Obserwuj nas na:

Nr 3/2020 (12)
Marzec 2020

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

ZAKRES DANYCH POZYSKIWANYCH PRZEZ GMINY W DEKLARACJACH ŚMIECIOWYCH NIE MOŻE BYĆ ZBYT SZEROKI

Rada gminy, określając wzór deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, nie może wymagać podania szerszego zakresu danych, niż ten określony przepisami ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach – przypomina Prezes UODO.

Jak stanowi art. 6m ust. 1b ustawy o utrzymaniu czystości i porządku w gminach, rada gminy, określając wzór deklaracji, może wymagać podania następujących danych:
- imię i nazwisko lub nazwa właściciela nieruchomości oraz adres miejsca zamieszkania lub siedziby,
- adres nieruchomości,
- dane stanowiące podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi,
- numer telefonu właściciela nieruchomości,
- adres poczty elektronicznej właściciela nieruchomości,
- inne informacje niezbędne do wystawienia tytułu wykonawczego,
- informacje dotyczące posiadania kompostownika przydomowego i kompostowania w nim bioodpadów stanowiących odpady komunalne.

Gminy nie są zatem uprawnione do pozyskiwania szerszego niż określony w tym przepisie zakresu danych osobowych właściciela nieruchomości, który jest zobowiązany do złożenia deklaracji śmieciowej, a tym bardziej do pozyskiwania danych osobowych osób zamieszkujących daną nieruchomość.

Nie mogą więc żądać podania przez właściciela nieruchomości np. daty urodzenia czy imion ojca oraz matki, jak również danych osób zamieszkujących w danym lokalu mieszkalnym czy ich numeru PESEL, co potwierdza także orzecznictwo (wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 12 stycznia 2017 r., sygn. akt I SA/Po 1459/16).

Ponieważ stosowana w gminach praktyka bywa nieprawidłowa, Prezes UODO zwrócił się do Ministra Spraw Wewnętrznych i Administracji o uczulenie na tę kwestię właściwych podmiotów nadzorczych w tym zakresie, tak by przyjmowane w uchwałach rozwiązania nie prowadziły do nakładania na właścicieli nieruchomości obowiązków niewynikających z ustawy. Podkreślił, że ich dowolne ukształtowanie, wbrew pierwotnym uprawnieniom ustawowym, będzie oznaczać naruszenie wynikających z RODO zasad - legalizmu, proporcjonalności i celowości.

W odpowiedzi resort wskazał, że przekazał wystąpienie Prezesa UODO do wszystkich prezesów regionalnych izb obrachunkowych, które są organem właściwym do oceny uchwał dotyczących określenia wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właścicieli nieruchomości.

KOMISJE DYSCYPLINARNE W SŁUŻBIE CYWILNEJ

Komisje dyscyplinarne w urzędach, w których działa korpus służby cywilnej, mają status administratora – takie stanowisko Prezes UODO zajął w odpowiedzi udzielonej na wniosek Szefa Służby Cywilnej.

Wyjaśniając kwestie związane z przetwarzaniem danych osobowych przez komisje dyscyplinarne orzekające w sprawach o naruszenie obowiązków służbowych członka korpusu służby cywilnej, Prezes UODO wskazał, że z przepisów ustawy o służbie cywilnej wynika autonomiczny charakter komisji dyscyplinarnych (także tych powołanych w drodze porozumienia dla kilku urzędów). Artykuł 122 tej ustawy stanowi bowiem, że członkowie komisji dyscyplinarnych są niezawiśli w zakresie orzecznictwa dyscyplinarnego oraz nie są związani rozstrzygnięciami innych organów stosujących prawo, z wyjątkiem prawomocnego wyroku sądu. Tym samym, w świetle przepisów RODO, należy uznać je za administratora. Jednocześnie organ ds. ochrony danych osobowych wyjaśnił, że biorąc pod uwagę kolegialny charakter komisji dyscyplinarnej urzędu oraz wspólnej komisji dyscyplinarnej, jej członkowie nie muszą posiadać odrębnych upoważnień związanych z pracami tych organów. Prezes UODO odniósł się także do kwestii zapewnienia obsługi administracyjnej komisji dyscyplinarnej, co budzi wątpliwości przede wszystkim w odniesieniu do wspólnej komisji dyscyplinarnej. Wskazał, że w tym przypadku właściwym rozwiązaniem wydaje się unormowanie tej kwestii w powołującym tę komisję porozumieniu dyrektorów generalnych urzędów i wskazanie w nim konkretnego podmiotu (organu) ją obsługującego.

TRWAJĄ PRACE NAD KRAJOWYMI WYMOGAMI AKREDYTACJI

Polska jest jednym z krajów z największą liczbą inicjatyw tworzących kodeksy postępowania. Świadczy to o chęci podnoszenia poziomu ochrony danych w wybranych sektorach.

Stosowanie postanowień kodeksów musi być monitorowane przez podmioty, które uzyskały akredytację Prezesa UODO. Będzie ona prowadzona na podstawie wymogów akredytacji zaopiniowanych przez Europejską Radę Ochrony Danych (EROD) w ramach mechanizmu spójności.

Obecnie EROD opiniuje projekty krajowych wymogów akredytacji podmiotów monitorujących przedstawione przez pierwsze organy nadzorcze. Wszystkie opinie są dostępne na stronie internetowej Rady. Także UODO przygotowuje swoją wersję takiego dokumentu, który po zaopiniowaniu przez EROD, zostanie opublikowany na stronie internetowej UODO w formie komunikatu Prezesa. O postępach tych prac informowane są inicjatywy, które zgłosiły się wcześniej do UODO, tak by ułatwić im prace nad postanowieniami kodeksu dotyczącymi podmiotu monitorującego oraz projektowania jego działalności. **Dlatego do kontaktu z Wydziałem Kodeksów i Certyfikacji zachęcamy wszystkie podmioty, które nie zgłosiły dotąd faktu rozpoczęcia prac nad kodeksem dla swojego sektora.**
Szczegółowe informacje o kodeksach postępowania są dostępne w zakładce Kodeksy i certyfikacja na stronie internetowej UODO.

KTO WYSYŁA POWIADOMIENIE O ODWOŁANIU INSPEKTORA OCHRONY DANYCH W PRZYPADKU LIKWIDACJI ADMINISTRATORA?

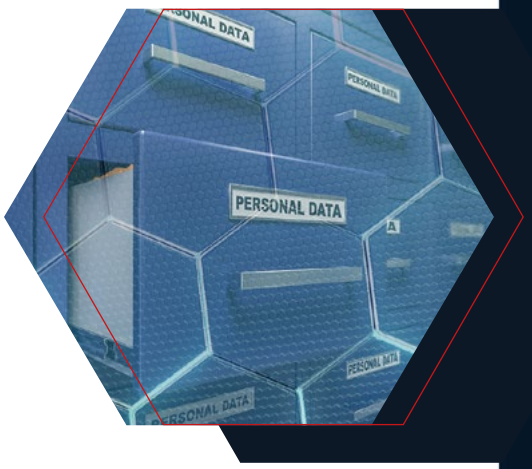
Kto powinien zawiadomić Prezesa UODO o odwołaniu inspektora ochrony danych w przypadku likwidacji/przejęcia administratora, który wyznaczył tego inspektora (np. w przypadku likwidacji gimnazjum)?

Powiadomienia Prezesa Urzędu Ochrony Danych Osobowych o odwołaniu dotychczasowego inspektora ochrony danych powinien dokonać podmiot, który go wyznaczył. Obowiązek ten wynika z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

W sytuacji zaś, gdy administrator nie zawiadomił Prezesa UODO o odwołaniu IOD, może to zrobić podmiot, który jest jego następcą prawnym, a zatem przejął prawa i obowiązki likwidowanego podmiotu, wstępując tym samym w jego prawa.

Więcej pod linkiem:
https://uodo.gov.pl/pl/223/1442

CZY KIEROWNIK URZĘDU STANU CYWILNEGO JEST ADMINISTRATOREM DANYCH OSOBOWYCH?



A jeśli tak, to czy powinien on wyznaczyć inspektora ochrony danych? W jakiej formie powinno być dokonane wyznaczenie IOD?

Odpowiadając na pierwsze pytanie zauważyć należy, że ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego określa wprost, kto realizuje cele z zakresu ustawy, w związku z tym, iż do dokonywania czynności z zakresu rejestracji stanu cywilnego został z mocy ustawy zobowiązany kierownik urzędu stanu cywilnego (art. 9 ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego). Z tego względu należy uznać, iż to kierownik urzędu stanu cywilnego jest administratorem danych osobowych, niezależnie od tego, czy w określonej sytuacji faktycznie stanowisko to będzie piastować organ gminy – wójt (burmistrz, prezydent miasta) – czy inna osoba wyznaczona na to stanowisko przez wójta (burmistrza, prezydenta miasta) na podstawie art. 6 ust. 4 lub 5 ustawy Prawo o aktach stanu cywilnego.

Odnosząc się natomiast do pytania dotyczącego ewentualnego obowiązku wyznaczenia inspektora ochrony przez kierownika urzędu stanu cywilnego, w pierwszej kolejności stwierdzić należy, że wobec brzmienia art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, który to przepis prawa krajowego ustala kierunek interpretacji w polskim systemie prawnym, użytego w art. 37 ust. 1 lit. a RODO pojęcia „organ lub podmiot publiczny", nie można przyjąć, aby obowiązek wyznaczenia inspektora ochrony danych wynikał z przesłanki wymienionej w art. 37 ust. 1 lit. a RODO. Warto mieć jednak na uwadze, że nawet w sytuacji braku takiego obowiązku, administrator – kierownik urzędu stanu cywilnego – może dobrowolnie takiego inspektora wyznaczyć.

Jednocześnie należy przypomnieć, że art. 37 ust. 3 RODO dopuszcza możliwość wyznaczenia przez kilku administratorów jednego inspektora ochrony danych, przy uwzględnieniu ich struktury organizacyjnej i wielkości.

Zaznaczyć jednak należy, że skorzystanie z takiego rozwiązania wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych.
Zatem w przypadku, gdyby burmistrz i kierownik USC wyznaczyli na swojego inspektora tę samą osobę, powinni wspólnie określić zasady dotyczące zapewnienia takiemu inspektorowi wystarczającej ilości czasu na wypełnianie jego obowiązków, pomocy w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów.

Ponadto wyznaczenie do piastowania stanowiska kierownika urzędu stanu cywilnego innej osoby niż wójt (burmistrz, prezydent), który jest odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych dotyczących przetwarzania w tym obszarze w odrębnym dokumencie.
Warto także pamiętać, że jeśli kierownik USC decydowałby się na wyznaczenie inspektora, to on jako administrator powinien dokonać tego wyznaczenia, a także zawiadomić Prezesa UODO o jego wyznaczeniu.

Odnosząc się zaś do pytania dotyczącego formy czynności polegającej na wyznaczeniu inspektora, wskazać należy przede wszystkim, że przepisy RODO oraz ustawy o ochronie danych osobowych nie zawierają szczegółowych uregulowań w tym zakresie. Wobec tego decyzja w tej kwestii należy do administratora. Biorąc jednak pod uwagę zasadę rozliczalności, zgodnie z którą **administrator musi być w stanie wykazać przestrzeganie przepisów w zakresie ochrony danych osobowych, co w praktyce najczęściej oznacza dokumentowanie wszelkich procesów związanych z ochroną danych osobowych, administrator powinien wybrać taką formę, która umożliwi mu wykazanie w szczególności: kiedy i kogo wyznaczył do pełnienia takiej funkcji.**

Więcej pod linkiem: https://uodo.gov.pl/pl/223/1443

CZY ŚWIADCZENIE USŁUGI KOLOKACJI IMPLIKUJE KONIECZNOŚĆ ZAWARCIA UMOWY POWIERZENIA?

Odpowiedź na to pytanie, jak na każde poruszające problematykę konieczności zawarcia umowy powierzenia, zależy od zakresu świadczonych usług i znajomości wszystkich okoliczności faktycznych w relacji między usługodawcą a klientem. Tak więc status podmiotu przetwarzającego powinien być przypisywany podmiotowi biorącemu rzeczywisty, nie jedynie formalny udział w zleconych na zasadzie outsourcingu operacjach przetwarzania

Centra danych w dobie postępu technologicznego i globalizacji są ważnym elementem zgodności z przepisami RODO, gdyż są właścicielami zasobów fizycznych, z użyciem których może dochodzić do przetwarzania danych osobowych na dużą skalę oraz ułatwiają ich przepływ. Należy pamiętać, że zgodnie z definicją zawartą w art.4 pkt.2 rozporządzenia RODO pojęcie przetwarzania obejmuje nie tylko potocznie rozumiane aktywne podejmowanie działań (takie jak zbieranie, porządkowanie czy usuwanie), ale również zachowanie bierne (jak przechowywanie). W tym sensie bardzo często podmioty takie będą uważane za podmioty przetwarzające, a umowy z podmiotami świadczącymi usługi hostingowe, chmurowe czy kolokacyjne powinny uwzględniać regulacje dotyczące powierzenia przetwarzania danych osobowych.

Czym jest kolokacja?
W branży IT, pojęcie kolokacji (bądź hotelingu) utożsamiane jest z usługą polegającą na zapewnieniu klientowi możliwości umieszczenia własnego sprzętu informatycznego i/lub telekomunikacyjnego zapewniającego przetwarzanie jego danych (bądź jego klientów) w niezbędnych warunkach zapewniających ww. urządzeniom prawidłowe działanie, tj. dostarczenie energii elektrycznej, ochrona fizyczna, usługi telekomunikacyjne, chłodzenie, zapewnienie stałej temperatury, czystości powietrza itp. Immamentną cechą usługi kolokacji jest więc przechowywanie sprzętu. Jest to więc też najmniej inwazyjna forma wpływu na dane osobowe przez podmiot świadczący usługę kolokacji (centra danych).

Ograniczenie się wyłącznie do tego zakresu usług, w którym istotą świadczonej usługi nie jest uprawnienie do operacji na danych osobowych a jedynie udostępnienie nieruchomości i odpowiedniej infrastruktury a usługodawca nie ma dostępu do pomieszczeń, w którym znajdują się serwery klienta, w większości przypadków nie będzie implikowała konieczności uwzględnienia w umowie regulacji dotyczących powierzenia przetwarzania.

W przypadku umowy, której zapisy przewidują możliwość uzyskania dostępu do pomieszczeń znacznie wzrasta prawdopodobieństwo konieczności uwzględnienia w umowie elementów powierzenia. W ramach stosownych umów, usługa kolokacji może obejmować wsparcie przy rozwiązywaniu problemów, monitorowanie, serwisowanie czy modernizowanie sprzętu klienta (służącego do przetwarzania danych) co jest utożsamiane w branży IT jako tzw. „remote hands". **Należy pamiętać, że istotą konstrukcji powierzania przetwarzania jest zlecenie przez administratora wybranemu podmiotowi dokonania określonych czynności przetwarzania, w imieniu i na rzecz administratora, tj. czynności o których mowa w art. 4 pkt. 2 rozporządzenia RODO**. Najczęściej administrator podejmuje decyzję o powierzeniu przetwarzania, gdy uzna, że podmiot, któremu powierzy te czynności, wykona je szybciej, taniej bądź skuteczniej. Podmiot świadczący usługę kolokacji, w zależności od treści umowy, może uzyskiwać fizyczny dostęp do nośników, na których znajdują się dane osobowe i na polecenie administratora wykonywać na nich operacje (np. tworzenia kopii zapasowych, usuwania danych, niszczenia danych poprzez niszczenie fizycznych nośników). W takich wypadkach konieczne jest uwzględnienie w umowie regulacji dotyczących powierzenia przetwarzania.

Jeśli nie dochodzi do powierzenia przetwarzania danych osobowych, stosowna umowa usługi kolokacyjnej powinna zawierać wymagania związane z prawidłowym zabezpieczeniem infrastruktury, gdyż to na administratorze, jako podmiocie decydującym o środkach przetwarzania danych osobowych, ciąży obowiązek zapewnienia właściwych środków technicznych i organizacyjnych, a co za tym idzie – obowiązek doboru środków adekwatnych do zagrożeń.

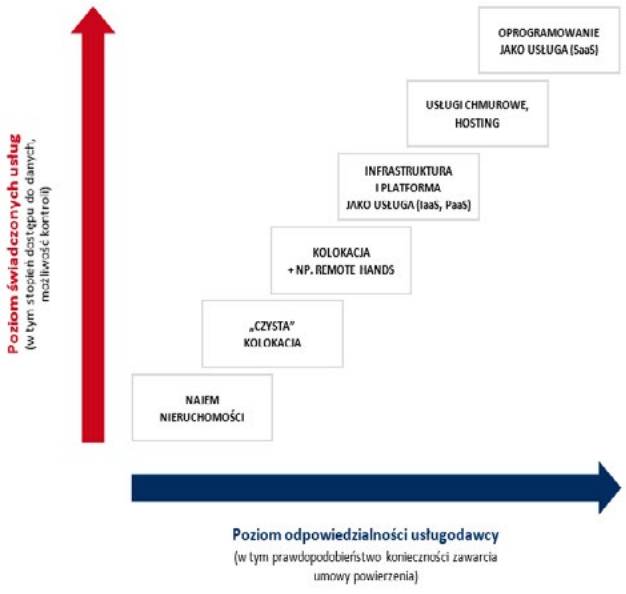
Konkluzja

Aby uznać czy w ramach przedmiotowych rozważań zachodzi konieczność zawarcia umowy powierzenia za każdym razem administrator musi dokonać oceny czy relacja z wybranym podwykonawcą nie jest przetwarzaniem danych osobowych w imieniu administratora (czyli dochodzi do powierzenia przetwarzania). W tym celu powinien dokonać analizy celu, sposobów i środków oraz skonsultować się z inspektorem ochrony danych (jeśli został wyznaczony).

Aby móc stwierdzić czy może zachodzić sytuacja, w której podmiot świadczący usługę kolokacji jest podmiotem przetwarzającym w rozumieniu rozporządzenia 2016/679, warto odpowiedzieć sobie na kilka pytań, tj. czy usługodawca:

- ma dostęp do danych osobowych, czy może je na polecenie klienta odczytywać, dokonywać na nich zmian bądź udostępniać?
- jest odpowiedzialny za takie procesy podejmowane w imieniu klienta jak przechowywanie, szyfrowanie, udostępnianie, analizowanie, usuwanie bądź niszczenie danych?
- czy w imieniu klienta może ingerować w zasoby fizyczne, tj. dyski twarde będące nośnikami danych osobowych, np. poprzez ich fizyczne usunięcie?
- czy ma fizyczny dostęp do maszyn klienta, może je w jego imieniu przenosić, wyłączać/włączać?
- czy w imieniu klienta podejmuje inne działania poza podstawowym zapewnieniem środowiska niezbędnego do prawidłowego działania zasobów sprzętowych?

Przynamniej jedna odpowiedź twierdząca może implikować konieczność zawarcia umowy powierzenia, jednakże każdą sytuację należy ocenić indywidualnie i poprzedzić stosowną, wyżej wymienioną analizą.



Rys. 1. Poziom świadczonych usług a odpowiedzialność usługodawcy w kontekście powierzenia przetwarzania

EROD

Przedstawiciele organów ochrony danych z EOG oraz Europejski Inspektor Ochrony Danych, zrzeszeni w Europejskiej Radzie Ochrony Danych (EROD), spotkali się na osiemnastym posiedzeniu plenarnym. Podczas posiedzenia omówiono szeroki zakres tematów.

Stosowanie RODO w pierwszych 20 miesiącach zakończyło się powodzeniem

Mimo niewystarczających zasobów i wyzwań jakie stoją przed wszystkimi organami nadzorczymi, wynikające na przykład z sieci procedur krajowych, Rada jest przekonana, że współpraca między organami nadzorczymi zaowocuje wspólną kulturą ochrony danych i spójną praktyką. EROD analizuje możliwe rozwiązania w celu przezwyciężenia tych wyzwań i ulepszenia istniejących procedur współpracy. Wzywa także Komisję Europejską do sprawdzenia, czy procedury krajowe wpływają na skuteczność procedur współpracy. To ostatecznie prawodawcy mogą odegrać rolę w zapewnieniu dalszej harmonii i stosowania przepisów. W swojej ocenie EROD odnosi się do takich kwestii jak: narzędzia międzynarodowego przekazywania danych, wpływ na MŚP, zasoby organów nadzorczych i rozwój nowych technologii. Zdaniem EROD, zmiana przepisów RODO byłaby przedwczesna.

Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych - powstał projekt wytycznych

Przepisy dotyczą przekazywania danych osobowych od organów publicznych lub organów z EOG do organów publicznych w krajach trzecich lub do organizacji międzynarodowych, w przypadku gdy takie przekazywanie nie jest objęte decyzją stwierdzającą odpowiedni stopień ochrony. Wytyczne zalecają, które zabezpieczenia należy wdrożyć w prawnie wiążących instrumentach - art. 46 ust. 2 lit. a) - lub w uzgodnieniach administracyjnych - art. 46 ust. 3 lit. b) - aby zapewnić, że poziom ochrony osób fizycznych przewidziany w RODO będzie osiągnięty a nie osłabiony. Trwają konsultacje społeczne w tej sprawie (https://uodo.gov.pl/pl/138/1440).

Oświadczenie w sprawie wpływu transakcji połączenia na prywatność

Po ogłoszeniu zamiaru Google LLC przejęcia Fitbit, EROD przyjęła oświadczenie podkreślające, że ewentualne dalsze połączenie i gromadzenie wrażliwych danych osobowych dotyczących osób w Europie przez dużą firmę technologiczną może wiązać się z wysokim zagrożeniem dla prywatności i ochrony danych.

EROD przypomina stronom proponowanego połączenia o ich zobowiązaniach wynikających z RODO oraz o konieczności przeprowadzenia pełnej oceny wymogów ochrony danych i wpływu połączenia na prywatność w przejrzysty sposób. Rada wzywa strony do ograniczenia potencjalnych zagrożeń dla prawa do prywatności i ochrony danych przed powiadomieniem Komisji Europejskiej o połączeniu.

EROD rozważy wszelkie skutki dla ochrony danych osobowych w EOG i jest gotowa udzielić porady WE, jeżeli zostanie o to poproszona.

KARY

Grecja: 15 tys. euro kary za nielegalny monitoring wizyjny
Grecki organ ochrony danych osobowych, w odpowiedzi na skargę, przeprowadził postępowanie w sprawie zgodności z prawem przetwarzania danych osobowych na serwerze Allseas Marine S.A. oraz zgodności z prawem dostępu do e-maili i kontroli usuniętych e-maili managera wyższego szczebla, wobec którego istniało podejrzenie o niedopuszczalne prawem działania przeciwko interesom firmy.

Organ stwierdził, że firma jako administrator danych zastosowała się do wymagań nałożonych przez RODO, jej wewnętrzna polityka i regulacje przewidywały zakaz użytkowania należących do przedsiębiorstwa sieci i środków komunikacji elektronicznej w celach prywatnych, a także możliwość przeprowadzania kontroli wewnętrznych. Zgodnie zatem z art. 5 ust. 1 oraz art. 6 ust. 1 lit. f) RODO, firma miała prawo dokonania przeszukania i usunięcia e-maili pracownika.

Jednocześnie organ stwierdził, że w firmie został zainstalowany system monitoringu wizyjnego, który działał w sposób niezgodny z prawem i że materiał przedłożony organowi nadzorczemu uznany został za nielegalny. Ostatecznie organ uznał, że przedsiębiorstwo nie zapewniło pracownikowi możliwości skorzystania z prawa dostępu do jego danych osobowych przechowywanych w komputerze firmowym, z którego korzystał. W związku z ustaleniami o naruszeniu przepisów RODO, organ zadecydował o skorzystaniu z uprawnień, przysługujących mu na mocy art. 58 ust. 2 tego rozporządzenia poprzez zastosowanie środków naprawczych. Po pierwsze, organ nakazał firmie natychmiast zastosować się do wniosku skarżącego o umożliwienie mu skorzystania z prawa dostępu i informacji w zakresie jego danych osobowych przechowywanych w komputerze firmowym, z którego korzystał – oraz powiadomienie organu nadzorczego o tym fakcie.

Po drugie, firma musi zapewnić, w terminie miesiąca od chwili otrzymania decyzji, zgodność operacji przetwarzania dokonywanych poprzez system monitoringu wizyjnego z przepisami RODO oraz powiadomienie o powyższym organu nadzorczego. W szczególności organ zarządził:
- Przywrócenia stosowania art. 5 ust. 1 lit a) i b) RODO zgodnie z decyzją organu;
- Przywrócenia stosowania przepisów art. 5 ust. 1 lit. b) do f) RODO w związku z faktem, że wykryte naruszenie dotyczy wewnętrznej organizacji firmy oraz zgodności z RODO, poprzez podjęcie wszelkich koniecznych środków w związku z zasadą rozliczalności.

Nałożenie na przedsiębiorstwo skutecznej, proporcjonalnej i odstraszającej kary administracyjnej, jak jest to stosowne w przypadku nielegalnego zainstalowania i operowania systemem monitoringu wizyjnego, zgodnie ze szczególnymi okolicznościami sprawy, której poziom ustalono na 15 tys. euro.

Źródło: https://edpb.europa.eu/news/national-news/2020/investigation-regarding-access-and-inspection-employer-employees-emails_en

Włoska firma zapłaci 11,5 mln euro za nielegalne przetwarzanie danych
Włoski organ nadzorczy nałożył na Eni Gas e Luce (EGL) dwie kary pieniężne o łącznej wysokości 11,5 mln euro w związku z nielegalnym przetwarzaniem danych osobowych w kontekście działalności promocyjnej oraz aktywowania niechcianych umów. Wysokość kar została określona w oparciu o parametry wyznaczone przez RODO i uwzględniła szeroki krąg zainteresowanych, skalę aktywności, czas trwania naruszenia oraz sytuację ekonomiczną firmy.

Pierwsza z kar, o wysokości 8,5 mln euro, ma związek z nielegalnym przetwarzaniem danych w związku z działalnością telemarketingową i telesprzedażową, co było przedmiotem postępowania organu nadzorczego w związku z licznymi zawiadomieniami i skargami, otrzymanymi niezwłocznie po rozpoczęciu stosowania RODO.

Przeprowadzone postępowania ujawniły, że działalność EGL miała charakter systematyczny i unaoczniły poważne błędy w związku z przetwarzaniem danych przez firmę.

Naruszenia objęły m.in. połączenia telefoniczne wykonywane bez zgody odbiorcy lub pomimo wyrażonej przezeń odmowy ich otrzymywania, która nie uruchamiała procedury opt-out. Nie zostały również wdrożone odpowiednie środki techniczne i organizacyjne celem rejestrowania zastrzeżeń użytkowników. Okres przechowywania danych był zbyt długi. Ponadto firma zakupiła dane od podmiotów, które nie uzyskały zgody osób, których dane dotyczą, na ujawnienie ich danych stronom trzecim.

Po stwierdzeniu nielegalności przetwarzania danych przez EGL, włoski organ nadzorczy nakazał przedsiębiorstwu wprowadzenie procedur i systemów, których zadaniem byłaby weryfikacja udzielenia zgody przez osoby, które znalazły się w jego listach kontaktowych, przed rozpoczęciem kampanii promocyjnych. EGL musi także zapewnić pełną automatyzację przepływu danych ze swojej bazy danych na tzw. czarną listę (tj. listę osób, które nie życzą sobie otrzymywania reklam). Włoski organ nadzorczy zakazał firmie wykorzystywania danych pochodzących z list kontaktowych zakupionych od brokerów danych w przypadkach, gdy nie uzyskali oni konkretnej zgody na przekazywanie tych danych EGL.

Druga kara pieniężna, w wysokości 3 mln euro, została nałożona w związku z naruszeniami dotyczącymi niechcianych umów na dostawę prądu i gazu „na zasadach wolnorynkowych". Liczni zgłaszający zawiadamiali organ, że o zawarciu nowej umowy dowiadywali się dopiero z pisma o zakończeniu umowy z poprzednim dostawcą lub z pierwszego rachunku wystawionego przez EGL. W niektórych przypadkach skarżący informowali o błędnych danych w umowach i o podrobionych podpisach.

Około 7200 klientów poniosło szkody w związku z powyższymi nieprawidłowościami. Ustalenia organu nadzorczego wykazały, że postępowanie firmy w trakcie pozyskiwania nowych klientów przez działające w jej imieniu agencje zewnętrzne prowadziło (w zakresie organizacyjnym i zarządczym) do operacji przetwarzania naruszających przepisy RODO i określone w nim zasady rzetelności i prawidłowości przetwarzania.

Wziąwszy pod uwagę te nielegalne działania, organ nadzorczy nakazał firmie wdrożenie środków naprawczych oraz wprowadzenie specjalnych powiadomień celem wykrywania anomalii proceduralnych. Wprowadzenie powyższych środków będzie miało miejsce oraz zostanie zakomunikowane organowi nadzorczemu w określonym terminie, zaś kary będą musiały zostać uiszczone w terminie 30 dni.

Źródło: https://edpb.europa.eu/news/national-news/2020/italian-supervisory-authority-fines-eni-gas-e-luce-eur-115-

Włochy: 27,8 mln euro kary za działania marketingowe naruszające ochronę danych osobowych

Włoski organ nadzorczy nałożył na TIM SpA karę pieniężną w wysokości 27,8 mln euro za niezgodne z prawem przetwarzanie danych w celach marketingowych. Naruszenie dotyczyło danych milionów osób.

Od stycznia 2017 r. do początku 2019 r. organ nadzorczy otrzymał setki skarg, dotyczących w szczególności niezamawianych marketingowych połączeń telefonicznych, wykonanych bez zgody osób, których dane dotyczą oraz wbrew ich rejestracji w publicznym wykazie opt-out. W innych przypadkach osoby, do których dzwoniono, w jasny sposób odmówiły wyrażenia zgody na otrzymywanie połączeń marketingowych. Procesy przetwarzania, względem których domniemywano nierzetelność, wspominane były również w skargach dotyczących konkursów oraz związanych z nimi formularzy, które firma przekazywała użytkownikom.

Kompleksowe dochodzenie w tej sprawie przeprowadzone zostało z udziałem wyspecjalizowanego oddziału włoskiej policji finansowej (Guardia di Finanza) i ujawniono szereg poważnych naruszeń ochrony danych osobowych.
Firmie TIM SpA wykazano niewystarczającą znajomość fundamentalnych cech jej procesów przetwarzania (brak spełnienia zasady rozliczalności).

W wielu przypadkach, spośród milionów połączeń marketingowych, które zostały wykonane w okresie sześciu miesięcy względem osób niebędących klientami przedsiębiorstwa, organ nadzorczy stwierdził, że operatorzy telefoniczni kontaktowali się z osobami, których dane dotyczą, na polecenie firmy TIM SpA przy braku ich zgody na to. W jednym przypadku kontaktowano się z osobą 155 razy w ciągu miesiąca. W około dwustu tysiącach przypadków wykonano połączenia z numerami spoza listy dostarczonej przez TIM. Ponadto stwierdzono inne niezgodne z prawem zachowania, takie jak brak nadzoru przedsiębiorstwa nad działaniem telefonicznych centrów obsługi klienta celem prawidłowego zarządzania i aktualizacji przez nie „czarnych list" (na których znajdują się osoby, które nie chcą otrzymywać połączeń marketingowych) oraz fakt, że zgoda na wykonywanie przez firmę działań marketingowych była wymagana w celu dołączenia do programu promocyjnego „Tim Party".

Nieprawidłowe, nieprzejrzyste informacje na temat przetwarzania danych były podawane w związku z aplikacjami dla klientów, zaś rozwiązania wprowadzone celem pozyskania wymaganej zgody były niewłaściwe. W kilku przypadkach do wypełnienia przedstawiane były papierowe formularze, w których pojedyncze oświadczenie zgody było przedłożone do kilku celów przetwarzania, w tym marketingu.

System zarządzania naruszeniami ochrony danych okazał się być nieskuteczny. Brakowało również odpowiednich systemów wdrożeniowych i zarządczych w związku z przetwarzaniem danych, co skutkowało brakiem spełnienia wymogów ochrony danych w fazie projektowania. „Czarne listy" przedsiębiorstwa okazały się być niespójne z tymi, którymi dysponowały operowane przez kontraktorów centra obsługi telefonicznej – dotyczyło to również nagrań „zamówień ustnych", tj. umów zawartych telefonicznie. Numery telefonów abonentów innych operatorów, które TIM SpA przechowywało jako dostawca usługi sieciowej, były przechowywane przez okres dłuższy niż przewidziany prawem i wykorzystywane w kampaniach marketingowych bez zgody klientów.

Prócz kary pieniężnej włoski organ nadzorczy nakazał firmie wdrożenie dwudziestu środków naprawczych w postaci zarówno nakazów, jak i zakazów. W szczególności przedsiębiorstwo otrzymało zakaz przetwarzania w celach marketingowych danych użytkowników, którzy odmówili wyrażenia zgody na otrzymywanie połączeń marketingowych z centrów obsługi telefonicznej, użytkowników ujętych na „czarnej liście" oraz osób niebędących klientami firmy, którzy nie wyrazili zgody na kontakt.

TIM SpA nie może również przetwarzać danych klientów, które pozyskało przez aplikacje „MyTim", „TimPersonal" oraz „TimSmartKid", do celów innych niż zapewnienie związanych z nimi usług, bez dobrowolnej, udzielonej w tym celu zgody.

Nakazy, które wydał włoski organ nadzorczy względem firmy, obejmują zobowiązanie do weryfikacji przez nie spójności „czarnych list" oraz terminowego pozyskiwania tych pozyskanych od centrów telefonicznych celem aktualizacji własnych wykazów. TIM SpA będzie musiało również przebudować swój program kliencki „Tim Party" oraz umożliwić swoim klientom dostęp do programów promocyjnych i konkursów bez wymuszania na nich zgody na działania marketingowe. Przedsiębiorstwo musi również dokonać przeglądu procedur aktywacji aplikacji; określić – jasnym i zrozumiałym językiem – wykonywane czynności przetwarzania wraz z ich celem oraz stosowanymi mechanizmami oraz uzyskać ważną zgodę użytkowników. TIM SpA będzie musiało wdrożyć środki techniczne i organizacyjne w związku z żądaniami osób, których dane dotyczą i wzmocnić te środki celem zapewnienia jakości, prawidłowości oraz terminowych aktualizacji danych osobowych przetwarzanych w poszczególnych systemach.

Nałożone na firmę środki naprawcze będą musiały zostać wdrożone i zgłoszone w określonym przez organ nadzorczy terminie, zaś kara finansowa musi zostać uiszczona w terminie 30 dni.

Źródło: https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-

URZĄD OCHRONY DANYCH OSOBOWYCH