URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

Nr 10/10/23

SPIS TREŚCI

Drodzy Czytelnicy!

Nowe technologie w założeniu mają być narzędziem rozwoju: ekonomicznego, społecznego, osobistego. Jako organ nadzorczy ochrony danych osobowych, mamy świadomość, że musi być to instrument doskonale przemyślany, przede wszystkim pod kątem analizy ryzyka. Na ile nowe technologie należy regulować, aby ich nie przeregulować, jaki mamy wpływ na to, aby nie zatrzymując postępu technologicznego dbać o to, by twórcy i kreatorzy cyfrowej rewolucji zawsze mieli człowieka i jego poszanowanie godności i prywatności w centrum uwagi? To niektóre pytania, na które szukamy odpowiedzi w październikowym wydaniu Biuletynu. W rozmowie z ekspertem numeru Jakubem Groszkowskim, Zastępcą Prezesa Urzędu Ochrony Danych Osobowych na temat sztucznej inteligencji w kontekście ochrony danych duży akcent pada właśnie na odpowiedzialność twórców sztucznej inteligencji za proponowane przez nich produkty oraz usługi. O innowacjach dyskutują również prelegenci dwudniowej konferencji „Forum Nowych Technologii" zorganizowanej przez Urząd Ochrony Danych Osobowych we współpracy ze Stowarzyszeniem Prawa Nowych Technologii i Akademią Ekonomiczno-Humanistyczną w Warszawie. Zachęcamy do zapoznania się z wnioskami i refleksjami z wydarzenia.

Cały październikowy numer zahacza o tematy nowych technologii, bo – pomimo, że prawo zdaje się nie nadążać za innowacjami, Urząd musi nieustająco je monitorować, by wiedzieć jak chronić obywateli w sposób nie blokujący im dostępu do korzyści płynących z wykorzystywania zaawansowanych technologii. Zaciekawić powinien Państwa również materiał o tym, jakie dane gromadzą tzw. urządzenia ubieralne (ang. Wearables) oraz na co warto zwrócić uwagę wybierając je, by zadbać o swoją prywatność.

Piszemy też o rekordowej karze, którą irlandzki organ ochrony danych nałożył na spółkę TikTok za przetwarzanie danych dzieci. Z jesiennego wydania czytelnicy dowiedzą się również, jakie informacje należy zawrzeć w zgłoszeniu naruszenia ochrony danych osobowych. Dokonując kompletnych zgłoszeń, administratorzy mogą uniknąć zarzutów związanych z niedopełnieniem obowiązku notyfikacyjnego, a także usprawnić podejmowane przez organ nadzorczy czynności wyjaśniające.

Na naszych subskrybentów czeka zajmująca decyzja UODO odnośnie do sprostowania danych przez administratora. Warto zapoznać się z materiałem dotyczącym realizacji programu „Laptop dla ucznia”. Dowiecie się Państwo z niego komu przysługuje status administratora danych gromadzonych przy okazji realizacji tego programu.

Kogo należy informować o możliwości popełnienia przestępstwa w związku ze zgłaszaniem kandydatów na posłów i senatorów? Nie jest to Prezes UODO. Wybory już za nami, ale treść materiału bardzo interesująca.

Podsumowując – jeśli jesteście Państwo ciekawi roli RODO w kontekście sztucznej inteligencji, chcielibyście dowiedzieć się, z jakimi skargami i zawiadomieniami mierzył się ostatnio organ nadzorczy oraz poznać wiele ciekawych dla administratorów danych zagadnień, koniecznie zasiądźcie do lektury tego numeru.

Adam Sanocki
Dyrektor Departamentu Komunikacji Społecznej, Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

WYZWANIA I ODPOWIEDZIALNOŚĆ W ERZE SZTUCZNEJ INTELIGENCJI

Z Jakubem Groszkowskim, Zastępcą Prezesa Urzędu Ochrony Danych Osobowych na temat sztucznej inteligencji w kontekście ochrony danych rozmawia Karol Witowski, Zastępca Rzecznika Prasowego UODO.

W ostatnim czasie bardzo popularny stał się temat sztucznej inteligencji. Jak w kontekście technologii SI wygląda temat ochrony danych?

Zagadnienie sztucznej inteligencji nie jest nową koncepcją – pierwsze dyskusje na ten temat toczyły się już w latach 60-tych XX wieku. Gwałtowny rozwój tej dziedziny zawdzięczamy zwiększonej mocy obliczeniowej komputerów, większej ilości dostępnych danych, lepszym algorytmom i ogromnym inwestycjom w rozwój technologiczny.

Rozwiązania z wykorzystaniem sztucznej inteligencji od dawna są znane m.in. w medycynie, gdzie ułatwiają rozpoznawanie chorób, w handlu czy marketingu, dzięki czemu możliwe jest m.in. przygotowanie zindywidualizowanych rekomendacji, a także w obszarze motoryzacji (chociażby na potrzeby pojazdów autonomicznych). W praktyce jest to również bardzo obiecujący obszar dla start-upów, w szczególności działających w sektorze finansów, sądownictwa czy wspomnianej już ochrony zdrowia.

Technologia SI nie jest tematem nowym również dla UODO. Od początku swego istnienia polski organ ds. ochrony danych z uwagą pochylał się nad zagadnieniami związanymi z rozwojem nowoczesnych technologii. Zmieniały się tylko oblicza technologicznych nowości, które były przedmiotem jego zainteresowania.

Ochrona danych w kontekście dynamicznego rozwoju technologii, jaki obserwujemy obecnie, jest zagadnieniem skomplikowanym i wymagającym. Sztuczna inteligencja jest zjawiskiem globalnym, ma charakter transgraniczny i może dotyczyć całej ludzkości. Rozwój i wykorzystanie sztucznej inteligencji musi odbywać się zgodnie z etyką i wartościami uznawanymi przez ludzkość oraz z poszanowaniem godności ludzkiej.

Jakie wyzwania stawia przed organem ds. ochrony danych tak dynamiczny rozwój technologii, która w swoim DNA ma przetwarzanie ogromnych ilości danych?

Sztuczna inteligencja to technologia oparta na danych. Mamy tu do czynienia z zaawansowanym procesem przetwarzania danych osobowych przez systemy komputerowe symulujące ludzkie myślenie. Proces ten nie jest związany wyłącznie z rozwojem przemysłowym i powstaniem nowych form działalności gospodarczej. Skutki rozwoju tej technologii mają również wymiar prawny, społeczny i etyczny.

1 ROZMOWA Z EKSPERTEM

Wymaga to od nas dogłębnego przyjrzenia się wielu obszarom, które z pozoru mogą wydawać się nam niezwiązane z techniczną czy informatyczną stroną zagadnienia, jak np. modele pomocy społecznej czy edukacji.

Podążanie za zasadami etycznymi w procesie tworzenia i wdrażania rozwiązań SI to konieczność i wymóg prawny, który powinien być wyraźnie sformułowany przez ustawodawcę. Konieczne jest pilne uregulowanie kwestii prawnych związanych z powstawaniem i wdrażaniem technologii SI, a także stały monitoring wszelkich zmian wprowadzonych do tego prawa. Zadanie to powinno być realizowane w porozumieniu z twórcami systemu sztucznej inteligencji, podmiotami wykorzystującymi tę technologię, a także z organizacjami społecznymi i środowiskiem naukowym. W tym obszarze konieczna jest bowiem szeroka platforma porozumienia, bo tylko ona daje gwarancje najlepszego wyważenia racji i przyczyni się do zwiększenia zarówno poczucia bezpieczeństwa przy prowadzeniu działalności naukowej czy biznesu, jak i pewności obowiązujących praw i wolności obywatelskich. Ważne jest, aby regulacje prawne dotyczące. technologii SI nie naruszały spójności prawa o ochronie danych osobowych i nie doprowadziły do nadmiernej inwigilacji obywateli czy niekontrolowanego profilowania osób.

Czy RODO wystarczająco chroni konsumentów przed nadmiernym wykorzystaniem ich danych osobowych przez sztuczną inteligencję? Czy potrzebne są zmiany w prawie regulujące tą kwestię?

Zautomatyzowane podejmowanie decyzji oraz profilowanie stanowią główną bramę, przez którą do naszego życia wkraczają algorytmy sztucznej inteligencji. Ci, którzy zamierzają wykorzystać sztuczną inteligencję do np. budowania profili konsumenckich i podejmowania decyzji, muszą liczyć się z ograniczeniami, które na ich działania nakłada ogólne rozporządzenie o ochronie danych – mając na uwadze prawa osób, których dane dotyczą (prawo do sprostowania, usunięcia danych, itd.). Zdarza się, że firmy wprowadzają dobre praktyki, takie jak opracowywanie wewnętrznych polityk, wytycznych w zakresie tworzenia i wdrażania technologii sztucznej inteligencji. Powoływane są też wewnętrzne zespoły reagujące w sytuacjach spornych lub kiedy wykorzystanie danego rozwiązania może podważyć zaufanie do technologii czy narazić na szwank dobro użytkownika.

Rozwój SI jest uzależniony od dostępu do informacji i danych osobowych. Kluczowe zatem jest stworzenie sprawnych programów gromadzenia danych oraz zarządzania nimi na potrzeby edukacji i badań nad rozwojem technologii SI.

Rozwój SI jest uzależniony od dostępu do informacji i danych osobowych. Kluczowe zatem jest stworzenie sprawnych programów gromadzenia danych i zarządzania nimi na potrzeby edukacji i badań nad rozwojem technologii SI.

1 ROZMOWA Z EKSPERTEM

Musimy pamiętać, że za konkretne rozwiązania informatyczne ZAWSZE odpowiedzialny jest człowiek, który je stworzył i wdrożył. Zasady odpowiedzialności za produkt czy usługę powinny być tutaj podobne do innych obszarów działalności człowieka.

Chodzi o zgodne z prawem ochrony danych zapewnienie jednostkom badawczym czy działom badań dostępu do danych. Niezmiernie istotny jest temat budowania zaufanych ekosystemów lub jednolitych wirtualnych hurtowni danych (data warehouse), które dzięki architekturze otwartych danych, umożliwią pracę nad technologią SI z pełnym zachowaniem zgodności z ogólnym rozporządzeniem o ochronie danych.
Musimy pamiętać, że za konkretne rozwiązania informatyczne zawsze odpowiedzialny jest człowiek, który je stworzył i wdrożył. Zasady odpowiedzialności za produkt czy usługę powinny być tutaj podobne do innych obszarów działalności człowieka. Odpowiedzialnością twórcy jest również okresowe sprawdzanie czy dane rozwiązanie wytrzymuje próbę czasu, czy nie pojawiają się nowe uwarunkowania, które mogą zaburzyć poprawne działanie danego produktu czy usługi opartej na technologii sztucznej inteligencji.
Warto mieć świadomość, że prawo zawsze będzie miało trudności z nadążaniem za rozwojem społeczeństwa, również w kontekście rozwoju technologicznego. Na szczęście RODO stanowi doskonały fundament, na którym można budować działania w obszarze dostosowania nowych technologii do stale ewoluujących potrzeb ochrony praw jednostki. Pamiętajmy jednak, że prawo podąża za rozwojem nowych technologii, a nie, że je wyprzedza. Obecnie istnieje potrzeba stworzeni globalnych, międzynarodowych ram prawnych dla rozwoju i wdrażania sztucznej inteligencji, by móc zapobiec niezgodnemu z prawem wykorzystywaniu tej technologii.

Jakimi zasadami powinni się kierować twórcy SI, aby technologia ta była bezpieczna dla ludzi w kontekście ochrony danych osobowych?
Zarówno sztuczna inteligencja, jak i technologie uczenia maszynowego powinny być projektowane, opracowywane i stosowane w sposób odpowiedzialny z poszanowaniem podstawowych praw człowieka. Zasady ochrony danych powinny być brane pod uwagę już na etapie projektowania rozwiązań czy systemów. Konieczne jest też zapewnienie przejrzystości i właściwego rozumienia SI. Ludzie korzystający z technologii sztucznej inteligencji powinni mieć pełną informację o tym, że właśnie wchodzą w interakcję z „systemem", że przekazują do niego swoje dane i powinni wyrazić na to zgodę.

Technologia SI daje na ogromne możliwości, należy jednak zachować ciągłą uwagę i czujność oraz odpowiedzialność za skutki związane z jej wykorzystaniem. Gotowe narzędzie wykorzystujące technologię SI powinny gwarantować, że nie niosą ze sobą istotnych zagrożeń.

1 ROZMOWA Z EKSPERTEM

W świecie nauki czy e-biznesu wykorzystującego zdobycze nowych technologii ważne jest wzajemne zaufanie odbiorców usług, kontrahentów i usługodawców, a także pewność prawa w tym obszarze. Chodzi tu szczególnie o zaufanie użytkownika do konkretnego rozwiązania technologicznego.

Technologia SI daje na ogromne możliwości, należy jednak zachować ciągłą uwagę i czujność oraz odpowiedzialność za skutki związane z jej wykorzystaniem.
Gotowe narzędzie wykorzystujące technologię SI powinny gwarantować, że nie niosą ze sobą istotnych zagrożeń społecznych w postaci niesprawiedliwego traktowania odbiorcy, np. w postaci wykluczenia czy niedostępności rozwiązania dla osób, np. o określonej narodowości czy kolorze skóry. Ważna jest też pewność, że przyjęte rozwiązania nie będą w stanie posłużyć do celów takich jak niszczenie praw i wolności obywatelskich, bez względu na to w czyich rękach się znajdą.
W świecie nauki czy e-biznesu wykorzystującego zdobycze nowych technologii ważne jest wzajemne zaufanie odbiorców usług, kontrahentów i usługodawców, a także pewność prawa w tym obszarze. Chodzi tu szczególnie o zaufanie użytkownika do konkretnego rozwiązania technologicznego i ogólnie do technologii informatycznych oraz ich długofalowych skutków społecznych i ekonomicznych.

Dziękuję za rozmowę.

2 UODO SYGNALIZUJE

„LAPTOP DLA UCZNIA” – ODPOWIEDZIALNOŚĆ ZA OBOWIĄZKI ZWIĄZANE Z OCHRONĄ DANYCH OSOBOWYCH

Przy realizacji programu „Laptop dla ucznia” status administratora danych przysługuje organowi prowadzącemu szkołę.

Kto – w związku z realizacją programu „Laptop dla ucznia”, w tym zawieraniem umowy użyczenia komputera przenośnego typu laptop rodzicowi ucznia klasy objętej wsparciem – jest administratorem danych i tym samym ma obowiązek spełnienia obowiązku informacyjnego wynikającego z RODO? Z takimi pytaniami w ostatnim czasie zwracali się do UODO inspektorzy ochrony danych.

W odpowiedzi organ nadzorczy wskazywał, że zgodnie z art. 7 ust. 3 ustawy z dnia 7 lipca 2023 r. o wsparciu rozwoju kompetencji cyfrowych uczniów i nauczycieli przekazanie laptopa uczniowi klasy objętej wsparciem, następuje na podstawie umowy zawartej przez organ prowadzący szkołę z rodzicem ucznia.

Stosownie do art. 7 ust. 5 organ prowadzący szkołę sporządza protokół z przekazania laptopa. Wzór umowy użyczenia komputera przenośnego typu laptop został określony w załączniku do rozporządzenia Ministra Cyfryzacji z dnia 8 września 2023 r. w sprawie określenia wzoru umowy użyczenia komputera przenośnego typu laptop rodzicowi ucznia klasy objętej wsparciem. Ze wzoru tej umowy (w tym § 1 pkt 4) wynika, że to organ prowadzący szkołę jest stroną umowy (reprezentowaną przez upoważnioną osobę z danej szkoły, zazwyczaj jej dyrektora) i użycza nowy, nieużytkowany i sprawny technicznie komputer przenośny typu laptop (§ 2 ust. 1 wzoru umowy) oraz odpowiada za obowiązki związane z ochroną danych osobowych dziecka i rodzica. Wśród tych obowiązków wskazane jest wypełnienie wobec biorącego w użyczenie obowiązku informacyjnego przewidzianego w art. 13 RODO (§ 5 ust. 2 wzoru umowy).

W związku z powyższym to organowi prowadzącemu szkołę, a nie szkole, należy przyznać status administratora w rozumieniu art. 4 pkt 7 RODO.

KWALIFIKACJA DO UCZESTNICTWA W KLUBIE SENIOR+ BEZ RODZINNEGO WYWIADU ŚRODOWISKOWEGO

Obecnie nie ma podstaw prawnych, by na potrzeby kwalifikacji do uczestnictwa w Klubie Senior+ w każdym przypadku przeprowadzać rodzinny wywiad środowiskowy.

Taką opinię UODO przedstawił, odpowiadając na pytanie jednego z inspektorów ochrony danych (IOD) oraz kierując do Minister Rodziny i Polityki Społecznej wniosek o rewizję „Stanowiska w sprawie kwalifikowania do uczestnictwa w klubach samopomocy (uczestnictwo w Klubie Senior+)".

Przyczyna wątpliwości IOD

Z wątpliwościami w tym zakresie zwrócił się do UODO jeden z IOD. Wskazał, że na obowiązek przeprowadzania rodzinnego wywiadu środowiskowego wobec osób chcących uczestniczyć w zajęciach Klubu „Senior+" wskazuje Ministerstwo Rodziny i Polityki Społecznej w opublikowanym na stronie internetowej senior.gov.pl „Stanowisku w sprawie kwalifikowania do uczestnictwa w klubach samopomocy (uczestnictwo w Klubie Senior+)". Resort stwierdza w nim wprost, że w przypadku udzielania świadczeń z pomocy społecznej, jak również „w przypadku udzielenia świadczenia w postaci uczestnictwa w zajęciach klubu samopomocy należy przeprowadzić rodzinny wywiad środowiskowy".

W opinii IOD obowiązek przeprowadzania rodzinnego wywiadu środowiskowego w celu kwalifikacji do uczestnictwa w Klubie Senior+ nie wynika z żadnego przepisu prawa. Biorąc zaś pod uwagę, jak wiele danych osobowych pozyskuje się za pośrednictwem takiego wywiadu, pytał, czy jego przeprowadzanie w analizowanym przypadku nie naruszałoby określonych w RODO zasad minimalizacji danych i ograniczenia celu.

Stanowisko UODO

W odpowiedzi UODO wskazał, że celem strategicznym (ustanowionego uchwałą nr 191 Rady Ministrów z dnia 21 grudnia 2020 r.) Programu wieloletniego „Senior+" na lata 2021-2025 jest zwiększenie aktywnego uczestnictwa seniorów – osób nieaktywnych zawodowo w wieku 60 lat i więcej – w życiu społecznym. Służyć ma temu m.in. dofinansowanie działań jednostek samorządu w rozwoju na ich terenie sieci Dziennych Domów „Senior+" i Klubów „Senior+". Działalność Klubu „Senior+" polegać ma zaś na motywowaniu seniorów do działań na rzecz samopomocy i działań wolontariackich na rzecz innych.

W punkcie IV.1.7 powołanego Programu wskazano, że „Dzienne Domy «Senior+» i Kluby «Senior+» są ośrodkami wsparcia, o których mowa w art. 51 ust. 4 ustawy o pomocy społecznej. Dzienny Dom «Senior+» jest dziennym domem pomocy, natomiast Klub «Senior+» jest klubem samopomocy.

2 UODO SYGNALIZUJE

Zasady funkcjonowania ośrodków wsparcia oraz tryb kwalifikowania osób do uczestnictwa w działaniach realizowanych przez ośrodki są określone w ustawie o pomocy społecznej (m.in. art. 106 dotyczący przyznania świadczeń)".

W ocenie UODO wprawdzie powołany w Programie art. 106 ustawy o pomocy społecznej stanowi, że przyznanie świadczeń z pomocy społecznej następuje w formie decyzji administracyjnej (ust. 1), a także że decyzję administracyjną o przyznaniu lub odmowie przyznania świadczenia, z wyjątkiem decyzji o odmowie przyznania biletu kredytowanego oraz decyzji w sprawach cudzoziemców i osób, o których mowa w art. 5a, wydaje się po przeprowadzeniu rodzinnego wywiadu środowiskowego (ust. 4), to istotny w tym przypadku jest ust. 2 powołanego przepisu. Stanowi on, że udzielenie świadczeń m.in. w postaci uczestnictwa w zajęciach klubu samopomocy nie wymaga wydania decyzji administracyjnej.

Przeprowadzenie wywiadu środowiskowego jest zatem co do zasady obligatoryjną czynnością organu przed dokonaniem rozstrzygnięcia w sprawie w drodze decyzji administracyjnej przyznającej prawo do świadczenia z pomocy społecznej lub takiego prawa odmawiającej. Tym samym w przypadkach, gdy nie jest wymagane wydanie decyzji administracyjnej, nie jest wymagane także przeprowadzenie wywiadu środowiskowego.

Zatem w sytuacji, gdy udzielenie świadczeń w postaci uczestnictwa w zajęciach klubu samopomocy nie następuje w drodze decyzji administracyjnej, nie jest wymagane przeprowadzenie wywiadu środowiskowego. Na taką interpretację powołanych wyżej przepisów wskazuje się również w doktrynie (np. w publikacji „Rodzinny wywiad środowiskowy w praktyce", red. Adam Lisowski, dostępnej w portalu informacji prawniczej Legalis).

Jednocześnie UODO podniósł, że dokonując oceny przedstawionego zagadnienia, należy mieć na uwadze, określoną w art. 7 Konstytucji RP, zasadę działania organów publicznych na podstawie i w granicach prawa. Oznacza ona, że organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. A zatem każdy administrator jest obowiązany do zbadania, czy istnieją właściwe podstawy prawne do przetwarzania (w tym pozyskiwania) określonych danych osobowych.

Dodatkowo, oceniając zakres pozyskiwanych danych, administrator musi pamiętać, że przetwarzanie danych musi być zgodne z zasadami ochrony danych osobowych określonymi w art. 5 RODO, w tym zasadą minimalizacji oraz z zasadą ograniczenia celu.

UODO podkreślił, że przeprowadzając rodzinny wywiad środowiskowy, administrator pozyskuje bardzo szeroki zakres danych osobowych, w tym danych szczególnych kategorii, a także danych osób trzecich.

Jeśli zaś jedynymi kryteriami uczestnictwa w Klubie „Senior +" są określony wiek oraz brak aktywności zawodowej, trudno byłoby uznać, że aby zweryfikować spełnianie tych kryteriów, niezbędne są wszystkie dane pozyskiwane w wywiadzie, a tym samym, aby pozyskiwanie tych danych było zgodne z zasadą minimalizacji. W analizowanej sytuacji administrator powinien przyjmować rozwiązania, które nie będą powodowały pozyskiwania nadmiarowych danych osobowych.

Wniosek o zmianę stanowiska

Żeby do tego nie dochodziło, Prezes UODO zwrócił się do Minister Rodziny i Polityki Społecznej o zmianę opublikowanego na stronie internetowej stanowiska resortu.

Oprócz powyższych argumentów dodatkowo podniósł, że powoływanie się w nim na art. 104 ust. 3 ustawy o pomocy społecznej, zgodnie z którym „wysokość należności z tytułu wydatków na świadczenia z pomocy społecznej oraz z tytułu opłat określonych przepisami ustawy o pomocy społecznej (w tym także odpłatności za korzystanie z usług ośrodka wsparcia) podlegających zwrotowi oraz terminy ich zwrotu ustala się jedynie w drodze decyzji administracyjnej", zauważyć należy, że przepis ten dotyczy innych sytuacji, tj. takich, w których organ zamierza dochodzić zwrotu wydatków poniesionych w związku z udzieloną pomocą. Przepis ten ma zatem zastosowanie wówczas, gdy organ zamierza dochodzić zwrotu należności, nie zaś na etapie przyznawania świadczenia. Podstawy prawnej do przeprowadzenia wywiadu środowiskowego w omawianej sytuacji nie kształtuje także art. 97 ust. 5 ustawy o pomocy społecznej, dotyczący odpłatności m.in. za pobyt w ośrodkach wsparcia, zwłaszcza w sytuacji, gdy uczestnictwo w Klubach „Senior+" w wielu przypadkach jest nieodpłatne albo też w sytuacji rezygnacji seniora z uczestnictwa w takim Klubie. Wskazywać to może na występowanie różnych rozwiązań dotyczących finansowania kosztów uczestnictwa w Klubie „Senior+". Dlatego w zależności od tego, czy uczestnictwo będzie odpłatne, czy też nieodpłatne, a także w jaki sposób będzie ustalana wysokość opłaty, różny może być sposób procedowania zgłoszeń seniorów.

Ponadto jak wskazuje się w doktrynie „wywiad nie jest jedynym możliwym dowodem, a w postępowaniu w sprawie świadczeń z pomocy społecznej należy dopuścić także inne dowody z odpowiednim zastosowaniem Kodeksu postępowania administracyjnego, zwłaszcza gdy występują przeszkody w przeprowadzeniu wywiadu." (I. Sierpowska [w:] Pomoc społeczna. Komentarz, wyd. VI, Warszawa 2023, art. 107.)

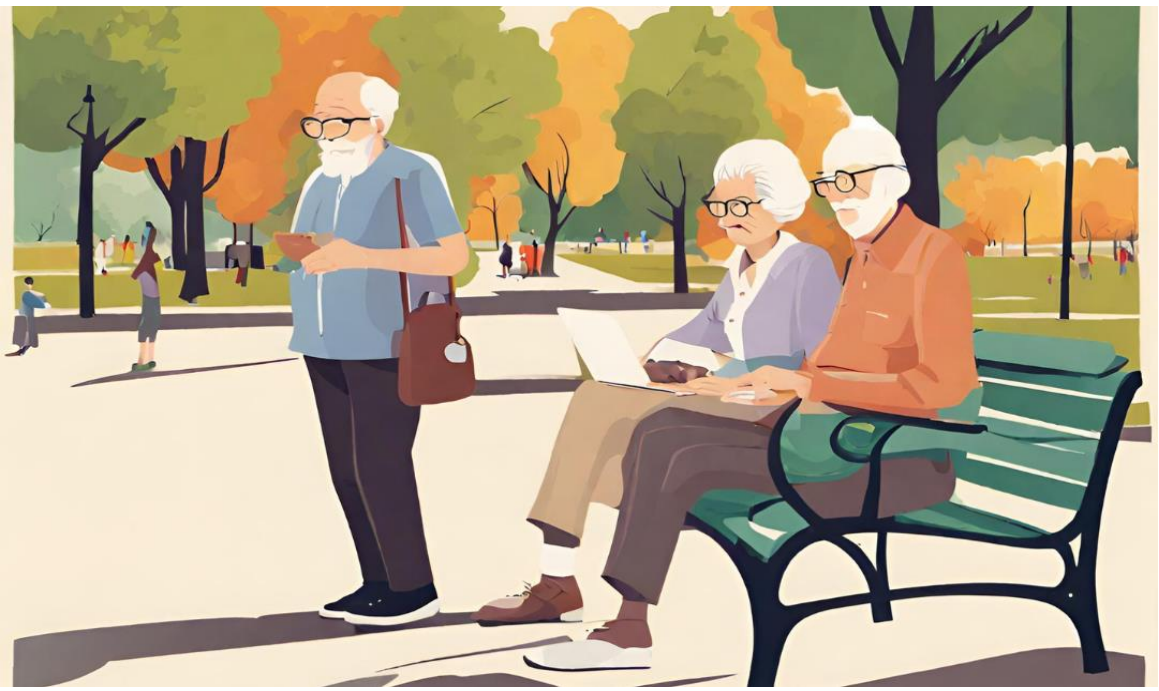
Jeśli jedynymi kryteriami uczestnictwa w Klubie „Senior +" są określony wiek oraz brak aktywności zawodowej, trudno byłoby uznać, że aby zweryfikować spełnianie tych kryteriów, niezbędne są wszystkie dane pozyskiwane w wywiadzie.

2 UODO SYGNALIZUJE

Wobec tego przyjęcie założenia, iż w każdym przypadku kwalifikowania do uczestnictwa w Klubie „Senior+” niezbędne jest przeprowadzenie rodzinnego wywiadu środowiskowego może być dezorientujące i prowadzić do nieuzasadnionego pozyskiwania zbyt szerokiego zakresu informacji, w tym danych osobowych.

W związku z tym Prezes UODO zwrócił się do Minister Rodziny i Polityki Społecznej o podjęcie działań mających na celu rewizję „Stanowiska w sprawie kwalifikowania do uczestnictwa w klubach samopomocy (uczestnictwo w Klubie Senior+)” poprzez rezygnację ze wskazywania na obowiązek przeprowadzania rodzinnego wywiadu środowiskowego we wszystkich przypadkach kwalifikowania osób do uczestnictwa w Klubie „Senior+”.

Obowiązujące przepisy kształtują obowiązek przeprowadzenia wywiadu środowiskowego w ściśle określonych warunkach prawnych, a mianowicie jedynie w sytuacji wydawania decyzji administracyjnej. Przeprowadzenie wywiadu środowiskowego jest bowiem ze swej istoty czynnością znacznie ingerującą w prywatność człowieka i nie ma podstaw domniemywania obowiązku realizacji takiej czynności w innych warunkach niż przewidziane w obowiązujących przepisach prawa. Jeżeli zatem udzielenie świadczenia w postaci skierowania do uczestnictwa w zajęciach klubu samopomocy nie następuje w drodze decyzji administracyjnej, nie ma podstaw do wymagania przeprowadzenia wywiadu środowiskowego.



KOGO NALEŻY INFORMOWAĆ O MOŻLIWOŚCI POPEŁNIENIA PRZESTĘPSTWA W ZWIĄZKU ZE ZGŁASZANIEM KANDYDATÓW NA POSŁÓW I SENATORÓW?

O podejrzeniu popełnienia przestępstwa z zakresu ochrony danych osobowych w związku ze zgłaszaniem kandydatów na posłów i senatorów należy zawiadamiać organy ścigania. Informacje dotyczące czynów zabronionych nie powinny być kierowane do Prezesa UODO z oczekiwaniem przeprowadzenia postępowania pod kątem ustalenia naruszenia przepisów karnych z zakresu ochrony danych osobowych.

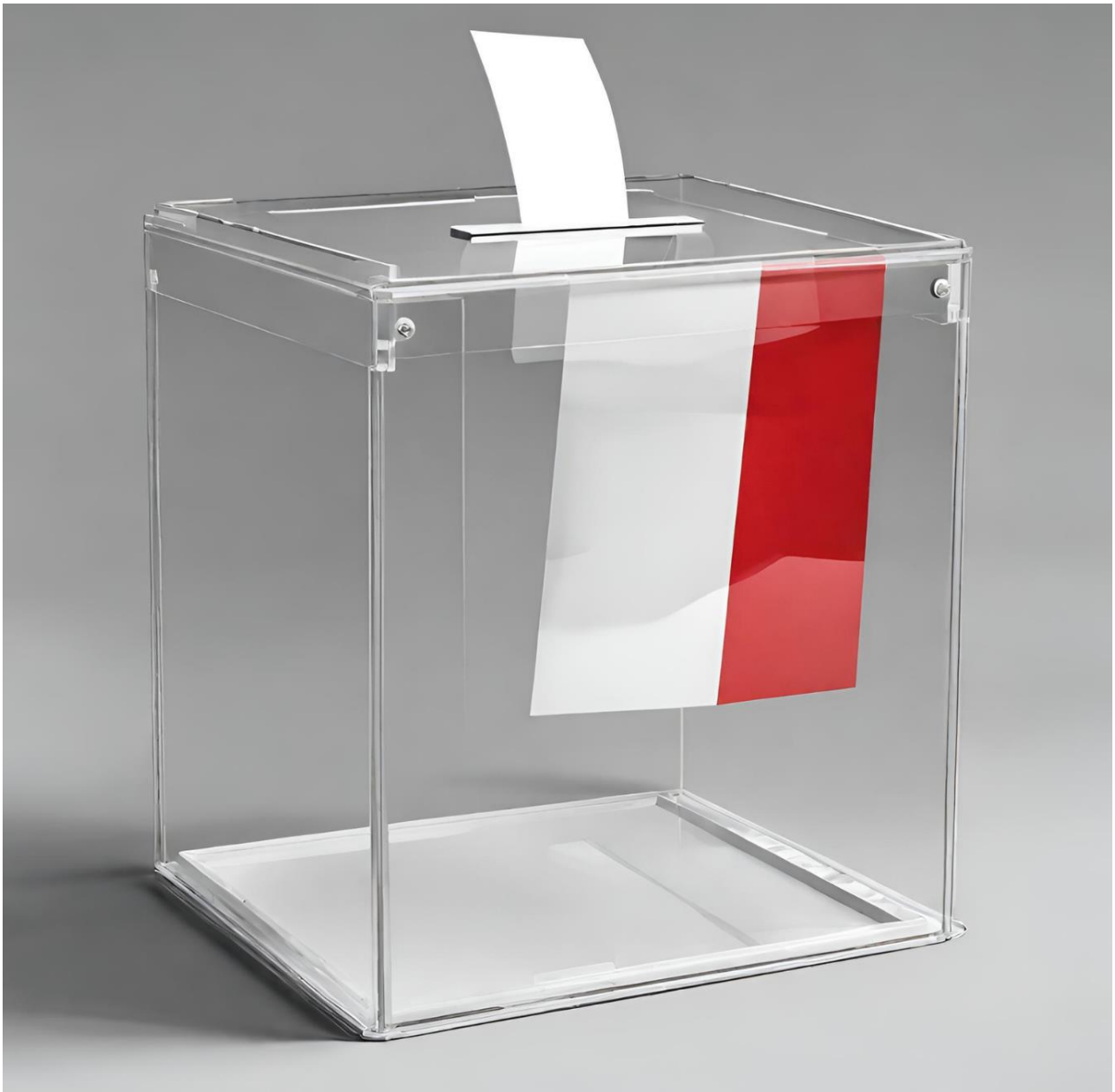
W okresie przedwyborczym do Urzędu Ochrony Danych Osobowych (UODO) wpływały liczne zawiadomienia o możliwości bezprawnego przetwarzania danych osobowych w związku ze zgłaszaniem kandydatów na posłów i senatorów. Ich nadawcy wskazywali, że w konkretnym przypadku mogło dojść do nadużyć w zakresie ochrony danych osobowych, gdyż na złożonych do okręgowej komisji wyborczej listach poparcia dla określonych osób kandydujących w wyborach parlamentarnych, znalazły się np. dane nieprawdziwe albo dane osób zmarłych. Zgłoszenia dotyczyły też prawdopodobnego nieuprawnionego wykorzystania danych osobowych zgromadzonych w różnego rodzaju bazach danych, a więc przetwarzania danych osobowych wyborców bez ich wiedzy.

Niewłaściwe przypisanie kompetencji

Przypomnieć jednak należy, że przyznane organowi nadzorczemu w przepisach RODO uprawnienia, nie przewidują prowadzenia postępowań pod kątem ustalenia naruszenia przepisów karnych z zakresu ochrony danych osobowych.

W takie kompetencje zostały wyposażone organy ścigania, tj. m.in. policja i prokuratura, które są uprawnione i zobowiązane do kompleksowej oceny prawnokarnej czynów, których dotyczą przesyłane zawiadomienia.

Bezprawne – w rozumieniu art. 107 ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. – przetwarzanie danych osobowych stanowi przestępstwo ścigane z urzędu. Stosownie zaś do art. 304 ust. 1 Kodeksu postępowania karnego, każdy, kto dowiedział się o popełnieniu przestępstwa ściąganego z urzędu, zobowiązany jest do powiadomienia prokuratora lub policji.



Organy ścigania ocenią wszystkie aspekty czynu

Wskazać zatem należy, że o możliwości popełnienia przestępstwa powiadomić należy prokuraturę lub policję. I jest to działanie wystarczające. Prokuratura i policja są bowiem tymi organami, które są uprawnione do kompleksowej oceny prawnokarnej czynu, również z punktu widzenia ewentualnego naruszenia zasad ochrony danych osobowych.

Ochrona danych osobowych w kampanii wyborczej – poradnik UODO

Jednocześnie warto przypomnieć, że wszystkie podmioty zaangażowane w kampanię wyborczą muszą przestrzegać nie tylko przepisów bezpośrednio regulujących jej przebieg, ale również przepisów o ochronie danych osobowych. Żeby im to ułatwić, UODO przygotował poradnik pt. „Ochrona danych osobowych w kampanii wyborczej”.

SPROSTOWANIE IMIENIA NIE TAKIE PROSTE. CZY ADMINISTRATOR MOŻE ZWLEKAĆ Z REALIZACJĄ ŻĄDANIA POPRAWIENIA NIEPRAWIDŁOWYCH DANYCH?

Organ nadzorczy udzielił upomnienia za brak niezwłocznego uwzględnienia żądania sprostowania danych oraz niedochowanie zaleceń przejrzystego informowania i komunikowania. Decyzja została zainicjowana skargą na bezskuteczne, ponawiane przez wiele miesięcy żądanie skarżącego o poprawienie nieprawidłowego imienia widniejącego w systemie administratora.

Skarżący zauważył, że na potwierdzeniach przelewów realizowanych z rachunku bankowego, którego jest wraz z żoną współwłaścicielem, widnieje nie jego imię (P. zamiast M.). Natychmiast po zauważeniu błędu żona skarżącego wystąpiła do banku ze stosownym zgłoszeniem i prośbą o jego sprostowanie. To pierwsze zgłoszenie okazało się dopiero wstępem do kolejnych, nieudanych, podejmowanych na przestrzeni wielu miesięcy i za pomocą wszelkich kanałów komunikacji, prób skłonienia administratora do realizacji tego, zdawałoby się prostego żądania.

Skarżący i jego żona zdecydowali się następnie skorzystać z uprawnienia jakie daje art. 16 RODO i wystąpili do inspektora ochrony danych osobowych banku z wnioskiem o zaktualizowanie danych osobowych Skarżącego. Również i na tym etapie sprawa nie znalazła jednak szczęśliwego zakończenia. Pomimo zapewnień ze strony pracownika banku o naprawieniu błędu, na wyciągu rachunku bankowego skarżącego wciąż widniało nie jego imię. Po tym niepowodzeniu pan M., a zdaniem banku nadal pan P., wniósł skargę do Prezesa Urzędu Ochrony Danych Osobowych z żądaniem nakazania administratorowi dokonania stosownego sprostowania.

Niezwłoczne sprostowanie danych i zasada ich prawidłowego przetwarzania

Rozpatrując skargę organ nadzorczy w pierwszej kolejności przypomniał, że zgodnie z treścią art. 16 RODO osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Organ zauważył również, że w doktrynie prawo to kojarzone jest z zasadą prawidłowości danych (merytorycznej poprawności) określonej w art. 5 ust. 1 lit. d RODO, zgodnie z którą dane osobowe powinny być prawidłowe i w razie potrzeby uaktualnianie, a administrator danych powinien podjąć wszelkie rozsądne działania, aby nieprawidłowe dane zostały niezwłocznie usunięte lub sprostowane. Sprostowanie takie może być dokonywane zarówno z inicjatywy administratora danych, jak i osoby, której dane dotyczą.

Organ nadzorczy udzielił upomnienia za brak niezwłocznego uwzględnienia żądania sprostowania danych oraz niedochowanie zaleceń przejrzystego informowania i komunikowania.

3 WYBRANE DECYZJE UODO

Rozpatrując skargę organ nadzorczy w pierwszej kolejności przypomniał, że zgodnie z treścią art. 16 RODO osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

Niezwłoczne sprostowanie danych i zasada ich prawidłowego przetwarzania

Rozpatrując skargę organ nadzorczy w pierwszej kolejności przypomniał, że zgodnie z treścią art. 16 RODO osoba, której dane dotyczą ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Organ zauważył również, że w doktrynie prawo to kojarzone jest z zasadą prawidłowości danych (merytorycznej poprawności) określonej w art. 5 ust. 1 lit. d RODO, zgodnie z którą dane osobowe powinny być prawidłowe i w razie potrzeby uaktualnianie, a administrator danych powinien podjąć wszelkie rozsądne działania, aby nieprawidłowe dane zostały niezwłocznie usunięte lub sprostowane. Sprostowanie takie może być dokonywane zarówno z inicjatywy administratora danych, jak i osoby, której dane dotyczą.

Żądaj, ale we własnym imieniu

Organ zwrócił również uwagę, że za skuteczne żądanie sprostowania danych można uznać dopiero to żądanie skarżącego, z którym wystąpił we własnym imieniu. W świetle przepisów rozporządzenia z takim żądaniem może bowiem wystąpić jedynie osoba, której dane dotyczą. Tym samym wcześniejszą korespondencję z bankiem, która była prowadzona z niedysponującą odpowiednim pełnomocnictwem żoną skarżącego, należy uznać za bezskuteczną.

Wnioskodawca powinien wiedzieć, co się dzieje z jego żądaniem. I to w wyznaczonym terminie.

Na skuteczną realizację uprawnienia do sprostowania nieprawidłowych danych składa się również obowiązek określony w art. 12 ust. 3 RODO, zgodnie z którym administrator udziela osobie, której dane dotyczą, informacji o podjętych, w związku z tym żądaniem, działaniach, którego to obowiązku administrator jednak nie dopełnił. Jak dalej wyjaśnia art. 12 ust. 3 administrator powinien udzielić takiej informacji bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania. Przedłużenie tego terminu o kolejne dwa miesiące może mieć jedynie wyjątkowy charakter i wiązać się ze skomplikowanym charakterem żądania lub liczbą żądań. O takim przedłużeniu osoba, która wniosła żądanie powinna zostać poinformowana w ciągu miesiąca ze wskazaniem przyczyn takiego przedłużenia. Również i w tym wypadku skarżący nie otrzymał jednak żadnego powiadomienia, co prowadzi do konkluzji, że administrator rozpatrywał żądanie skarżącego z całkowitym pominięciem wskazań, o których mowa w art. 12 ust. 3.

3 WYBRANE DECYZJE UODO

Administrator ma obowiązek sprostować dane niezwłocznie

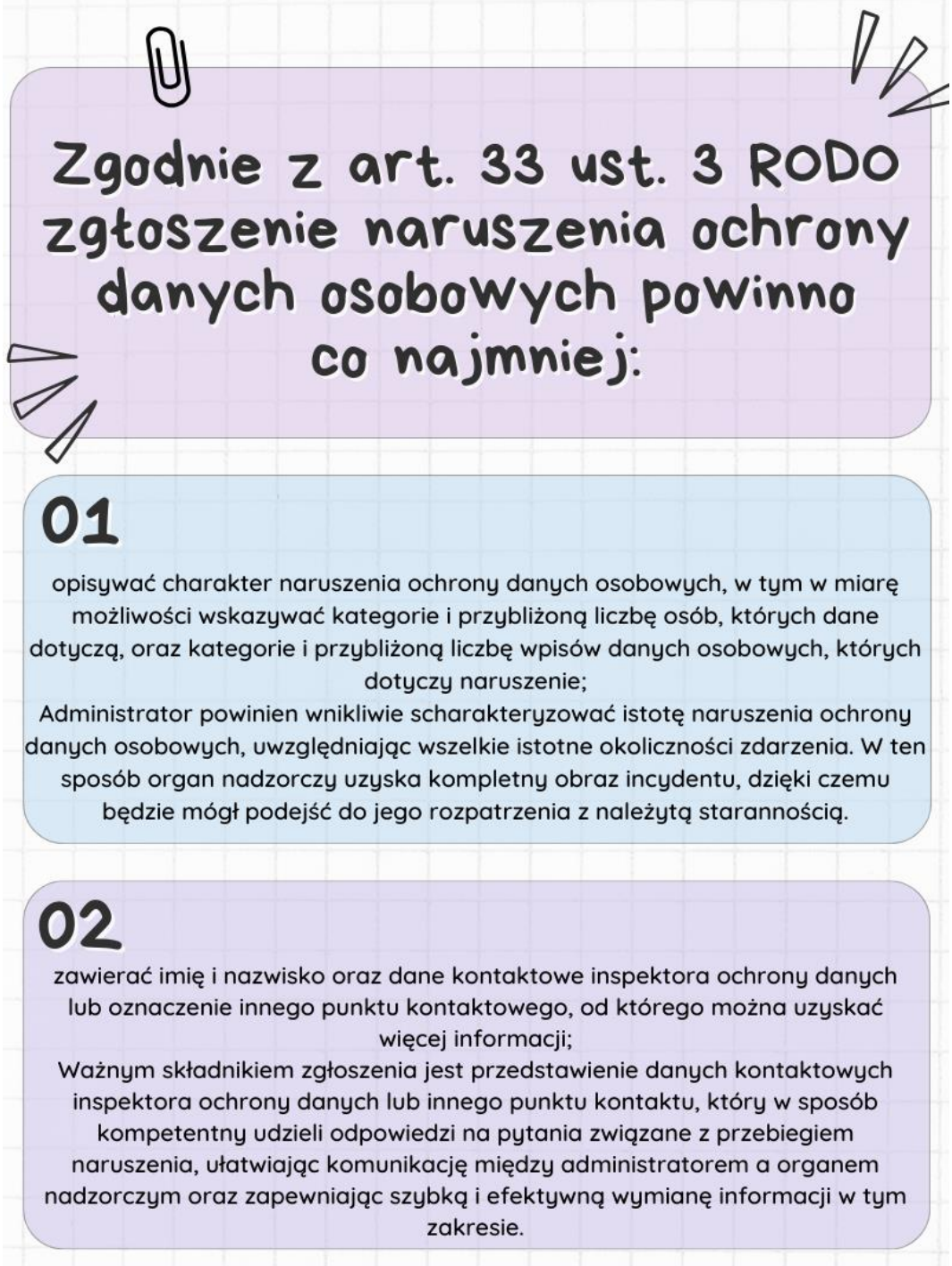
Organ stwierdził, że w niniejszej sprawie administrator nie uwzględnił żądania sprostowania danych niezwłocznie, czyli tak jak wymaga tego art. 16 RODO. Ostatecznie bowiem bank dokonał niezbędnej korekty imienia Skarżącego dopiero po kilku miesiącach od wniesienia skutecznego w myśl przepisów RODO żądania i już po zainicjowaniu postępowania skargowego przed organem nadzorczym. Biorąc powyższe pod uwagę Prezes UODO udzielił administratorowi upomnienia za naruszenie art. 16 w zw. z art. 12 ust. 3 rozporządzenia.

Nakładając na administratora upomnienie organ przypomniał, że obowiązek dochowania terminu o którym mowa w art. 16 RODO nie może być realizowany w sposób dowolny. Administrator powinien dążyć do jak najszybszej realizacji żądania podmiotu danych i podjąć w tym celu wszelkie rozsądne działania. Każde odstępstwo od tego obowiązku powinno zaś mieć swoje wyraźnie uzasadnienie, o którym podmiot danych powinien być terminowo i na bieżąco informowany.

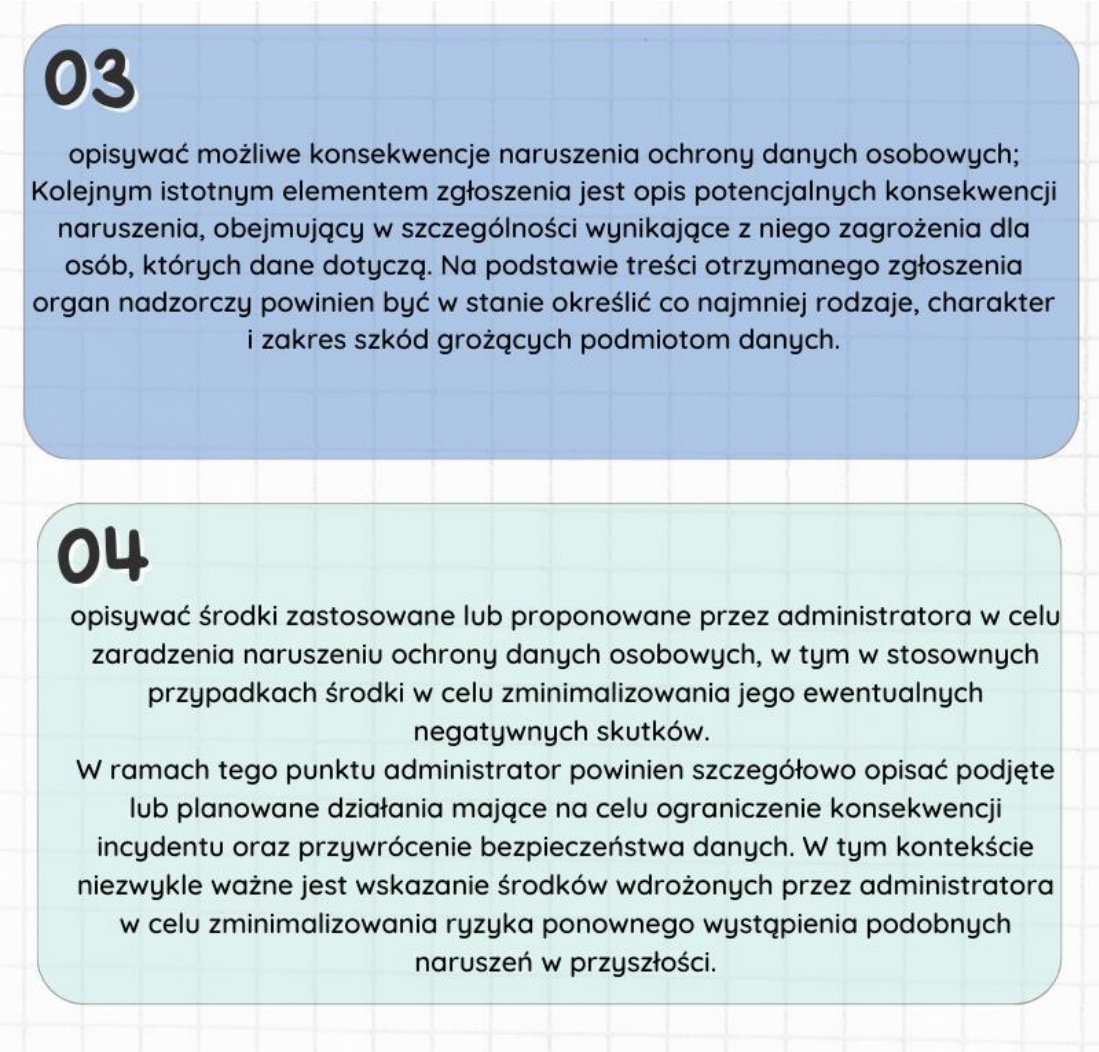
3 NARUSZENIA I KONTROLE

JAKIE INFORMACJE NALEŻY ZAWRZEĆ W ZGŁOSZENIU NARUSZENIA OCHRONY DANYCH OSOBOWYCH?

Konieczność bezzwłocznego zawiadamiania organu nadzorczego o naruszeniach ochrony danych osobowych, to jeden z kluczowych obowiązków administratorów przewidzianych w przepisach RODO. Odpowiednio przygotowane zgłoszenie, oprócz szczegółowych informacji dotyczących zaistniałego incydentu, powinno uwzględniać szereg dodatkowych elementów potrzebnych Prezesowi Urzędu Ochrony Danych Osobowych do realizacji swoich zadań. Dokonując kompletnych zgłoszeń, administratorzy mogą uniknąć zarzutów związanych z niedopełnieniem obowiązku notyfikacyjnego, a także usprawnić podejmowane przez organ nadzorczy czynności wyjaśniające.



4 NARUSZENIA I KONTROLE



Dodatkowe informacje, które warto zawrzeć w zgłoszeniu naruszenia

Opisane powyżej elementy stanowią podstawę skutecznego zgłoszenia naruszenia ochrony danych osobowych. Należy jednak pamiętać, iż art. 33 ust. 3 RODO ogranicza się do określenia wymagań minimalnych. W wielu sytuacjach uwzględnienie w treści zgłoszenia dodatkowych informacji pomoże w przedstawieniu organowi nadzorczemu pełnego obrazu sytuacji oraz dostarczeniu dowodów na zastosowanie się przez administratora do pozostałych regulacji przewidzianych przez przepisy RODO. W stosownych przypadkach konieczne może być więc m.in. podanie przyczyn opóźnienia w zgłoszeniu naruszenia czy wskazanie szczegółów dotyczących realizacji obowiązku zawiadomienia o naruszeniu osób, których dane dotyczą (art. 34 RODO).

Dedykowany formularz elektroniczny

Należy podkreślić, że RODO nie narzuca konkretnego sposobu dokonywania zgłoszeń i można to uczynić w dowolny sposób. Mimo to szczególnie zalecane jest korzystanie przez administratorów z dedykowanego formularza elektronicznego dostępnego na stronie internetowej Urzędu Ochrony Danych Osobowych (www.uodo.gov.pl). Skrupulatne wypełnienie go usprawni i usystematyzuje proces notyfikacji, pozwoli na zachowanie kompletności zgłoszenia oraz ułatwi organowi nadzorczemu realizację swoich zadań.

5 NOWE TECHNOLOGIE

URZĄDZENIA UBIERALNE – MODA, FUNKCJONALNOŚĆ CZY JEDNAK COŚ WIĘCEJ?

Rewolucja cyfrowa ciągle nabiera tempa, oferując nie tylko niezliczone nowe możliwości, ale również stawiając szereg wyzwań. Coraz większą popularność w ciągu ostatnich kilku lat zdobywają urządzenia ubieralne (wearable device). Kategoria ta zawiera wszelkiego rodzaju urządzenia elektroniczne przeznaczone do noszenia na ciele użytkownika, które przybierają różne formy, od biżuterii, przez wyroby medyczne, aż po odzież lub elementy ubioru. Jest to jedna z najbardziej popularnych i ogólnodostępnych kategorii urządzeń, które zaliczane są do koncepcji Internetu Rzeczy (ang. Internet of Things, IoT). Przynoszą wiele korzyści i możliwości, które wpływają na nasze życie codzienne w różnych dziedzinach, takich jak zdrowie, aktywność fizyczna, komunikacja czy rozrywka, jednak wraz z dynamicznym rozwojem tego segmentu pojawia się szereg kwestii związanych z ochroną danych osobowych i prywatnością użytkowników.

Jakie dane mogą gromadzić urządzenia ubieralne?

Urządzenia ubieralne regularnie badają wiele parametrów życiowych i w zależności od rodzaju, funkcji i zastosowań mogą zbierać różnorodne dane o użytkowniku w tym m.in. na temat tętna, ciśnienia krwi, temperatury ciała, czy lokalizacji.

Monitorowanie zdrowia: Urządzenia ubieralne często mierzą różne parametry, takie jak tętno, ciśnienie krwi, poziom tlenu we krwi (SpO2), poziom stresu, temperaturę ciała, a nawet elektrokardiogram (EKG).

Aktywność fizyczna: Niektóre urządzenia mogą także zbierać dane dotyczące kroków, dystansu, spalonych kalorii oraz czasu poświęconego na aktywność fizyczną, co umożliwia użytkownikowi monitorować codzienną aktywność i osiągane cele.

Monitorowanie snu: Taka funkcja obejmuje szereg parametrów i cech związanych m.in. z jakością i długością snu użytkownika.

Lokalizacja: Wiele urządzeń ubieralnych pozwala śledzić przebyte trasy, dystanse lub dostarczać informacji o położeniu.

Użytkowanie: Urządzenia mogą również zbierać dane na temat sposobu użytkowania, takie jak częstotliwość korzystania z różnych funkcji, preferencje użytkownika czy zachowania online.

Komunikacja i powiadomienia: Funkcja ta pozwala na odbieranie powiadomień, wiadomości SMS, połączeń telefonicznych i e-maili, co może wymagać dostępu do kontaktów i treści komunikatów.

5 NOWE TECHNOLOGIE

To tylko kilka przykładów, ale jak widać niezależnie od tego, czy jest to opaska fitness, smartwatch czy element garderoby, to ilość danych, które mogą gromadzić jest ogromna. Często są to również dane wrażliwe, które zgodnie z RODO podlegają szczególnej ochronie. Dla użytkowników oznacza to potrzebę świadomego korzystania z tych urządzeń, a dla producentów i dostawców obowiązek dostosowania się do przepisów prawnych i norm etycznych. Dlatego niezwykle ważne jest zrozumienie i przestrzeganie przepisów RODO oraz dbałość o prywatność, aby w pełni korzystać z możliwości tych urządzeń przy jednoczesnym zachowaniu ochrony naszych danych osobowych. RODO przewiduje wiele wymogów koniecznych do zastosowania w celu przetwarzania danych osobowych, między innymi obowiązek oceny skutków oraz minimalizowanie ryzyka. W tym miejscu warto wspomnieć, że w komunikacie opublikowanym przez Prezesa Urzędu Ochrony Danych Osobowych w sprawie **wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków** przetwarzania dla ich ochrony wskazano m.in. innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych, co swoim zakresem może obejmować systemy stosowane do analizy i przekazywania danych dostawcom usługi przy użyciu aplikacji mobilnych z urządzeń przenośnych typu: smartwatch, inteligentne opaski, beacony itp. analizujące i przekazujące dane dostawcom przy użyciu aplikacji mobilnych.

„Co do zasady, przetwarzanie spełniające przynajmniej dwa ze wskazanych kryteriów będzie wymagać oceny skutków dla ochrony danych. W niektórych przypadkach administrator danych może jednak uznać, że przetwarzanie spełniające tylko jedno z wymienionych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych. Im więcej kryteriów spełnia przetwarzanie, tym bardziej prawdopodobne jest wystąpienie wysokiego ryzyka naruszenia praw lub wolności podmiotów danych, a w konsekwencji, niezależnie od środków przewidzianych przez administratora do zastosowania, wymagana będzie ocena skutków dla ochrony danych.”
Źródło: Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

5 NOWE TECHNOLOGIE

Ponadto administrator musi dostarczyć użytkownikowi kompleksowych wyjaśnień na temat działania danej technologii zgodnie z art. 13 i 14 RODO i uzyskać wyraźną, jednoznaczną i dobrowolną zgodę użytkownika na zbieranie, przetwarzanie i przechowywanie danych osobowych. Zgoda powinna być łatwo dostępna i możliwa do wycofania w dowolnym momencie. Warto jednak podkreślić, że często brak zgody na przetwarzanie danych przez urządzenie ubieralne może skutkować ograniczeniem wielu funkcjonalności, w związku z tym, pojawia się pytanie czy zgoda udzielona przez użytkownika rzeczywiście ma charakter dobrowolny zgodnie z art. 4 ust. 11 RODO. Należy również pamiętać, że użytkownik ma prawo żądać dostępu do swoich danych (art. 15 RODO), sprostowania (art. 16 RODO), ograniczenia przetwarzania (art. 18 RODO), oraz ich usunięcia (art. 17 RODO). Niewystarczająca wiedza na temat praw jakie przysługują użytkownikom inteligentnych urządzeń może prowadzić do wielu nadużyć ze strony producentów, a co za tym idzie brak kontroli nad przetwarzaniem przekazanych informacji, które często stanowią dane osobowe.

Podsumowując, urządzenia ubieralne bez wątpienia niosą ze sobą wiele korzyści, ale jednocześnie stwarzają szereg wyzwań związanych z ochroną danych osobowych. Warto, aby użytkownicy byli świadomi tych kwestii i podejmowali właściwe środki ostrożności, a także aby organizacje i producenci tych urządzeń przestrzegali odpowiednich regulacji oraz dbali o bezpieczeństwo i prywatność swoich użytkowników.

6 SPRAWY MIĘDZYNARODOWE

345 MLN EURO KARY DLA TIKTOKA

Po orzeczeniu Europejskiej Rady Ochrony Danych irlandzki organ ochrony danych nałożył na spółkę TikTok Technology Limited (TikTok) karę 345 mln euro za nieprawidłowe przetwarzanie danych osobowych dzieci.

Irlandzki organ nadzorczy wydał ostateczną decyzję, w której stwierdził w szczególności naruszenie przez spółkę TikTok zasady rzetelności RODO podczas przetwarzania danych osobowych dzieci w wieku od 13 do 17 lat.

Ostateczna decyzja irlandzkiego organu ochrony danych uwzględnia ocenę prawną wyrażoną przez EROD w jej wiążącej decyzji. Decyzja ta została przyjęta na podstawie art. 65 ust. 1 lit. a RODO po tym, jak irlandzki organ ochrony danych, jako wiodący organ nadzorczy, uruchomił procedurę rozstrzygnięcia sporu dotyczącego sprzeciwów wniesionych przez organy, których sprawa dotyczy. Decyzja EROD została wydana 2 sierpnia 2023 r. i obejmuje działania związane z przetwarzaniem danych przez TikToka w okresie od 31 lipca do 31 grudnia 2020 r.

EROD przeanalizowała praktyki projektowania stosowane przez TikToka w kontekście dwóch wyskakujących powiadomień, wyświetlanych dzieciom: wyskakującego okienka rejestracji i wyskakującego okienka zamieszczania filmów. Analiza wykazała, że obydwa wyskakujące okienka nie przedstawiały użytkownikowi opcji wyboru w obiektywny i neutralny sposób. Użytkownicy byli zachęcani do wyboru domyślnych ustawień publicznych, a TikTok utrudniał im dokonywanie wyborów, sprzyjających ochronie ich danych osobowych. W wyskakującym okienku rejestracji dzieci były nakłaniane do wybrania konta publicznego, co miało niebagatelny wpływ na ich prywatność, na przykład poprzez udostępnianie komentarzy do tworzonych przez nich treści wideo. Wyskakujące okienko publikowania wideo sugerowało dzieciom wybór przycisku „Opublikuj teraz”. Przedstawiono go pogrubionym, ciemniejszym tekstem po prawej stronie, podczas gdy obok znajdował się słabiej widoczny przycisk „Anuluj”. Ci, którzy chcieli uczynić swój post prywatnym, musieli najpierw wybrać „Anuluj”, a następnie poszukać ustawień prywatności, aby przełączyć się na „konto prywatne”.

EROD wyraziła również poważne wątpliwości co do skuteczności środków weryfikacji wieku i ich zgodności z wymogami uwzględniania ochrony danych w fazie projektowania (art. 25 ust.1 RODO), stosowanych przez TikTok w okresie przeprowadzonej kontroli.

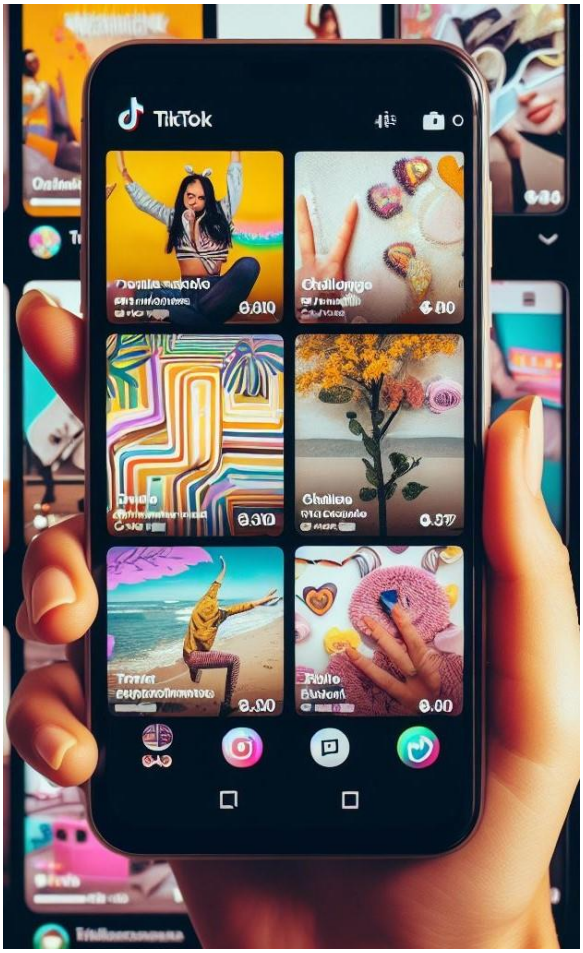
Konsekwencje wyborów opcji były niejasne dla dzieci, korzystających z platformy. EROD potwierdziła, że administratorzy nie powinni utrudniać osobom, których dane dotyczą, dostosowania ustawień prywatności i ograniczenia przetwarzania.
EROD poleciła irlandzkiemu organowi ochrony danych, aby w swojej ostatecznej decyzji nakazał TikTokowi przestrzeganie RODO poprzez wyeliminowanie wskazanych wyżej praktyk projektowania.

EROD wyraziła również poważne wątpliwości co do skuteczności środków weryfikacji wieku i ich zgodności z wymogami uwzględniania ochrony danych w fazie projektowania (art. 25 ust. 1 RODO), stosowanych przez TikTok w okresie przeprowadzonej kontroli. Uwzględniając powagę zagrożeń dla dużej liczby dzieci, których te środki dotyczyły, EROD stwierdziła między innymi, że bramka wiekowa wykorzystywana przez TikToka w celu uniemożliwienia dostępu do platformy użytkownikom poniżej 13 roku życia nie była skuteczna, a więc mechanizm weryfikacji wieku, zastosowany przez TikTok nie działał właściwie.

W oparciu o elementy dostępne w kontekście procedury rozstrzygania sporów EROD stwierdziła, że nie posiada wystarczających informacji, w szczególności w odniesieniu do aktualnego stanu wiedzy, aby ostatecznie ocenić zgodność TikToka z art. 25 ust. 1 RODO w tym okresie. Biorąc jednak pod uwagę poważne wątpliwości, co do skuteczności środków wybranych przez TikToka, EROD zobowiązała irlandzki organ ochrony danych do odzwierciedlenia tego w wydanej przez niego ostatecznej decyzji.

Uwzględniając powagę zagrożeń dla dużej liczby dzieci, których te środki dotyczyły, EROD stwierdziła między innymi, że bramka wiekowa wykorzystywana przez TikToka w celu zakazu dostępu do platformy użytkownikom poniżej 13 roku życia nie była skuteczna.

6 SPRAWY MIĘDZYNARODOWE



Ostateczna decyzja irlandzkiego organu ochrony danych zawiera również ocenę prawną, która nie była przedmiotem sprzeciwów organów, których sprawa dotyczy, taką jak stwierdzenie, że domyślne ustawienia publiczne były sprzeczne z zasadami ochrony danych w fazie projektowania, domyślnej ochrony danych, minimalizacji danych i przejrzystości.

Źródło: **komunikat EROD**

7 EDUKACJA

NAJWAŻNIEJSZE TRENDY NOWYCH TECHNOLOGII W KONTEKŚCIE OCHRONY DANYCH OSOBOWYCH

Zwieńczeniem dwudniowej konferencji pn. „Forum Nowych Technologii" zorganizowanej przez Urząd Ochrony Danych Osobowych we współpracy ze Stowarzyszeniem Prawa Nowych Technologii i Akademią Ekonomiczno-Humanistyczną w Warszawie była debata, moderowana przez Adama Sanockiego, dyrektora Departamentu Komunikacji Społecznej i rzecznika prasowego UODO.

Uczestnicy debaty dyskutowali na temat kierunku, jaki powinna przybrać ochrona danych w kontekście rozwoju nowych technologii. Zastanawiali się m.in. nad tym, jak rekomendacje, dobre praktyki, standardy branżowe mogą pomóc firmom oraz organizacjom w zachowaniu równowagi między wdrażaniem innowacji a ochroną danych osobowych oraz jak zaspokoić w tym wszystkim potrzeby użytkowników.

Regulacje nie nadążają za innowacjami

Debata rozpoczęła się od zagadnienia: co zrobić, żeby regulacje prawne odpowiadały wymogom klientów nowych technologii. Podkreślono jak bardzo regulacje nie nadążają za rozwojem nowych technologii: wciąż nie obowiązuje nas akt o sztucznej inteligencji, nie powstało żadne rozporządzenie o chmurze czy o blockchainie, z których na co dzień masowo korzystają ludzie na całym świecie. Uczestnicy rozmowy zwrócili uwagę, jak ważne jest przestrzeganie zasad zgodności i rozliczalności w zakresie ochrony danych i prywatności. Debatujący podali także przykłady kilku rozwiązań, m.in. piaskownic regulacyjnych, które pozwalają testować nowe technologie w bezpiecznej przestrzeni, sprawdzić jakie niosą za sobą potencjalne zagrożenia i na podstawie zebranych wniosków formułować odpowiednie regulacje, czy rekomendacje. Mówcy wyrazili potrzebę tworzenia kodeksów dobrych praktyk, certyfikacji oraz wytycznych, cennych z punktu widzenia danych osobowych, które powinny powstawać zarówno na poziomie europejskim, jak i krajowym.

Zaakcentowano znaczenie przeprowadzenia oceny wpływu na prywatność oraz wagę udziału specjalistów od prywatności w procesie budowania rozwiązań technologicznych już na samym ich początku, a więc na etapie projektowania. Zaznaczono, że zasada rozliczalności, zasada oceny skutków dla ochrony danych to podstawowe normy, które należy wdrożyć w firmie czy w organizacji, by działać zgodnie z ochroną prywatności. Eksperci wygłosili przekonanie, że organy – w granicach rozsądku – powinny narzucać pewne regulacje innym podmiotom. To zapewni równe warunki działania wszystkim podmiotom na rynku UE, tzw. level-playing field, niezależnie od ich wielkości i pochodzenia, wesprze zdrową konkurencję, innowacje, a w rezultacie zapewni ochronę interesów użytkowników.

7 EDUKACJA

Pułapka przeregulowania

Nowe technologie w założeniu są narzędziem rozwoju: ekonomicznego, gospodarczego, społecznego, dlatego muszą być instrumentem przemyślanym oraz przetestowanym. Debatujący rozważali, na ile należy ująć je w ramy prawne. Podkreślili wagę dyskusji wewnętrznej, która powinna odbyć się w każdej firmie, tworzącej czy stosującej nowe technologie. Dyskusja ta musi opierać się nie tylko na liczeniu zysków i strat po stronie biznesu, ale też po stronie praw, po stronie budowania konkurencyjności opartej o zaufanie konsumentów, którzy z tej technologii korzystają. Powstało już wiele instrumentów, które pozwalają regulować kwestie ochrony danych w kontekście nowych technologii, dlatego prelegenci przestrzegli przed pułapką nadmiernego przeregulowania. Równocześnie zauważyli, że liczne projekty wciąż nie weszły w ogóle lub w pełni w życie: rozporządzenie o sztucznej inteligencji, akt o rynkach cyfrowych, o usługach cyfrowych, o danych, dlatego należy korzystać z tych narzędzi, które już funkcjonują w RODO oraz z wykładni prawa – orzecznictwa i decyzji organów nadzorczych. To one pozwalają obecnie obowiązujące przepisy interpretować w taki sposób, żeby odpowiadały potrzebom rynku i obywateli.

Słyszalny głos inspektora ochrony danych

Podczas debaty mocno wybrzmiał temat pozycji, jaką inspektor ochrony danych zajmuje w procesie analizy rozwiązań wpisanych w tworzenie nowych technologii. Analiza inspektora ochrony danych, pokazująca na ile dane rozwiązania można wdrożyć potrzebna jest szczególnie gdy rozwiązania budowane są przez instytucje komercyjne. To właśnie inspektor powinien przyjąć rolę badacza wpływu technologii na prywatność i na rozwój firm. Dobry administrator musi brać pod uwagę porady swojego inspektora ochrony danych i wyznaczyć mu mocną pozycję w organizacji, co przełoży się na prawidłowe działanie całego systemu ochrony danych osób w jej modelu biznesowym. Inspektorzy ochrony danych osobowych, przy wsparciu których administratorzy podejmują działania w zakresie ochrony danych, działają często w warunkach konfliktu interesów, tym bardziej organy nadzorcze muszą stać
u ich boku, aby pokazywać administratorom, że powinni się liczyć z ich zdaniem.

Etyczny aspekt regulacji

Jak powiedział Zastępca Prezesa Urzędu Ochrony Danych Osobowych Jakub Groszkowski, za Prezesem UODO Janem Nowakiem: „Jesteśmy Urzędem od ochrony człowieka, praw człowieka, poprzez ochronę jego danych”. Etyka to podejście humanistyczne, które musi towarzyszyć także rozwojowi biznesu i rozwojowi każdego społeczeństwa, które zapewnia odpowiedzialność za jednostkę. Potrzebują jej zarówno administratorzy, jak i regulatorzy tworzący przepisy.

7 EDUKACJA


Instytut Prawa
Ochrony Danych
Osobowych


URZĄD OCHRONY DANYCH OSOBOWYC

7 EDUKACJA

Dyskusja na temat etyki zawsze zajmowała dużo miejsca podczas debat dotyczących nowych technologii organizowanych przez Urząd Ochrony Danych Osobowych. Tak było i podczas „Forum Nowych Technologii". Podkreślono, że etyka musi być wbudowana w rozwiązania technologiczne i jest jednym z głównych celów regulacji. Technologie niestety mają tendencję do dyskryminacji, do pewnych tendencyjnych rozwiązań, do wykorzystywania słabszych jednostek, tym bardziej ochronę danych osobowych należy traktować jako instrument zapewniający przestrzeganie praw i wartości związanych z podstawowymi wolnościami obywatelskimi. Trudno sobie wyobrazić, żeby przeciętny konsument rozumiał, na czym polegają nowoczesne technologie, ponieważ nawet osoby zajmujące się nimi na co dzień nie są w pełni w stanie rozpoznać mechanizmów, które stoją za rozwiązaniami technologicznymi. To organy nadzorcze mają zadanie stania na straży przestrzegania tych przepisów poprzez wspieranie legislacji, przestrzeganie prawa.

Instrumentem służącym spełnieniu moralnej funkcji nowych technologii są: regulaminy, statuty wewnętrzne, kodeksy postępowania; one również kształtują pewne podstawy etyczne. Choć przepisy wyznaczają ramy, to, jak będą stosowane, zależy od odpowiedniego kształtowania postaw etycznych oraz edukacji – zarówno w organizacjach, jak i w najmniejszej jednostce rodzinnej.

7 EDUKACJA

Internet rzeczy (ang. Internet of Things - IoT) – obawy dotyczące bezpieczeństwa stosowanych rozwiązań

Adam Sanocki przytoczył dane nt. Internetu rzeczy z serwisu Statista oraz raportu Cyfrowej Polski, które podkreśliły jak bardzo jest on wszechobecny na całym świecie. Według zacytowanych danych w 80% dużych przedsiębiorstw wdrożono już rozwiązania z zakresu Internetu rzeczy, jednak 97% z nich ma obawy dotyczące bezpieczeństwa stosowanych rozwiązań. Debatujący zastanawiali się jak zminimalizować te obawy zarówno u firm, jak i – przede wszystkim – u obywateli. Podstawą jest budowanie rozwiązań w postaci systemu cyberbezpieczeństwa: aktualizacji ustawy o krajowym systemie cyberbezpieczeństwa, nowej dyrektywy NIS 2, która ma poszerzyć standardy i wymogi w tym zakresie.

Prelegenci przyjrzeli się bliżej Internetowi rzeczy w formie urządzeń, które nosimy na ciele. Zawierają one bardzo sensytywne dane informujące np. o aktywności fizycznej. Wędrują one ostatecznie do chmury, gdzie są względnie bezpieczne, często jednak są również przechowywane w samych urządzeniach. W przeciwieństwie do centrów danych, gdzie chronią je najlepsi eksperci, na ochronę danych w urządzeniach największy wpływ mają sami użytkownicy – poprzez ich konfigurację czy wprowadzenie dodatkowych zabezpieczeń, o jakich informują ich producenci urządzeń. To kwestia wymagająca dużej uwagi regulatora.

W opinii Grupy Roboczej art. 29 daną osobową jest już sama informacja o tym, że jest się członkiem gospodarstwa domowego, w którym są urządzenia z zakresu Internetu Rzeczy. To bardzo istotne z perspektywy Urzędu Ochrony Danych Osobowych – organ nadzorczy, dopiero gdy ma przesłanki do tego, by zaliczyć daną informację do danych osobowych, może walczyć o jego prawa. To, co zostanie potraktowane przez sąd jako dana osobowa i ukształtuje linię orzeczniczą, pozwala Urzędowi działać pro obywatelsko.

Kultura korzystania z nowych technologii

Prowadzący spotkanie zadał pytanie, gdzie leży odpowiedzialność za tworzenie kultury korzystania z nowych technologii – na konsumentach, państwie, regulatorach, czy biznesie? Zastanawiał się również nad koniecznością dostrzeżenia przez biznes wartości w społecznej odpowiedzialności odnośnie do ochrony danych, co nie należy do łatwych zadań.

Paneliści wykazali, że użytkownicy powinni dostawać zagwarantowane pod kątem bezpieczeństwa oraz adekwatności danych produkty – przetestowane rozwiązania, tworzone ze świadomością, że coraz więcej informacji stanowi dane osobowe.

Budowanie świadomości u obywateli, inspektorów ochrony danych oraz uczestników rynku to złożony proces, na który składa się wiele ogniw, Prezes Urzędu Ochrony Danych Osobowych robi to chociażby poprzez prowadzone przez siebie programy edukacyjne, powołanie Instytutu Prawa Ochrony Danych czy publikacje decyzji, z którymi każdy obywatel może się zapoznać.

7 EDUKACJA

Najlepszym kierunkiem w stronę tworzenia odpowiedniej kultury korzystania z nowych technologii jest uwzględnienie na samym początku, w fazie produkcji – standardów ochrony danych i wymaganie ich od wszystkich producentów. Muszą oni szczególnie mieć na względzie dane biometryczne jako dane szczególnej kategorii. Jak podkreślili uczestnicy spotkania – jeżeli się je pozyskuje za zgodą, to ta zgoda musi być możliwa do odwołania bez negatywnych konsekwencji (np. bez straszenia podwyższeniem kosztów obsługi), tak aby nie wywierać wpływu na klienta. Wszyscy regulatorzy, tacy jak UOKiK, UODO, UKE muszą bacznie przyglądać się nowym technologiom – bo tylko działając zespołowo i wypracowując pewne rekomendacje można wpływać na rynek, instytucje czy resorty.

To człowiek i jego prawa muszą być w centrum uwagi

Jak podkreślił Jakub Groszkowski, Zastępca Prezesa UODO: „W dobie rozwoju technologii, w tym sztucznej inteligencji, o której tak wiele mówimy, to człowiek i jego prawa mają być w centrum uwagi". Prezes UODO wszystkie wnioski oraz analizy z debaty podda refleksji Urzędu i przekaże na forum Europejskiej Rady Ochrony Danych, by podzielić się nimi z innymi organami nadzorczymi. Prelegenci „Forum Nowych Technologii" akcentowali, że sztuczna inteligencja ma służyć człowiekowi, być homocentryczna, bo tylko w ten sposób może chronić prawa i wolności człowieka.

7 EDUKACJA

W debacie udział wzięli:
mecenas Ewa Kurowska-Tober, Stowarzyszenie Prawa Nowych Technologii;
Monika Krasińska, Dyrektor Departamentu Orzecznictwa i Legislacji, Urząd Ochrony Danych Osobowych;
radca prawny Agnieszka Gajewska-Zabój, Sekretarz Krajowej Rady Radców Prawnych;
Marcin Wysocki, Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji;
mecenas Xawery Konarski, Prezes Stowarzyszenia Prawa Nowych Technologii;
mecenas Maciej Gawroński, GP Partners, członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych;
Jakub Groszkowski, Zastępca Prezesa Urzędu Ochrony Danych Osobowych.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl