpenAI twierdzi, że ich praktyki są zgodne z przepisami UE i obiecuje współpracę z Garante. Właściciel OpenAI, Microsoft, ma 30 dni na przedstawienie obrony przed włoskim organem nadzoru. Inicjatywa Włoch w kontroli ChatGPT odzwierciedla rosnące zainteresowanie polityków i regulatorów wobec szybkiego rozwoju sztucznej inteligencji.

Źródło: https://reut.rs/49GQaec

Automaty z M&M zbierały wizerunek studentów bez zgody

Studenckie dochodzenie na University of Waterloo odkryło, że inteligentne automaty z M&M na kampusie zbierały dane biometryczne bez zgody. Kontrowersje wybuchły, gdy student pod pseudonimem SquidKid47 opublikował na Reddit zdjęcie automatycznego komunikatu o błędzie, który wskazywał na aktywację aplikacji do rozpoznawania twarzy. Prowadzący śledztwo student River Stanley zauważył, że automatyczne skanowanie twarzy bez zgody narusza prawa prywatności. Pomimo zapewnień producenta automatów, Adaria Vending Services, że maszyny są zgodne z RODO, wątpliwości studentów wzrosły.

Adaria Vending Services tłumaczy, że “najważniejsze jest, rozumienie, że maszyny nie robią, ani nie przechowują żadnych zdjęć, i nie da się zidentyfikować pojedynczej osoby za pomocą kamer w maszynach. Technologia działa jak czujnik ruchu, który wykrywa twarze, więc maszyna wie, kiedy aktywować interfejs zakupu — nigdy nie robiąc ani nie przechowując zdjęć klientów.”

Reakcją uczelni było wyłączenie oprogramowania

automatów, a następnie ich usunięcie z kampusu. Studenci wyrażają zaniepokojenie, sugerując, że technologia ta może być stosowana w innych miejscach na terenie uczelni.

Źródło: https://bit.ly/3wS0lOe

Falszywe nagie zdjęcia, generowane przez AI, jako nowy sposób nękania w szkołach średnich USA

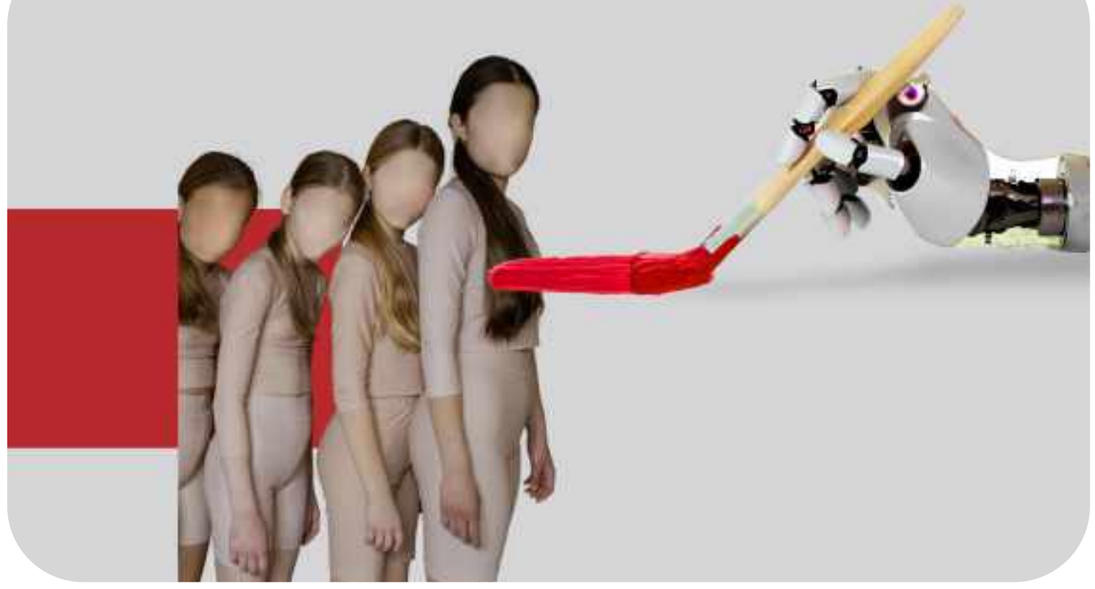
W Beverly Hills w Kalifornii kilkoro uczniów szkół średnich złapano na tworzeniu i rozpowszechnianiu fałszywych zdjęć nagich swoich rówieśników. Urzędnicy szkolni poinformowali rodziców o "nagich zdjęciach generowanych przez sztuczną inteligencję" uczniów w Beverly Vista Middle School. Zdjęcia zawierały twarze uczniów nałożone na nagie ciała. To wydarzenie wywołało oburzenie i zaniepokojenie, ponieważ dzieci tak młode jak te zostały zdehumanizowane przez swoich kolegów i koleżanki, a ich prywatność została naruszona w miejscu, gdzie powinny czuć się bezpiecznie.

Sprawa Beverly Hills jest następstwem serii podobnych incydentów z udziałem uczniów,, którzy tworzą i udostępniają nagie zdjęcia generowane przez AI swoich koleżanek z klasy w szkołach średnich na całym świecie. Ofiara nastolatków z New Jersey opowiedziała o swoich doświadczeniach w styczniu przed federalnymi prawodawcami w Waszyngtonie, aby popierać prawo federalne kryminalizujące wszystkie podobne podróbki seksualizowanych materiałów. Obecnie takiego prawa wciąż nie ma. W 2020 r. Kalifornia uchwaliła ustawę, która zezwala ofiarom jawnych, jednoznacznie seksualnych deepfake'ów, na pozywanie osób, które stworzyły i rozpowszechniły materiał. Powód może odzyskać do $ 150 000 odszkodowania, jeżeli okaże się, że sprawca popełnił czyn w sposób zamierzony. Nie wiadomo, czy odszkodowanie kiedykolwiek zostało przyznane na mocy prawa.

Przewodnicząca Cyber Civil Rights Initiative, Mary Anne Franks, profesor w George Washington University Law School, powiedział, że przepisy Kalifornii nadal nie zabraniają wyraźnie tego, co wydarzyło się w gimnazjum Beverly Vista. Nie wszystkie nagie przedstawienia dzieci są prawnie uznane za pornograficzne, więc bez dodatkowych informacji na temat tego, co przedstawiają zdjęcia, ich legalność jest niejasna.

"Postępowanie cywilne w Kalifornii może potencjalnie mieć zastosowanie tutaj, ale ofiarom zawsze trudno jest ustalić, kim są sprawcy, uzyskać potrzebną pomoc prawną, a następnie faktycznie kontynuować sprawę," mówi Franks.

Źródło: https://nbcnews.to/3TqONKJ



Włoska policja nielegalnie uzyskała informacje o tysiącach kierowców UE

Włoska służba ochrony danych prowadzi dochodzenie w sprawie nielegalnego dostępu włoskiej policji do danych tysięcy kierowców z Unii Europejskiej. Te dane zostały przekazane firmie, która pobiera kary za naruszenia związane z emisją w Londynie. Dochodzenie rozpoczęło się po doniesieniach belgijskiego rządu. Twierdzi on, że nieokreślone oddziały policji wykorzystały swoje uprawnienia, aby przekazać dane osobowe belgijskich kierowców firmie Euro Parking Collections. Ta firma współpracuje z Transport for London w wystawianiu mandatów za naruszenia stref emisji w Londynie.

Chociaż TfL zaprzecza, że Euro Parking korzystało z pomocy włoskiej policji, poważne zarzuty wskazują na naruszenie prywatności. W szczególności po Brexicie dostęp do danych osobowych obywateli UE przez Wielką Brytanię jest ograniczony do przypadków przestępstw kryminalnych. TfL twierdzi, że zatrzymało prośby o belgijskie dane kierowców, ale doniesienia o wydaniu kar belgijskim kierowcom po tym terminie podważają te zapewnienia.

Belgia domaga się od Komisji Europejskiej nowych zabezpieczeń, aby zapobiec nadużyciom praw prywatności przez nieuczciwych pośredników.

Źródło: https://bit.ly/3PhaSZN

Polska

PUODO nałożył administracyjną karę pieniężną w wysokości 9.903,60 PLN na firmę B. za naruszenie przepisów dotyczących zgłaszania naruszeń ochrony danych osobowych oraz zawiadamiania osób, których dane dotyczą, o takich naruszeniach zgodnie z wymaganiami prawa. Firma B. dopuściła się wysłania niezabezpieczonej wiadomości e-mail z pełną listą uczestników konferencji do nieuprawnionego adresata przez osobę prowadzącą działalność gospodarczą. Pomimo trudności w uzyskaniu informacji od administratora danych, ustalono, że wiadomość została wysłana przez osobę fizyczną, a dane dotyczyły łącznie 91 osób, w tym niektóre informacje o zdrowiu. Administrator opóźniał udzielenie wyjaśnieńi argumentował, że dane były publicznie dostępne lub mogły zostać uzyskane za pomocą kontaktu z podmiotami z branży. W związku z tym na Pana B.W. nałożono karę pieniężną oraz nakazano zawiadomienie osób, których dane zostały ujawnione nieuprawnionie. Karę nałożono w wysokości 9.903,60 PLN, a osoba ta ma także obowiązek zawiadomienia wymienionych osób o naruszeniu ochrony ich danych osobowych.

Źródło: https://bit.ly/3ItehRt

Świat

Grecki Urząd Ochrony Danych nałożył karę w wysokości 2000 € na administratora danych za nielegalne wykorzystanie danych geolokalizacyjnych pracownika poza godzinami pracy. Pracownik otrzymał połączenie od pracodawcy podczas urlopu. Administrator użył danych z systemu geolokalizacyjnego zainstalowanego w samochodzie służbowym, ponieważ pracownik nie odbierał telefonu trzykrotnie. Twierdził, że troszczył się o zdrowie pracownika po wcześniejszym wypadku. HDPA stwierdziła nielegalne przetwarzanie danych osobowych pracownika z naruszeniem artykułu 5(1) RODO oraz niepełne informowanie o systemie geolokalizacyjnym i zakazie używania go poza godzinami pracy, co stanowiło także naruszenie artykułów 12 i 13 RODO. Nakładając karę, HDPA odniosła się do Opinii 2/2017 Grupy Roboczej Artykułu 29, zgodnie z którą monitorowanie lokalizacji pojazdów pracowniczych poza godzinami pracy jest nielegalne, chyba że zachodzi taka konieczność, a samo korzystanie z danych powinno być uzależnione od ryzyka i służyć jedynie wybranym celom, takim jak zapobieganie kradzieży pojazdów.

Źródło: https://bit.ly/3wHYGem

Hiszpański Urząd Ochrony Danych (AEPD) nałożył karę w wysokości 56 000 € na firmę Vodafone za udostępnienie poufnych danych innego klienta podczas udzielania odpowiedzi na prawo dostępu innego klienta. Administrator otrzymał zniżkę w wysokości 14 000 € za zrzeczenie się wszelkich apelacji przeciwko karze. 21 sierpnia 2021 roku osoba zgłosiła skargę przeciwko Vodafone España, S.A.U., zarządcy, za naruszenie ich prawa dostępu. Osoba ta poprosiła Vodafone o udostępnienie kopii ich umowy telefonicznej, ponieważ rzekomo firma nie stosowała się do umówionej taryfy. Po kilku nieudanych próbach otrzymania umowy administrator wysłał e-mail zawierający umowę innego klienta oraz nagranie audio z danymi tego klienta.

AEPD podkreślił naruszenie poufności i bezpieczeństwa przez Vodafone za udostępnienie umowy handlowej innego klienta osobie składającej wniosek, naruszając art. 5(1)(f) RODO. Według przedstawionych dowodów osoba uzyskała dostęp do nazwiska, numeru identyfikacyjnego i numeru telefonu nieznanego klienta bez żadnej autoryzacji do ujawniania ich danych osobom trzecim. AEPD uznał zatem naruszenie art. 32 RODO za brak wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapobieżenia takim incydentom. Nałożył karę w wysokości 50 000 € za naruszenie art. 5(1)(f) RODO i 20 000 € za naruszenie art. 32 RODO. Jednak w tym przypadku AEPD dał dwie możliwości Vodafone: uznania odpowiedzialności, co prowadziło do większego obniżenia ostatecznej kwoty, wynoszącego 42 000 €, lub zapłacenia kary w wysokości 56 000 € i zrzeczenia

się wszelkich apelacji przeciwko karze. Vodafone wybrał opcję dobrowolnej zapłaty, płacąc karę w wysokości 56 000 €. Zapłata ta wykorzystała zniżkę oferowaną w początkowej umowie za wczesną zapłatę, wskazując na zrzeczenie się wszelkich form apelacji przeciwko karze.

Źródło: https://bit.ly/4a5Ioue

Austriacki Urząd Ochrony Danych nałożył karę w wysokości 5 900 € na administratora za zawiadomienie o naruszeniu danych osobowych w zbyt ogólny sposób i ponad miesiąc po wystąpieniu zdarzenia. Administrator nie udzielił również jasnej odpowiedzi na żądanie wyjaśnień, co zostało uznane za naruszenie obowiązku współpracy. W kwietniu 2023 roku dyrektor zarządzający firmy zgłosił atak ransomware, w wyniku którego dane zostały zaszyfrowane. Mimo wezwania do udzielenia dodatkowych informacji, administrator dostarczył niejasne wyjaśnienie, co spowodowało zainicjowanie postępowania karnej przez urząd. Ostatecznie, DPA uznała, że administrator nie spełnił wymogów określonych w art. 33(1) i (3) RODO oraz naruszył obowiązek współpracy zgodnie z art. 31 RODO.

Źródło: https://bit.ly/3PdDzGX

Francuski organ ochrony danych osobowych nałożył karę w wysokości 100 000 € na dostawcę usług nieruchomości, Société PAP, między innymi za stosowanie okresów retencji wynoszących 10 lat dla umów zawartych elektronicznie o wartości poniżej 120 €. Kontroler - Société Particulier à Particulier - Editions Neressis - świadczy usługi umożliwiające osobom zawieranie transakcji nieruchomości bez pośredników. CNIL przeprowadził śledztwo w sprawie ich strony internetowej, www.pap.fr, w celu zweryfikowania metod informowania osób o ich prawach jako podmiotów danych oraz bezpieczeństwa procedury tworzenia kont użytkowników. Podczas dochodzenia CNIL stwierdził, że kontroler określił systematyczny okres retencji wynoszący dziesięć lat od akceptacji zamówienia na stronie internetowej. CNIL zainicjował procedurę sankcjonowania przeciwko kontrolerowi w dniu 6 lutego 2023 r.

Organ nadzorczy uznał, że okres retencji wynoszący 10 lat jest nadmierny dla umów o wartości poniżej 120 € i narusza art. 5(1)(e) RODO. Ponadto stwierdził, że kontroler naruszył art. 13 RODO, nie uwzględniając prawa do złożenia skargi do CNIL oraz udzielając nieprawidłowych informacji o okresie retencji danych w polityce prywatności. CNIL również uznał naruszenie art. 28(3) RODO, gdy kontroler próbował retrospektywnie zmienić umowę z przetwarzającym dane, nie obejmując wszystkich wymagań tego artykułu. Na koniec, CNIL uznał naruszenie art. 32 RODO, stwierdzając, że środki bezpieczeństwa i poufności danych nie były wystarczające. Dla tych naruszeń CNIL nałożył karę w wysokości 100 000 € na kontrolera.

Źródło: https://bit.ly/3wDYooA

Brytyjski organ ochrony danych osobowych (ICO) nałożył karę w wysokości 409 080 € (350 000 GBP) na Ministerstwo Obrony Wielkiej Brytanii za ujawnienie 265 unikalnych adresów e-mail osób poszukujących przesiedlenia z Afganistanu po przejęciu władzy przez Talibów w lecie 2021 roku. W dniu 20 września 2021 roku, po przejęciu władzy przez Talibów, Ministerstwo Obrony (MoD) wysłało e-mail do listy osób uprawnionych do ewakuacji z Afganistanu, używając pola „Do" zamiast „ukrytej kopii" („Bcc"). Ta decyzja spowodowała ujawnienie wszystkim odbiorcom adresów e-mail tych osób, co stanowiło naruszenie bezpieczeństwa danych osobowych. Dodatkowo, po incydencie MoD zidentyfikowało dwa podobne wydarzenia, w których również nastąpiło niezamierzone ujawnienie danych. Ogółem ujawniono 265 unikalnych adresów e-mail.

ICO stwierdził, że MoD naruszyło art. 5(1)(f) (UK) RODO, ponieważ nie posiadało odpowiednich

procedur operacyjnych zapewniających bezpieczeństwo przesyłania grupowych wiadomości e-mail do osób poszukujących przesiedlenia z Afganistanu. W momencie naruszenia MoD nie miało wdrożonych procedur zapewniających bezpieczne wysyłanie takich wiadomości. Osoby odpowiedzialne za komunikację nie otrzymały specyficznych wytycznych dotyczących ryzyka związanego z przesyłaniem grupowych wiadomości e-mail zawierających wrażliwe informacje. Ten błąd ludzki doprowadził do potencjalnego nieuprawnionego ujawnienia wrażliwych informacji, zagrażając życiu osób objętych ewakuacją. Z uwagi na ryzyko represji ze strony talibów wobec zwolenników sił zachodnich, ICO podkreślił, że dane osobowe były wyjątkowo wrażliwe i wymagały ostrożnego traktowania.

Ostatecznie ICO nałożył karę w wysokości 409 080 € (350 000 GBP) na MoD. Kara ta została obniżona z początkowej kwoty 818 090 € (700 000 GBP) z uwagi na nietypowe i pilne okoliczności wycofania się z Afganistanu. Ponadto uwzględniono fakt, że MoD jest organem publicznym, co również skłoniło do zmniejszenia kary.

Źródło: https://bit.ly/3TqOf7D

Dziękujemy za przeczytanie naszego Newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI

P.S. Czy wiesz, że...

Prywatność danych pozostaje najwyższym priorytetem dla użytkowników mediów społecznościowych, z większą niż kiedykolwiek kontrolą działań tych firm. Badanie SAS wykazało, że 38% respondentów korzysta z mediów społecznościowych rzadziej niż kiedyś z powodu obaw o prywatność danych, a 36% stwierdziło, że usunęło konto w mediach społecznościowych.