Nr 3/2022 (36)
Marzec 2022

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

NIE WOLNO UPUBLICZNIAĆ DANYCH OSÓB SKŁADAJĄCYCH SKARGI

Nie ma uzasadnienia, by podczas sesji rady gminy upubliczniać dane osobowe osób, które złożyły skargę na burmistrza. Takie stanowisko UODO – wyrażone w decyzji udzielającej upomnienia radzie miejskiej i burmistrzowi – potwierdził ostatnio Wojewódzki Sąd Administracyjny w Warszawie (sygn. akt II SA/1/Va 1855/21).

Podczas jednej z sesji rady miejskiej, na której radni mieli ustosunkować się do skargi złożonej na burmistrza do kuratorium, przewodniczący rady, rozpoczynając ten punkt programu, odczytał treść skargi wraz z imionami i nazwiskami osób ją składających. Następnie skarga została przekazana komisji skarg wniosków i petycji, która przed podjęciem przez radę miejską uchwały o jej zasadności lub niezasadności, miała zająć co do niej stanowisko.

Sesja rady była transmitowana on-line, a jej nagranie zostało następnie udostępnione w Internecie.

Osoby, których dane osobowe upubliczniono podczas sesji, wniosły do Prezesa UODO skargę, wskazując na naruszenie ich prawa do ochrony danych osobowych.

Co stanowią przepisy?

W toku prowadzonego w tej sprawie postępowania organ nadzorczy ustalił, że zgodnie z art. 18b ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, rada gminy rozpatruje skargi na działania wójta i gminnych jednostek organizacyjnych; wnioski oraz petycje składane przez obywateli; w tym celu powołuje komisję skarg, wniosków i petycji. Ponadto na podstawie art. 229 pkt 3 Kodeksu postępowania administracyjnego, rada gminy jest właściwa do rozpatrywania skarg dotyczących zadań lub działalności wójta, burmistrza lub prezydenta miasta.

Przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (art. 18 ust. 1) stanowią natomiast, że posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów są jawne i dostępne, zaś zgodnie z postanowieniami ustawy o samorządzie gminnym (art. 20 ust. 1b), obrady rady gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk, a nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty.

Ustalenia UODO

W analizowanym przypadku dane osobowe skarżących były przetwarzane przez radę gminy w związku z rozpatrywaniem skargi złożonej na działania burmistrza. Organ nadzorczy ocenił, że w tym zakresie to rada była administratorem tych danych.

W wydanej w tej sprawie decyzji wskazał, że obowiązkiem administratora, o którym mowa w art. 5 ust. 1 lit. c RODO, jest zaś zapewnienie, by przetwarzane dane były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Jego rolą jest również, stosownie do art. 5 ust. 1 lit. f RODO, przetwarzanie danych w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem

przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Zaznaczył, iż Wojewódzki Sąd Administracyjny w wyroku z 26 sierpnia 2020 r. (sygn. akt II SA/Wa 2826/19) wskazał, że od administratora wymagane jest podjęcie proporcjonalnych środków celem zabezpieczenia danych. Wymienione w tym przepisie „zagrożenia", przed którymi administrator musi się zabezpieczyć, mają charakter katalogu otwartego, na co wskazuje użyte w tym przepisie pojęcie „w tym".

Administrator jest też zobowiązany (art. 24 ust. 1 i art. 32 ust. 1 lit. a RODO) wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych odbywało się zgodnie z RODO i aby zapewnić im bezpieczeństwo. Z kolei wdrażane środki powinny być – na co wskazał Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 26 sierpnia 2020 r. (sygn. akt II SA/Wa 2826/19) – adekwatne i proporcjonalne do stopnia ryzyka.

Ponieważ zgodnie z przepisami sesja rady miejskiej była transmitowana w sieci, to planując jej przebieg, należało właściwie przygotować się do omówienia skargi, tak by przedstawić ją w sposób zapewniający odpowiedni stopień ochrony danych osobowych. W ocenie organu nadzorczego, określenie podmiotu i przedmiotu skargi oraz wskazanie jej nadawców jako pracowników konkretnej instytucji, bez wskazywania ich imion i nazwisk, byłoby wystarczające dla umożliwienia burmistrzowi merytorycznego odniesienia się do stawianych mu zarzutów.

W wyjaśnieniach składanych w toku prowadzonego postępowania, burmistrz oświadczył, że zgodnie z postanowieniami statutu miasta, obsługę sesji rady zapewnia urząd miasta, którego kierownikiem jest burmistrz, a zatem to on realizuje transmisję posiedzeń rady. Przyznał, że nie opracował jednak wewnętrznych uregulowań określających szczegółowe zasady tej transmisji. Wprowadził natomiast, jak wskazał „(...) do obiegu urzędowego ogólne informacje oraz wskazówki i wytyczne dotyczące postępowania oraz zakresu danych osobowych ujawnianych podczas obrad rady miejskiej", przedstawiając klauzulę informacyjną zawieszoną przed wejściem na salę obrad oraz zamieszczoną w Biuletynie Informacji Publicznej.

Odnosząc się do tego aspektu sprawy, organ nadzorczy podniósł, że proces projektowania realizacji transmisji obrad rady miasta składa się z wielu etapów. Spełnienie obowiązku informacyjnego wobec uczestników tych obrad jest tylko jednym z nich. Brak lub nieodpowiednie zastosowanie wdrożonych procedur w zakresie transmisji i publikacji nagrań w Internecie będzie miał wpływ na ryzyko wystąpienia naruszenia praw i wolności osób, których dane zostały utrwalone. Burmistrz, jako administrator danych osobowych przetwarzanych w związku z transmisją, nagraniem i upublicznieniem nagrania sesji rady miasta w sieci, zapewnił niezbędne do osiągnięcia tego celu środki techniczne, jednak nie przygotował odpowiednich procedur zapewniających realizację zasad wskazanych w art. 5 ust. 1 RODO.

Tymczasem orzecznictwo sądów administracyjnych wskazuje, że publikacja informacji publicznej w BIP powinna wiązać się z usunięciem danych osobowych osób prywatnych lub ich zanonimizowaniem. W wyroku Naczelnego Sądu Administracyjnego z 14 marca 2013 r. (sygn. akt I OSK 620/12) wskazywano, że usunięcie z opublikowanej w BIP uchwały rady gminy personaliów osób prywatnych, czy też ich zanonimizowanie w ogłoszonej w BIP uchwale organu gminnego, nie wpływa na czytelność dokonanego w ten sposób przekazu. Sąd podkreślał również, że jeżeli celem zamieszczenia informacji publicznej w BIP-ie jest transparentność działalności publicznej rady gminy, to cel ten zostaje spełniony także wówczas, gdy w związku z ochroną prywatności z informacji usunięte zostaną dane dotyczące osób prywatnych.

Upomnienia

W tym stanie faktycznym i prawnym Prezes UODO, biorąc

pod uwagę incydentalny charakter naruszenia oraz fakt, że udostępnione w sieci nagranie sesji rady zostało zanonimizowane, uznał, że wystarczającą reakcją będzie udzielenie upomnienia:

- radzie miejskiej za odczytanie przez jej przewodniczącego pełnej treści skargi wraz z danymi osobowymi osób ją wnoszących, podczas gdy dane te nie były niezbędne do jej rozpatrzenia, co stanowiło naruszenie zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c RODO;
- burmistrzowi za niezapewnienie odpowiedniego bezpieczeństwa danych osobowych podczas transmisji on-line w Internecie oraz poprzez zamieszczenie niezanonimizowanego nagrania z obrad sesji rady miejskiej, co stanowiło naruszenie zasady integralności i poufności danych wyrażonej w art. 5 ust. 1 lit. f w zw. z art. 24 ust. 1 i art. 32 ust. 1 lit. a RODO.

Rozstrzygnięcie WSA

Upomniane podmioty odwołały się od tej decyzji organu nadzorczego do Wojewódzkiego Sądu Administracyjnego, lecz ich skargi zostały oddalone.

Pomocny poradnik

Jednocześnie warto przypomnieć, że na stronie internetowej UODO jest dostępny materiał pt. „Projektowanie ochrony danych osobowych w związku z transmisją i nagrywaniem obrad kolegialnych organów jednostek samorządu terytorialnego", zawierający wskazówki, jak spełniać obowiązek jawności działań władzy samorządowej przy jednoczesnym zachowaniu przepisów o ochronie danych osobowych.

ZAWIADOMIENIE O WYZNACZENIU IOD LUB JEGO ZASTĘPCY TRZEBA PRZESŁAĆ NA WŁAŚCIWYM FORMULARZU

Jedynym prawidłowym i skutecznym sposobem zawiadomienia Prezesa UODO o wyznaczeniu inspektora ochrony danych lub jego zastępcy jest zawiadomienie w postaci elektronicznej. Jednocześnie musi ono zostać przesłane na właściwym formularzu.

Do UODO wciąż wpływają liczne pytania dotyczące tego, czy administrator skutecznie powiadomił Prezesa UODO o wyznaczeniu inspektora ochrony danych (IOD) lub jego zastępcy.

W związku z tym raz jeszcze warto przypomnieć, że jedynym prawidłowym i skutecznym sposobem zawiadomienia Prezesa UODO o wyznaczeniu inspektora ochrony danych jest zawiadomienie w postaci elektronicznej - zgodnie z art. 10 ust. 6 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz z art. 46 ust. 9 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. W analogiczny sposób należy także przesyłać zawiadomienia dotyczące zastępcy inspektora ochrony danych (art. 11a ust. 3 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz art. 46 ust. 6 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości).

Przesłanie zawiadomienia w innej postaci, nie jest traktowane jako wywiązanie się z obowiązku określonego w powołanych ustawach (co zostało wskazane m.in. w osobnym komunikacie zamieszczonym na stronie internetowej UODO).

Ważne jest również, by skorzystać z właściwego formularza elektronicznego, tj. dotyczącego IOD bądź zastępcy IOD, jak również odpowiedniego do podstawy powołania IOD. Administratorzy wyznaczający IOD na podstawie art. 37 ust. 1 RODO (częściowo doprecyzowanego w art. 9 ustawy o ochronie danych osobowych) powinni skorzystać z formularzy oznaczonych jako RODO, natomiast administratorzy wyznaczający IOD na podstawie ustawy z dnia 14 grudnia 2018 r. powinni skorzystać z formularzy DODO.

Podkreślić też należy, że niektórzy administratorzy są zobowiązani do wyznaczenia IOD zarówno na podstawie RODO, jak i ustawy z dnia 14 grudnia 2018 r. (np. Policja), a wówczas muszą oni przesłać osobne zawiadomienia, korzystając przy tym z właściwych formularzy.
Ponadto wypełniony formularz musi zostać opatrzony kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP osoby uprawnionej do reprezentowania administratora. W zawiadomieniu należy podać wszystkie wymagane przepisami prawa informacje. **Do zawiadomienia składanego przez pełnomocnika należy załączyć pełnomocnictwo udzielone w formie elektronicznej oraz opłatę skarbową** od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia).

Najważniejsze informacje nt. zawiadomień Prezesa UODO związanych z IOD znajdują się w zakładce "Inspektor ochrony danych" na stronie www.uodo.gov.pl.

Jednocześnie warto przypomnieć, że w materiale pt. „Wielu pełnomocników błędnie, a przez to nieskutecznie, zawiadamia o wyznaczeniu IOD" zamieszczonym w Newsletterze UODO dla IOD z listopada ub. r. (nr 11/2021), zawarte są wskazówki związane z dokonywaniem zawiadomienia dotyczącego IOD przez pełnomocnika.

KARY

Finlandia: kara pieniężna za zbieranie niepotrzebnych informacji o pacjentach

Organ nadzorczy nałożył na Fińskie Centrum Ubezpieczycieli administracyjną karę pieniężną w wysokości 52 tys. euro, a także upomnienie oraz nakazał doprowadzenia do stanu zgodności.

Urząd Rzecznika Ochrony Danych zbadał praktyki Fińskiego Centrum Ubezpieczycieli Komunikacyjnych w zakresie żądania dokumentacji pacjentów od podmiotów świadczących usługi opieki zdrowotnej w celu likwidacji szkód.

Administrator danych stanął na stanowisku, że ma prawo gromadzić obszerne informacje o pacjencie i żądać od dostawców usług opieki zdrowotnej nieredagowanej dokumentacji pacjenta w celu obsługi roszczeń. Administrator gromadził również informacje o wizytach pacjentów w placówkach służby zdrowia w celu ustalenia, czy świadczeniodawca pobierał opłaty za wizyty niezwiązane z badaniem lub leczeniem obrażeń odniesionych w wypadkach drogowych.

Administrator systematycznie żądał pełnej dokumentacji pacjentów wnoszących roszczenia, zamiast ograniczać swoje żądania do informacji niezbędnych do obsługi roszczeń. Praktyka ta naruszyła RODO.

Rzecznik Ochrony Danych zauważył, że ustawa o ubezpieczeniach komunikacyjnych nie daje bezpośredniego dostępu do całej dokumentacji pacjenta. Wymagane informacje muszą być niezbędne do ustalenia i zaspokojenia roszczenia.

Fiński organ nadzorczy stwierdził również, że informacje na temat stanu zdrowia danej osoby powinny być przede wszystkim ujawniane firmom ubezpieczeniowym w formie oświadczenia, zgodnie z zaleceniami Fińskiego Stowarzyszenia Medycznego.

Dodatkowo organ nadzorczy udzielił ubezpieczycielowi upomnienia za naruszenie przepisów o ochronie danych osobowych i nakazał mu dostosowanie swoich praktyk w zakresie żądania informacji o pacjentach do przepisów o ochronie danych osobowych.

Źródło:
https://edpb.europa.eu/news/national-news/2022/administrative-fine-imposed-finnish-motor-insurers-centre-collection_en

Finlandia: obowiązkiem administratora jest właściwa ochrona danych i ich bezpieczne przetwarzanie

Rada ds. sankcji przy Urzędzie Rzecznika Ochrony Danych nałożyła administracyjną karę pieniężną w wysokości 6 500 euro na małą grupę przedsiębiorców z branży turystycznej, której częścią jest biuro podróży, które dopuściło się naruszeń.

Klient biura podróży poinformował Urząd Rzecznika Ochrony Danych o podejrzeniach, że biuro podróży nie przetwarza danych zawartych w elektronicznym formularzu zamówienia wizy zgodnie z przepisami o ochronie danych osobowych. Klient zwrócił się również do biura podróży z prośbą o usunięcie jego danych z systemu, jednak przedsiębiorstwo nie spełniło prośby klienta.

Jak ustalono w działalności przedsiębiorstwa występowały nieprawidłowości w zakresie bezpiecznego przetwarzania danych i realizacji praw osób, których dane dotyczą.

Biuro podróży korzystało z niezaszyfrowanego połączenia sieciowego do wypełniania formularzy wniosków wizowych i przechowywało dane osobowe na publicznym serwerze internetowym. Informacje wprowadzone do formularza zostały zapisane w formie pliku PDF w folderze plików na serwerze internetowym, do którego można było uzyskać dostęp z Internetu.

Informacje wpisane do formularzy obejmowały imię i nazwisko klienta, dane kontaktowe i numer paszportu.

Rzecznik Ochrony Danych stwierdził, że biuro podróży zaniedbało swój obowiązek właściwej ochrony danych i ich bezpiecznego przetwarzania. Spółka naruszyła również obowiązek spełnienia żądania osoby, której dane dotyczą, o ich usunięcie.

Źródło:
https://edpb.europa.eu/news/national-news/2022/finnish-dpa-administrative-fine-imposed-travel-agency-data-protection_en

Hiszpania: kara pieniężna za brak konkretnej i świadomej zgody na profilowanie

Hiszpański organ nadzorczy nałożył administracyjną karę pieniężną w wysokości 3 mln euro za brak konkretnej i świadomej zgody osób, których dane przetwarzano na potrzeby profilowania do celów handlowych.

Dochodzenie w tej sprawie zostało wszczęte w związku z pojawieniem się przesłanek wskazujących na możliwość istnienia nieprawidłowych praktyk w zakresie zautomatyzowanego profilowania i podejmowania decyzji przez spółkę Caixabank w kontekście jej działalności handlowej.

Administrator ten działa jako instytucja finansowa i płatnicza, której działalność polega na wprowadzaniu do obrotu kart kredytowych lub debetowych, rachunków kredytowych z kartą lub bez karty oraz pożyczek za pośrednictwem trzech kanałów:
- bezpośrednio przez spółkę,
- za pośrednictwem agenta,
- za pośrednictwem innych punktów sprzedaży, z którymi współpracuje spółka.

W ramach swojej działalności handlowej, Caixabank tworzy profile do następujących celów:
- analiza ryzyka niewykonania zobowiązania w momencie składania wniosku o produkt,
- analiza ryzyka niewykonania zobowiązania w trakcie składania wniosku o produkt,
- wybór grupy docelowej.

W przedstawionej sprawie podstawą działania była zgoda podmiotu danych, pozyskiwana za pomocą różnych kanałów od podmiotów pośredniczących i agentów, w celu przeprowadzenia badań i profilowania. W przedstawionym przypadku osoba zainteresowana badaniem otrzymała tylko ogólne informacje o różnych sposobach profilowania. Informacje te jednak

uniemożliwiały dokładne określenie, na jaki sposób postępowania dana osoba wyraża zgodę. Zastrzeżenia budził również brak zapisów umożliwiających osobie zainteresowanej dokonanie wyboru celów, dla których dane miały być przetwarzane.

Organ nadzorczy nakazał administratorowi dostosowanie operacji przetwarzania danych do przepisów RODO w ciągu sześciu miesięcy od wydania tej decyzji.

Źródło:
https://edpb.europa.eu/news/national-news/2022/aepd-fine-eur-3000000-caixabank-payments-consumer-efc-ep-sau-lack-specific_en

Belgia: 250 tys. euro dla IAB Europe

Belgijski organ ochrony danych uznał, że opracowane przez IAB Europe „Ramy przejrzystości i zgody" (Transparency and Consent Framework – TCF) nie są zgodne z RODO.

Od 2019 roku belgijski organ ochrony danych otrzymał wiele skarg skierowanych do Interactive Advertising Bureau Europe (IAB Europe). Skargi kwestionowały zgodność mechanizmu TCF z RODO.

TCF to szeroko rozpowszechniony mechanizm, który ułatwia zarządzanie preferencjami użytkowników w zakresie spersonalizowanej reklamy on-line. Mechanizm TCF, ma na celu również przyczynienie się do zgodności z RODO organizacji opierających się na protokole OpenRTB. Z kolei protokół Open RTB jest jednym z najszerzej stosowanych protokołów „Real-Time Bidding", tj. natychmiastowej, zautomatyzowanej aukcji online profili użytkowników w celu sprzedaży i zakupu powierzchni reklamowej w Internecie.

Kiedy użytkownicy wchodzą na stronę internetową lub w aplikację, która zawiera reklamę, firmy technologiczne reprezentujące tysiące reklamodawców mogą natychmiast („w czasie rzeczywistym") składać zakulisowe oferty na tę reklamę za pośrednictwem zautomatyzowanego systemu aukcyjnego wykorzystującego algorytmy w celu wyświetlania ukierunkowanych reklam dostosowanych do profilu danej osoby.

Kiedy użytkownicy po raz pierwszy odwiedzają stronę internetową lub aplikację, pojawia się interfejs (platforma zarządzania zgodą, dalej również „CMP"), poprzez który mogą oni wyrazić zgodę na gromadzenie i udostępnianie swoich danych osobowych lub wyrazić sprzeciw wobec różnych rodzajów przetwarzania w oparciu o uzasadnione interesy dostawców technologii reklamowych. Tu właśnie wkracza TCF: ułatwia przechwytywanie, poprzez platformę zarządzania CMP, preferencji użytkowników. Preferencje te są następnie kodowane i przechowywane w postaci „ciągu TC", który jest udostępniany organizacjom uczestniczącym w systemie Open RTB, aby wiedziały one, na co użytkownik wyraził zgodę/sprzeciw. CMP umieszcza również plik cookie (euconsent-v2) na urządzeniu użytkownika.

W połączeniu, ciąg przejrzystości i zgody (Transparency and consent string – ciąg TC) i plik cookie (euconsent-v2) mogą zostać powiązane z adresem IP użytkownika, co umożliwia identyfikację autora preferencji.

TCF odgrywa kluczową rolę w architekturze systemu OpenRTB, ponieważ wyraża preferencje użytkowników dotyczące potencjalnych sprzedawców i różnych celów przetwarzania, w tym oferowania reklam dostosowanych do indywidualnych potrzeb.

Wbrew twierdzeniom IAB Europe, belgijski organ ochrony danych stwierdził, że spółka działa jako administrator danych w odniesieniu do rejestracji sygnału zgody poszczególnych użytkowników, sprzeciwów i preferencji za pomocą unikalnego ciągu TC, który jest powiązany z identyfikowalnym użytkownikiem.

Belgijski organ ochrony danych zidentyfikował wiele naruszeń RODO popełnionych przez IAB Europe. Dla przykładu, IAB Europe nie zapewniło ram prawnych dla przetwarzania danych zawartych w ciągu TC, a podstawy prawne oferowane przez TCF dla późniejszego przetwarzania przez sprzedawców adtech są nieodpowiednie.

Informacje przekazywane użytkownikom za pośrednictwem interfejsu CMP były zbyt ogólne i niejasne, aby umożliwić użytkownikom zrozumienie charakteru i zakresu przetwarzania, biorąc zwłaszcza pod uwagę złożoność TCF. Dlatego też użytkownikom trudno jest zachować kontrolę nad swoimi danymi osobowymi.

Wobec braku środków organizacyjnych i technicznych zgodnych z zasadą ochrony danych w fazie projektowania i domyślnej ochrony danych, w tym w celu zapewnienia skutecznego wykonywania praw osób, których dane dotyczą, jak również monitorowania ważności i integralności wyborów dokonywanych przez użytkowników, zgodność TCF z RODO nie jest odpowiednio zagwarantowana ani wykazana.

Projekt decyzji przygotowany przez belgijski organ ochrony danych został przeanalizowany w ramach mechanizmu współpracy przewidzianego w RODO („mechanizm kompleksowej współpracy”). Po analizie i dwóch sprzeciwach, które belgijski organ ochrony danych uwzględnił w nowym projekcie, decyzję zatwierdziły zainteresowane organy reprezentujące większość z trzydziestu krajów Europejskiego Obszaru Gospodarczego.

W świetle tych naruszeń belgijski organ nadzorczy poza sankcją finansową nakazał administratorowi podjęcie wielu działań naprawczych, mających na celu dostosowanie obecnej wersji TCF do RODO. Środki te obejmują m.in.:

– stworzenie ważnej podstawy prawnej przetwarzania i rozpowszechniania preferencji użytkowników w kontekście TCF, jak również zakaz wykorzystywania prawnie uzasadnionego interesu jako podstawy przetwarzania danych osobowych przez organizacje uczestniczące w TCF;

– ścisłą weryfikację organizacji uczestniczących w TCF w celu zapewnienia, że spełniają one wymogi RODO.

Belgowie wyznaczyli IAB Europe dwa miesiące na przedstawienie planu działania w celu wdrożenia tych środków naprawczych.

Źródło:
https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

EDUKACJA

W związku z trudną sytuacją spowodowaną atakiem Federacji Rosyjskiej na Ukrainę do Polski przybyło bardzo wielu uchodźców szukających schronienia i pomocy. Wiele osób, organizacji i instytucji włącza się w pomoc, zajmując się najważniejszymi kwestiami, jak zapewnienie noclegu, wyżywienia czy opieki medycznej.

Warto w tym kontekście mieć również na uwadze, że osoby, które przebywają na terytorium Unii Europejskiej mogą korzystać z praw, jakie daje im RODO.

UODO dołączyło do obchodów Światowego Dnia Konsumenta, który w tym roku wspólnie z UOKiK i wieloma innymi instytucjami dedykowany jest uchodźcom z Ukrainy.

Urząd przygotował specjalny materiał poradnikowy, który przybliża uchodźcom z Ukrainy prawa, jakie im przysługują na gruncie RODO i tłumaczy, w jaki sposób z tych praw korzystać.

Przydatne kontakty do instytucji, które pomagają:

- pomagamukrainie.gov.pl – to ważny adres, jeśli szukasz noclegu, pomocy humanitarnej, transportu i szeroko rozumianego wsparcia;

- Reklamacje, zwroty produktów, zasady i prawa obowiązujące w Polsce w kontaktach konsument-przedsiębiorca (sprzedawca, usługodawca) - wejdź na stronę Urzędu Ochrony Konkurencji i Konsumentów – https://www.uakonsument.uokik.gov.pl/

- Przydatne porady jak korzystać z usług operatorów telekomunikacyjnych znajdziesz na stronie Urzędu Komunikacji Elektronicznej - to #PomagamUkrainie - Centrum Informacji Konsumenckiej (uke.gov.pl)

- Informacje na temat ubezpieczycieli i banków - wyszukiwarka podmiotów - https://www.knf.gov.pl/en/CONSUMERS/Information_for_the_financial_market_consumers/Entities_search

- Poznaj swoje prawa związane z korzystaniem z produktów finansowych i ubezpieczeniowych oraz zobacz jak może Ci pomóc Rzecznik Finansowy - https://rf.gov.pl/en/important-views/

- Informacje na temat podróżowania koleją. Zobacz jakie masz prawa i możliwości na stronie Urzędu Transportu Kolejowego UTK – www.utk.gov.pl/ukraina oraz https://www.utk.gov.pl/en/passenger-rights

- Jeśli planujesz wyjechać z Polski do innego kraju, zapoznaj się z podstawowymi informacjami w zakresie praw konsumenta podczas podróży po UE, Norwegii, Islandii i Wielkiej Brytanii - ECK w Europie - Europejskie Centrum Konsumenckie (konsument.gov.pl)

- Osoby, które przebywają na terytorium Unii Europejskiej mogą korzystać z praw, jakie daje im RODO. Więcej na ten temat oraz wskazówki jak chronić dane osobowe i prywatność oraz jak bezpiecznie poruszać się w Internecie znajdziesz na stronie Urzędu Ochrony Danych Osobowych - https://uodo.gov.pl/p/forukraine

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy OPS może weryfikować źródła ogrzewania z CEEB przy rozpatrzeniu wniosku o dodatek osłonowy?

Czy członkom wspólnoty mieszkaniowej można udostępnić dane innych jej członków?

Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD?

URZĄD OCHRONY DANYCH OSOBOWYCH