URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 05/05/24

www.uodo.gov.pl

SPIS TREŚCI

WPROWADZENIE

Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych S. 3
Karol Witowski, p.o. Rzecznika Prasowego UODO S. 5

1. ROZMOWA Z EKSPERTEM

Cenię sobie jasne procedury, bo one pozwalają na działanie w granicach prawa – Agnieszka Grzelak, Zastępczyni Prezesa Urzędu Ochrony Danych Osobowych S. 7

2. UODO SYGNALIZUJE

Po wyroku TSUE konieczna jest analiza przepisów regulujących działanie biur informacji kredytowej i gospodarczej S. 16
Udostępnianie pacjentom ich surowych danych genetycznych S. 21

3. WYBRANE DECYZJE UODO

Upomnienie dla PZU za przetwarzanie niewłaściwych danych klienta S. 24

4. NARUSZENIA I KONTROLE

Rola kierownictwa administratora w procesie wykonywania przepisów RODO S. 26

5. NOWE TECHNOLOGIE

Dzień Dziecka w erze cyfrowej: Jak w kilku krokach zadbać o prywatność i bezpieczeństwo najmłodszych online? S. 29

6. SPRAWY MIĘDZYNARODOWE

Dni Otwarte Unii Europejskiej 2024 S. 34
Sprawozdanie roczne EROD za 2023 r.: Ochrona praw cyfrowych osób fizycznych S. 37
Grecki organ nadzorczy nałożył na tamtejsze Ministerstwo Migracji i Azylu administracyjną karę pieniężną i nakazał przestrzegania RODO S. 38
Hiszpański organ nadzorczy trzeci rok z rzędu otrzymuje największą liczbę skarg w swojej historii S. 39
EIOD bada Frontex i Europol S. 40
Obchody 20-lecia istnienia instytucji Europejskiego Inspektora Ochrony Danych S. 41
Wyrok TSUE w sprawie C-61/22 | Landeshauptstadt Wiesbaden S. 42
Wyrok ETPC w sprawie Zöldi przeciwko Węgrom (nr 49049/18) S. 44

7. EDUKACJA

Rozmowę trzeba zacząć od słuchania – Joanna Hałoń-Gnutek, lauretka Nagrody im. Michała Serzyckiego S. 45

Szanowni Państwo,

za nami kolejny – pracowity, ale równocześnie satysfakcjonujący – miesiąc, który przyniósł dalsze zmiany.

Mija sześć lat od rozpoczęcia stosowania RODO. Uznaliśmy to za właściwy moment, by przyjrzeć się treści poradników, procedurom, zastanowić się czy przystają one do współczesnych wyzwań – i w konsekwencji – dokonać aktualizacji zaleceń organu nadzorczego. Nasze materiały muszą być zrozumiałe i odpowiadać na kluczowe problemy obywateli, naszych partnerów, organizacji społecznych, przedstawicieli biznesu i innych instytucji. Dlatego też rozpoczęliśmy od otwartych konsultacji dwóch poradników – o przetwarzaniu danych przy zatrudnianiu (poradnik z 2018 roku) oraz o reagowaniu na naruszenia danych osobowych (poradnik z 2019 roku). Proponujemy miesiąc na konsultacje. Uwagi do poradników można zatem zgłaszać do dnia 21 czerwca 2024 r. W przyszłości zamierzamy poddać publicznym konsultacjom szereg innych poradników.

9 maja 2024 r. przedstawiłem posłom z podkomisji stałej do spraw sztucznej inteligencji i przejrzystości algorytmów informację o prowadzonych w Urzędzie pracach nad propozycją wskazówek dotyczących projektowania i dostosowania prawa krajowego do wymogów ochrony danych w związku ze stosowaniem systemów sztucznej inteligencji. Wskazówki te mogą być wsparciem w pracach legislacyjnych.

2 czerwca rusza bus IV edycji „Tour de Konstytucja" pod patronatem UODO. Będę obecny na rozpoczęciu jego trasy w Tomaszowie Mazowieckim. Bieżąca edycja Tour de Konstytucja „Siła Młodych – Most Pokoleń" koncentruje się na edukacji młodzieży w zakresie społeczeństwa obywatelskiego, Konstytucji RP i Karty Praw Podstawowych UE. W tym roku inicjatywa podkreśla znaczenie 20-lecia Polski w Unii Europejskiej i promuje nadchodzące wybory do Parlamentu Europejskiego. Cieszę się, że Urząd Ochrony Danych Osobowych może być częścią tego przedsięwzięcia, by móc przekazywać wiedzę o ochronie prywatności i danych osobowych w bezpośrednich spotkaniach z obywatelami.

Ukazały się wyniki tegorocznej edycji badania nt. świadomości Polaków w obszarze ochrony danych osobowych i prywatności. Badanie zostało przeprowadzone na zlecenie KRD i ChrońPESEL pod patronatem UODO. Wnioski z niego jak zawsze skłaniają do refleksji, co organ nadzorczy może zrobić, by ta świadomość była coraz większa.

Myślę, że poza edukacją, jasnymi komunikatami i wytycznymi na tę świadomość w obszarze ochrony danych osobowych i prywatności ma wpływ poczucie sprawczości. Gdy Urząd chowa głowę w piasek i unika rozwiązywania problemów, z którymi zwracają się do niego obywatele, brakuje właśnie tej siły sprawczej i zaufania do organu. A co za tym idzie, ich zainteresowania ochroną własnych praw w zakresie danych osobowych. Bo po co zwracać się o pomoc do Urzędu, który nie staje po stronie obywatela?

Chcę jako prezes tego organu wziąć odpowiedzialność za jego działania i realnie wywiązywać się z powierzonych mi zadań. Nie unikać problemów, a starać się je rozwiązać. Dlatego też po kolei dokonuję wraz ze współpracownikami w UODO przeglądu spraw, którymi wcześniej nie zajął się rzetelnie organ. Mówiłem o tym w ostatnich wywiadach dla Dziennika Gazety Prawnej oraz TVN24.

Wyzwania są liczne, zagadnień do poruszenia dużo, a szukanie właściwych odpowiedzi często wymaga zaangażowania wielu stron. Na szczęście wciąż możemy, a nawet musimy reagować, gdy w przeszłości naruszone zostały prawa osób do ochrony ich danych. Jak się okazuje, na wcześniejsze niewystarczające działania wciąż mamy wpływ. I możemy je przekierować na odpowiednie tory.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Postanowiliśmy zaprosić na łamy „Biuletynu UODO" pracowników Urzędu. Liczymy, że pomysł Wam się spodoba. Na początek relacja z Dnia Otwartego Komisji Europejskiej, które odbyło się 4 maja 2024 roku w Brukseli. Nasza koleżanka z Departamentu Komunikacji Społecznej uczestniczyła w tym evencie jako wolontariuszka i specjalnie dla Was zrelacjonowała swój udział w wydarzeniu. Mamy dzięki temu okazję by przyjrzeć się z bliska europejskim instytucjom w ich mniej formalnym wydaniu.

Kolejne teksty chętnych do podzielenia się z Nami swoimi refleksjami pracowników UODO będą pojawiać się w różnych miejscach Biuletynu.

Po lekturze relacji z Dni Otwartych KE, wielu z Was z pewnością będzie miało ochotę odwiedzić europejskie instytucje, które zajmują się ochroną danych. Świetną okazją ku temu będą obchody 20-lecia istnienia Europejskiego Inspektora Ochrony Danych. Za niecały miesiąc, 20 czerwca odbędzie się Europejski Szczyt Ochrony Danych – debata na temat roli państw w czasach stale rosnącego gromadzenia informacji o obywatelach oraz roli, jaką ochrona danych powinna odgrywać we współczesnych demokracjach. Dyskusja będzie dotyczyć ochrony danych, jej możliwości, ograniczeń, sukcesów oraz straconych szans, w przyczynianiu się do rozwoju fundamentów demokratycznych społeczeństw. O inicjatywach zaplanowanych w związku z obchodami piszemy na naszych stronach.

W tym numerze Biuletynu przedstawiamy wywiad z zastępczynią prezesa UODO, Agnieszką Grzelak. To wyjątkowa postać bardzo otwarta na głosy innych. Pełna zaangażowania, bezpośrednia w kontaktach, zafascynowana ochroną danych i systemem prawnym UE. Urzeczona bogactwem języka polskiego i jego formami (tak, rozmawialiśmy o feminatywach). Z jednej strony niezwykła ekspertka i naukowczyni, która o dyrektywie policyjnej mogłaby mówić godzinami, z drugiej bezpretensjonalna szefowa, nie przepadająca za zbędnymi formalizmami. Bardzo się cieszę, że możemy razem pracować.

W numerze zamieszczamy też niezwykle ważny tekst dotyczący roli kierownictwa administratora w procesie wykonywania przepisów RODO. Rozporządzenie obowiązuje od sześciu lat i nakłada na administratorów szereg rozmaitych obowiązków mających na celu ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych. Niestety, bezpieczeństwo danych wciąż nie jest traktowane priorytetowo przez organy kierownicze wielu organizacji.

Po wyroku TSUE konieczna jest analiza przepisów regulujących działanie biur informacji kredytowej i gospodarczej. W ocenie Prezesa UODO wyrok TSUE w połączonych sprawach C-26/22 i C-64/22

SCHUFA Holding i in. powinien być podstawą do podjęcia rozważań nad zmianą przepisów ustawy Prawo bankowe oraz ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.

Jak zawsze przedstawiamy wybraną decyzję Prezesa UODO. Tym razem piszemy o upomnieniu dla PZU SA za sposób, w jaki potraktował klienta, który zalegał z opłatami za OC samochodu. Przekazał jego dane do Krajowego Rejestru Długów, bowiem pomylił jego adresy i całą korespondencję o długu kierował na niewłaściwy adres. Spółka naprawiła pomyłkę w swojej bazie i po spłacie zadłużenia usunęła wpis w rejestrze dłużników.

W związku ze zbliżającym się Dniem Dziecka zachęcamy do wprowadzenia nowych zasad bezpieczeństwa lub odświeżenia istniejących, by cyfrowy świat był dla najmłodszych miejscem bezpiecznym i przyjaznym. Zadbanie o bezpieczeństwo dzieci online jest procesem ciągłym, który wymaga współpracy, edukacji i odpowiedzialności zarówno ze strony dzieci, jak i ich opiekunów. Jak w kilku krokach zadbać o prywatność i bezpieczeństwo najmłodszych online? Mamy dla Was liczne wskazówki.

Wszystkim Dzieciom życzymy poczucia bezpieczeństwa, a ich opiekunom, by z łatwością im je zapewniali.

I oczywiście – odchodząc na chwilę od ochrony danych, by nie przesadzić w tak wyjątkowy dzień z nadmiarem dydaktyzmu – Spełnienia marzeń!

Karol Witowski
p.o. Rzecznika Prasowego UODO

1 ROZMOWA Z EKSPERTEM

CENIĘ SOBIE JASNE PROCEDURY, BO ONE POZWALAJĄ NA DZIAŁANIE W GRANICACH PRAWA

Z Agnieszką Grzelak, Zastępczynią Prezesa UODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO

Na konferencji „Przyszłość ochrony danych osobowych w Polsce – w przededniu wyboru nowego Prezesa Urzędu Ochrony Danych Osobowych" w Sejmie powiedziała Pani, że ustawa wdrażająca dyrektywę policyjną jest niestosowalna w kontekście praw osób, które w założeniu ma chronić. Z kolei 20 maja w ramach Koła Naukowego Prawa Ochrony Danych Osobowych i Sztucznej Inteligencji „Salus Populi" działającego na WPiA Uniwersytetu im. Adama Mickiewicza w Poznaniu wygłosiła Pani wykład pt. „Dyrektywa policyjna 2016/680 – (nie)chciana siostra RODO?". Może Pani przybliżyć istotę i implikacje tej dyrektywy dla praktyki prawniczej oraz polityki bezpieczeństwa? Jakie są relacje dyrektywy z RODO?

Na początek dwa słowa wyjaśnienia. W 2016 r., obok znanego powszechnie RODO, instytucje unijne przyjęły dyrektywę 2016/680, która uzupełnia system ochrony danych osobowych w Unii Europejskiej i zobowiązuje państwa członkowskie do wprowadzenia przepisów regulujących zasady przetwarzania danych osobowych przez organy publiczne, do celów – ogólnie ujmując – walki z przestępczością. Z tego względu na dyrektywę potocznie mówi się „policyjna", chociaż naturalnie nie dotyczy wyłącznie Policji. Przypomnę tylko, że w przeciwieństwie do RODO – dyrektywy zasadniczo nie można stosować bezpośrednio i wymaga przyjęcia stosownych przepisów krajowych.

W Polsce w 2018 r. uchwalono ustawę, która miała implementować przepisy tej dyrektywy do prawa krajowego, jednak – w mojej ocenie – jest to wybitny przykład, który mogę wykorzystywać w pracy akademickiej na to, jak nie należy implementować dyrektyw. Niestety – bowiem uważam, że przepisy dyrektywy dawały szansę na to, by spróbować wyważyć dwie wartości, nie rezygnując z żadnej z nich – z jednej strony zapewnienia bezpieczeństwa publicznego i efektywnego działania służb, a z drugiej strony praw osoby, której dane dotyczą. Oczywistym jest, że prawo do ochrony danych osobowych czy prawo do prywatności musi w pewnych okolicznościach ustąpić i być ograniczone po to, by dało się zrealizować inne obowiązki. Trudno przecież wyobrazić sobie, że prawo dostępu do danych czy prawo do zapomnienia albo do bycia poinformowanym o fakcie

przetwarzania danych będą realizowane w pełnym wymiarze w przypadku przetwarzania danych osób, które są podejrzane o popełnienie przestępstwa. Dyrektywa w mojej ocenie – chociaż ogólna – dawała szansę na znalezienie właściwego punktu, w którym obie wartości mogłyby się spotkać. Niestety, polski ustawodawca nie wykorzystał tych możliwości prawidłowo, o czym wielokrotnie pisałam nie tylko jako naukowiec, tworząc i redagując komentarz do ustawy, ale również wspierając – wraz z obecnym Prezesem Urzędu Ochrony Danych Osobowych Mirosławem Wróblewskim – Rzecznika Praw Obywatelskich, prof. Adama Bodnara, który występował z zastrzeżeniami dotyczącymi sposobu implementacji tej dyrektywy. Co więcej, po przyjściu do UODO dowiedziałam się, że w ostatnich latach również poprzedni Prezes Urzędu Ochrony Danych Osobowych starał się interweniować w tej sprawie – znów bezskutecznie.

Jest kilka istotnych wad. Po pierwsze, bardzo niejasny jest zakres zastosowania przepisów ustawy i wprowadzone w niej wyłączenia. Niektóre z nich mogłyby zostać uznane za dopuszczalne, gdyby równolegle istniały inne przepisy regulujące sposób przetwarzania danych. Mam na myśli np. wyłączenia dotyczące danych zawartych w aktach postępowań sądowych czy też przetwarzanych przez określone służby, w tym CBA czy ABW albo informacji niejawnych. Z jednej strony ustawa wdrażająca dyrektywę policyjną nie ma zastosowania, ale z drugiej nie ma dobrych przepisów, które wprowadzałyby wymagany – nie tylko przez dyrektywę, ale właściwie nawet przede wszystkim przez Konstytucję RP czy też Europejską Konwencję o ochronie praw człowieka – standard minimalny.

Niestety, przypadki omawiane publicznie takie jak sprawa Pegasusa czy aktualny problem sędziego, który być może pracował na rzecz innych państw pokazują jak ważne jest uregulowanie tych kwestii w sposób prawidłowy.

Po drugie, przepisy ustawy w zakresie ograniczenia praw osób, których dane dotyczą są bardzo blankietowe i zezwalają na dużą dowolność w uzasadnieniu odmowy realizacji tych praw przez służby. To może z kolei prowadzić do nadużyć, które – w dalszej konsekwencji – nie będą mogły zostać ocenione w kontroli sądowej z racji właśnie zbyt ogólnikowej treści przepisów.

Po trzecie, w dyrektywie wprowadzono bardzo ciekawy i ważny art. 17 – podaję numer, bo często jest przywoływany w rozmowach. Filozofia kryjąca się za tym przepisem jest następująca: skoro osoba, która chce się dowiedzieć, czy jej dane przetwarza np. policja, nie może takiej informacji otrzymać ze względu np. na dobro toczącego się postępowania (co jest całkowicie zrozumiałe), ma prawo poprosić o sprawdzenie pośrednie, które miałoby być dokonane przez niezależny organ. I ten organ miałby uprawnienia kontrolne, a zainteresowanego informowałby jedynie, że sprawdzenie zostało dokonane. W idealnym modelu, taka osoba powinna mieć ogromne zaufanie do organu i uspokoić się po

otrzymaniu takiej informacji, w zaufaniu że procedury działają prawidłowo i gdyby doszło do nadużycia, ten organ podjąłby właściwe kroki zmierzające do naprawy sytuacji. Niestety, przepis ten nie został wdrożony do prawa polskiego, możliwość jego zastosowania bezpośrednio jest teoretyczna (chociaż ja jej całkowicie nie wykluczam), no i pozostaje jeszcze kwestia zaufania do organu ochrony danych osobowych i jego niezależności. Nad tą ostatnią sprawą Mirosław Wróblewski, prezes UODO w następnych tygodniach i latach będzie wraz z zespołem pracował.

Wreszcie można jeszcze dodać, że przepisy RODO w połączeniu z przepisami ustawy wdrażającej dyrektywę policyjną i przepisami ustaw szczególnych stworzyły dość znaczący chaos prawny w odniesieniu do przetwarzania danych osobowych w sądach i w prokuraturze. To jest kolejny, bardzo obszerny wątek, którego już tu rozwijać nie będę, ale mogę zapewnić, że również ten temat będzie jednym z priorytetów naszych działań w najbliższych miesiącach. Proszę jednak pamiętać, że Prezes UODO nie posiada inicjatywy legislacyjnej i to, co może robić przede wszystkim, to apelowanie o zmiany legislacyjne.

Na konferencji dla kandydatów na Prezesa UODO spytała Pani, jakie konkretnie działania powinny być podjęte w celu zwiększenia efektywności rozpatrywania skarg – przy założeniu, że budżet UODO nie wzrośnie. Jak dziś Pani, jako zastępczyni Prezesa UODO, odpowie na tak postawione pytanie?

Budżet UODO faktycznie nie wzrósł, a liczba zadań rośnie. Liczba skarg utrzymuje się na bardzo wysokim poziomie – w tym roku wpłynęło ich już 3066 [dane na 24.05.2024].

W 2023 roku do Departamentu Skarg wpłynęły 6962 skargi. Mimo że w porównaniu do roku poprzedniego to o 33 skargi mniej, to wysoki wskaźnik skarg w latach poprzednich przełożył się na zwiększoną liczbę spraw prowadzonych w Departamencie Skarg UODO. To sprawy, które wpłynęły do UODO w roku poprzedzającym, ale podjęcie czynności niezbędnych do zebrania materiału dowodowego i wydania decyzji administracyjnej nastąpiło w 2023 roku.

W pierwszych tygodniach pracy w Urzędzie wraz z prezesem Wróblewskim i zastępcą prezesa Konradem Komornickim przyglądaliśmy się – i nadal to czynimy – organizacji pracy w Urzędzie. Zbieramy informacje na temat dotychczasowych metod pracy, podziału zadań między departamentami, a w ramach departamentów między poszczególnymi pracownikami i przedstawiamy pewne propozycje, które mają usprawnić i przyspieszyć nie tylko rozpatrywanie skarg, ale też np. zwiększenie liczby prowadzonych kontroli. Chcielibyśmy np. w ramach istniejących możliwości kadrowych utworzyć zespół wstępnej oceny skarg, który zajmowałby się selekcją i odpowiadałby na te pisma, które nie mogą być uznane za skargę czy też na takie, które dotyczą problemów

powtarzalnych. Mam nadzieję, że takie rozwiązanie spowoduje, że pracownicy merytoryczni będą mieli więcej czasu na sprawy trudniejsze.

9 kwietnia br. wzięła Pani udział w spotkaniu z inspektorami ochrony danych oraz przedstawicielami organizacji zrzeszających inspektorów i firm zatrudniających inspektorów, by porozmawiać o niezależności IOD. W konferencji wzięło udział 600 osób. Konferencja poprzedzona było spotkaniami Prezesa z licznymi organizacjami reprezentującymi różne środowiska IOD-ów. Czy widać już rezultaty tego dialogu z IOD-ami?

Spotkanie było bardzo cenną lekcją wymiany poglądów oraz doświadczeń dotyczących konkretnych problemów i zagrożeń dla niezależności IOD. Rozmawialiśmy o obciążeniu inspektorów obowiązkami administratora, zawieraniu umów powierzenia pomiędzy administratorem a IOD, a także udzielaniem IOD pełnomocnictwa do reprezentowania administratora w sprawach z zakresu ochrony danych osobowych.

Uważnie wsłuchujemy się w głosy tego niezwykle ważnego dla nas środowiska. Rezultaty dialogu już są widoczne poprzez jasną komunikację Urzędu, wytyczne, jakie zaczęliśmy zamieszczać w komunikatach. To wsłuchanie się w poglądy IOD-ów będzie też widoczne, chociażby przy opracowywaniu poradników dla podmiotów stosujących RODO. Zależy nam na tym, by poprzez przyjmowane dokumenty wskazać inspektorom, że działania Urzędu są przewidywalne, a sam Urząd jest otwarty na współpracę ze środowiskiem.

Konsultacje dotyczące poradników rozpoczęły się 21 maja. Urząd zaczął od zbierania uwag do dwóch poradników – o zatrudnieniu i naruszeniach. Proszę powiedzieć, jaki jest cel prowadzenia takich konsultacji, jak wyglądają takie konsultacje społeczne, kto może wziąć w nich udział, czy będzie można zapoznać się z uwagami zgłaszających?

W ocenie kierownictwa UODO konsultacje są właśnie takim przykładem otwarcia się na środowisko, o którym wspomniałam wyżej. Czas płynie, praktycy zbierają doświadczenia i teraz będą mieli okazję, by podzielić się z nami tymi doświadczeniami. Poradniki powstają po to, aby ułatwić stosowanie przepisów o ochronie danych osobowych w poszczególnych sektorach. Aby tak się działo muszą one udzielać jasnych wskazówek i odpowiedzi na kluczowe problemy interesariuszy czyli przedstawicieli biznesu, instytucji, organizacji społecznych i społeczeństwa. Od rozpoczęcia stosowania w Polsce RODO minęło już sześć lat, nasze poradniki nie zawsze zawierają aktualne treści. Chcielibyśmy, aby dzięki konsultacjom nasze poradniki odpowiadały współczesnym potrzebom i wyzwaniom.

1 ROZMOWA Z EKSPERTEM

W niektórych przypadkach konieczne będzie również zaktualizowanie stanowiska organu nadzorczego. Plan jest zatem taki, by najpierw zapoznać się z oceną środowiska, zbierając uwagi i publikując je na stronie UODO, a następnie dokonana zostanie analiza i wypracowana treść nowej wersji dokumentu.

UODO podpisał porozumienie z Biurem Rzeczniczki Praw Dziecka i zorganizował niedawno konferencję „Wyzwania dla ochrony danych osobowych dzieci". Ochrona wizerunku dzieci to temat bliski UODO, tymczasem działania podejmowane na rzecz takich osób przez instytucje publiczne i różne organizacje nie zawsze są ze sobą skoordynowane czy znane innym podmiotom. Co w obszarze ochrony dzieci i współpracy instytucjonalnej wymaga największej uwagi?

Organizacja tej konferencji i podpisanie porozumienia to przykład działań, podejmowanych właśnie po to, by znaleźć dobre rozwiązania merytoryczne. Konferencja pokazała, że możemy działać razem, korzystając ze swoich kompetencji, co – miejmy nadzieję – pomoże już niedługo efektywniej odpowiedzieć na wyzwania. Chcemy czerpać z doświadczeń obu organów, by nasz przekaz był mocniejszy.

Oczywiście samo podpisanie porozumienia to nie wszystko, za tym muszą iść kolejne działania, chociażby edukacyjne, czego przykładem jest wspólny webinar „RODO w szkolnej ławce. Wykorzystanie wizerunku dziecka – prawo i praktyka", dotyczący ochrony danych dzieci w placówkach edukacyjnych, który odbył się w połowie maja. To dopiero początek.

To, co silnie wybrzmiewa podczas tych konferencji, na co musimy zwracać szczególną uwagę, to uznanie podmiotowości dzieci, poszanowania autonomii młodych ludzi w wymiarze również informacyjnym. Bazując na tym możemy dopiero myśleć o szukaniu rozwiązań legislacyjnych i technicznych. Te z kolei nie mogą być wymyślone wyłącznie przez prawników i informatyków, powinny zostać wypracowane wspólnie przez wszystkie środowiska i z dużym udziałem organizacji pozarządowych oraz ekspertów.

Niezwykła aktywność młodych w Internecie, od coraz wcześniejszego wieku, którzy korzystają z jego dobrodziejstw, ale również wpadają w zastawione przez sieć pułapki, rodzi liczne zagrożenia. Tu pojawia się chociażby temat wyrażania przez osoby młode zgody na przetwarzanie ich danych osobowych, również poprzez niejasne, niespełniające wymogów klauzule informacyjne napisane takim językiem, że nawet osoba dorosła nie poradziłaby sobie z ich zrozumieniem.

1 ROZMOWA Z EKSPERTEM

Do tego dodać należy aktywność osób dorosłych w sieci – nauczycieli czy rodziców, którzy niejednokrotnie bezrefleksyjnie publikują dane i wizerunek swoich dzieci w mediach społecznościowych, również w celach reklamowych i zarobkowych.

Uważam, że podpisanie porozumienia o współpracy między Prezesem UODO a Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych i badawczych dotyczących danych osobowych dzieci i młodzieży jest bardzo ważnym krokiem w stronę większej aktywności obu organów. Trzeba jednak dodać, że również w innych obszarach taką współpracę instytucjonalną podejmujemy – Prezes UODO spotykał się w ostatnim czasie również z osobami kierującymi innymi instytucjami publicznymi, w tym z Ministrem Cyfryzacji, Prezesem Urzędu Ochrony Konkurencji i Konsumentów, Prezesem Urzędu Komunikacji Elektronicznej i in. – te wszystkie spotkania mają służyć wzmocnieniu wspólnych działań, wypracowaniu wspólnych stanowisk również w kontekście nowych, nadchodzących wyzwań związanych ze stosowanie nowych aktów, w tym aktu o usługach cyfrowych (DSA) czy aktu o zarządzaniu danymi (DGA).

Jest Pani autorką licznych publikacji z zakresu systemu prawnego Unii Europejskiej, wykłada Pani prawo Unii Europejskiej w Akademii Leona Koźmińskiego, a naukowo działa Pani również na styku ochrony danych osobowych i bezpieczeństwa. Jak wyglądają wzajemne relacje systemów prawnych UE i Polski, jak zadbać o to, by sprawnie działały?

Cały obszar systemu prawnego UE, jego relacji do prawa krajowego jest dla mnie fascynujący. Zaczęłam się rozwijać zawodowo i naukowo wtedy, gdy Polska stawała się członkiem Unii Europejskiej. W latach 2000-2004 pracowałam w Urzędzie Komitetu Integracji Europejskiej i miałam okazję uczestniczyć w procesie harmonizacji prawa, a 20. rocznica akcesji Polski do UE, która przypada w tym roku jest dla mnie momentem refleksji. Od samego początku swojej kariery w szczególności interesowały mnie zagadnienia współpracy policyjnej i sądowej w sprawach karnych – czyli takiego obszaru współdziałania państw, który najwolniej poddawał się systemowi uwspólnotowienia, jako silnie powiązany z państwowością i kompetencjami krajowymi. Dołączając do tego zainteresowanie prawami człowieka – stąd już była krótka droga do ochrony danych osobowych i prawa do prywatności właśnie w relacji do bezpieczeństwa obywateli, o czym powiedziałam wcześniej.

Unia Europejska – jakkolwiek górnolotnie to zabrzmi – była marzeniem moich rodziców, uosobieniem wolności, której oni w czasach PRL nie doświadczali. Ja patrzę na tę organizację międzynarodową już bardziej realistycznie, widzę jej różne wady, ale nadal dostrzegam więcej zalet, do których zaliczam przede wszystkim jej konstrukcję instytucjonalną, która pozwala na zrównoważenie uprawnień

poszczególnych instytucji, reprezentujących interesy państw członkowskich (Rada), obywateli (Parlament Europejski) czy samej UE (Komisja Europejska).

Dla naukowca system prawny UE jest nowatorski – UE jest organizacją o charakterze ponadnarodowym, a zatem prawo stanowione w jej ramach, w którego tworzeniu wszystkie państwa, w tym Polska biorą udział na równych zasadach, bez wątpienia silnie ingeruje w porządki prawne państw członkowskich, chociażby poprzez przyjmowanie rozporządzeń, które stosowane są bezpośrednio, tak jak RODO czy w najbliższym czasie DSA czy DGA. Nie ukrywam też, że pozytywnie oceniam powrót na drogę praworządności i stopniową naprawę tych naruszeń prawa UE, które miały miejsce w ostatnich latach w Polsce, a które były stwierdzane orzeczeniami Trybunału Sprawiedliwości, co też było przedmiotem naszej – mojej i Pana prezesa Wróblewskiego – naukowej aktywności w ostatnich latach.

Z prawem do prywatności i prawem do ochrony danych osobowych wiąże się wiele ważnych orzeczeń TSUE. Rola Trybunału wymagałaby pewnie osobnego wywodu, ale przypomnieć należy, że to właśnie Trybunał dokonuje wykładni przepisów traktatów, których Polska stała się stroną na mocy decyzji Narodu. W najbliższym czasie będziemy szerzej o tym rozmawiać podczas konferencji poświęconej m.in. 20. rocznicy członkostwa Polski w UE, na którą wszystkich już teraz zapraszam.

Nie ukrywa Pani swojej niechęci do biurokracji i zbędnych formalizmów. Jednocześnie od dawna piastuje Pani wysokie stanowiska. Zdawałoby się, że to wymaga przestrzegania wielu procedur biurokratycznych. Chciałbym Pani pogratulować tej bezpośredniości, jestem przekonany, że przekłada się to bardzo pozytywnie nie tylko na komunikację wewnętrzną w Urzędzie, ale również na komunikację Urzędu z obywatelami. Czy to jest właśnie Pani styl zarządzania?

Cenię sobie jasne procedury, bo one pozwalają na działanie w granicach prawa. Nie ma potrzeby jednak ich nadmiernie rozbudowywać, a szczególnie ważne, by w relacjach pracowniczych kontakty ze mną były bezpośrednie. Często skracają one drogę do ustalenia wspólnych działań i przyspieszenia pracy. Dlatego też, gdy zaczęłam pracę w Urzędzie chciałam jak najszybciej poznać jego załogę osobiście. W mailu powitalnym zaoferowałam pracownikom lojalność, życzliwość, zaangażowanie i otwartość i muszę przyznać, że dostaję to samo w zamian. Chciałam, aby relacje między mną a resztą zespołów odbywały się bez zbędnej otoczki „urzędniczej" i formalizmów.

Staram się odpowiadać możliwie szybko na prośby o wszelkie spotkania bezpośrednie z pracownikami, sama również je inicjuję. Jeżeli jest problem, który można rozwiązać poprzez jedno

spotkanie, zamiast zakładania spraw w elektronicznym systemie zarządzania dokumentacją i przerzucania się mailami, w których główną treścią jest wstęp pełen odwołań do tytułów i stanowisk, jakie ktoś pełni, to zdecydowanie wybieram ten pierwszy styl zarządzania.

Poza tym uważam, że to pracownicy znają ten urząd i problemy od podszewki, ja mogę tylko nieco pomóc. Chcę się skupić na rozwiązaniu problemów, jakie wystąpiły, a nie na bezmyślnym staniu przy swojej racji z uwagi na pełnione stanowisko. Jesteśmy tu nie po to, żeby pokazać jacy jesteśmy ważni, a po to, by dane obywateli były lepiej chronione. Same tytuły o niczym nie świadczą.

Myślę, że rzeczywiście ten jasny sposób komunikacji przekłada się też na kontakt z obywatelami i ten aspekt bezpośredniości jest dla mnie bardzo ważny. Wystarczy spojrzeć chociażby na komunikaty na naszej stronie. Kiedy mogą, przestają być czysto informacyjne. Nie piszemy już wyłącznie o tym, że jakiś podmiot dostał karę, ale też wyraźnie i wprost tłumaczymy, jak w danej sytuacji należy postąpić właściwie, żeby inny podmiot mógł uniknąć podobnie przykrych konsekwencji. To nie powinno być w strefie domysłów.

Wiem, że podobne oczekiwania mają nasi klienci – obywatele, chociażby ci, którzy dzwonią po rady na numer Infolinii UODO. Chcą jasnych wytycznych, co mogą, a czego nie powinni w danej sytuacji robić. Pracujemy również nad uproszczeniem języka wystąpień i pism kierowanych do osób zwracających się ze swoimi sprawami do Urzędu.

Używa Pani feminatywów. Dotychczas pomimo obecności wielu kobiet w UODO, na wszystkich stanowiskach, feminatywy nie były u nas stosowane. Pani jako pierwsza przedstawia się jako zastępczyni. Dla wielu to miła odmiana. Czy będą obowiązkowe w Urzędzie?

Dyskusja o formach żeńskich w języku polskim trwa od ponad stu lat. Aktualnie zauważalna jest tendencja do regularnego tworzenia form żeńskich, ale jednocześnie widać, że zaznaczanie żeńskości może następować za pomocą rzeczownika pani, poprzedzającego formę męską. Muszę przyznać, że moje stanowisko w tej sprawie uległo znaczącej ewolucji, co również zawdzięczam prezesowi Wróblewskiemu, który mnie do zasadności feminatywów przekonywał jeszcze w czasach naszej wspólnej pracy w BRPO.

Obecnie można powiedzieć, że jestem wręcz zafascynowana bogactwem języka polskiego i formami, w jakich feminatywy mogą występować. Uważam jednak również, że język polski jest językiem bogatym, żywym, ale jednocześnie zależnym od użytkownika czy użytkowniczki i to im należy

pozostawić decyzję co do tego, jakiej formy będą używać. Wydaje mi się, że kobiety powinny nauczyć się deklarować, jak chcą, by się do nich zwracać, choć jednocześnie nie powinny mieć pretensji, jeśli rozmówca zwróci się do nich w innej formie. Tak to też będzie działać w urzędzie – z pewnością nie narzucimy niczego bez woli użytkowniczek.

Ostatecznie o tym, jak oceniana będzie moja praca i co sobą reprezentuję w żadnej mierze nie świadczy to, czy ktoś nazwie mnie Wiceprezeską, Panią Prezes, Profesorką czy Panią Profesor czy po prostu Agnieszką – mam nadzieję, że to jednak działania i osiągnięcia będą świadczyły o tym, co robię, a nie forma, w jakiej się przedstawiam.

Dziękuję za rozmowę.

Na fotografii Agnieszka Grzelak, Zastępczyni Prezesa Urzędu Ochrony Danych Osobowych

PO WYROKU TSUE KONIECZNA JEST ANALIZA PRZEPISÓW REGULUJĄCYCH DZIAŁANIE BIUR INFORMACJI KREDYTOWEJ I GOSPODARCZEJ

W ocenie Prezesa UODO wyrok TSUE w połączonych sprawach C-26/22 i C-64/22 SCHUFA Holding i in. powinien być podstawą do podjęcia rozważań nad zmianą przepisów ustawy Prawo bankowe oraz ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.

Trybunał Sprawiedliwości Unii Europejskiej w powołanym wyroku, w którym odpowiadał na pytania niemieckiego sądu, odniósł się do funkcjonowania baz danych tworzonych przez prywatne biura informacji kredytowej, a zawierających dane z publicznych rejestrów dłużników i upadłości.

Opis przypadku

Sprawa dotyczy SCHUFA Holding AG – prywatnego biura utworzonego według prawa niemieckiego.

• Rejestrowało i przechowywało ono we własnych bazach danych informacje pochodzące z publicznych rejestrów, w tym te dotyczące zwolnienia z pozostałej części długu.

• Udostępniało je w razie potrzeby swoim kontrahentom – głównie bankom na potrzeby dokonywania przez nie oceny zdolności kredytowej ich klientów.

• Zebrane informacje były usuwane z upływem trzech lat od ich zarejestrowania, zgodnie z kodeksem postępowania opracowanym w Niemczech przez zrzeszenie biur informacji kredytowej.

Uzyskawszy w ramach postępowań upadłościowych na mocy postanowień sądowych przedterminowe zwolnienie z pozostałej części długu, UF i AB zwrócili się do SCHUFA o usunięcie wpisów dotyczących tych postanowień. SCHUFA odmówiło jednak uwzględnienia ich wniosków, wyjaśniając, że przewidziany w przepisach niemieckich sześciomiesięczny termin na usunięcie tych danych z rejestru publicznego nie ma w tym przypadku zastosowania.

UF i AB wnieśli przeciwko SCHUFA skargi do właściwego organu nadzorczego, które ten oddalił, gdyż w jego ocenie przetwarzanie danych przez SCHUFA było zgodne z prawem.

2 UODO SYGNALIZUJE

Niemiecki sąd administracyjny, do którego UF i AB wnieśli skargi na decyzje organu nadzorczego, zwrócił się do TSUE z pytaniami związanymi z wykładnią kilku przepisów RODO. Dotyczyły one m.in. podstaw prawnych przetwarzania danych osobowych przez prywatne biuro informacji kredytowej oraz prawa do usunięcia danych.

Stanowisko TSUE

W wyroku TSUE podniósł, że

• stosownie do brzmienia art. 5 ust. 1 lit. a) RODO dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

• Jednocześnie uznał, że przesłanką legalizującą przetwarzanie danych osobowych przez prywatne biura informacji kredytowej jest art. 6 ust. 1 lit. f) RODO. Zgodnie z tym przepisem przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadku, gdy – i w takim zakresie, w jakim – jest ono niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez osobę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zatem przetwarzając dane na podstawie tego przepisu, należy dokonać wyważenia praw i interesów poszczególnych stron.

W ocenie Trybunału przetwarzanie danych osobowych przez prywatne biura informacji kredytowej służy interesom gospodarczym prywatnego biura, a także realizacji prawnie uzasadnionych interesów jego kontrahentów, którzy mają obowiązek przeprowadzenia oceny zdolności kredytowej osób, z którymi zamierzają zawrzeć umowy związane z kredytem. A zatem służy interesom sektora kredytowego na płaszczyźnie społeczno-gospodarczej.

Jednak żeby przetwarzanie danych dla realizacji prawnie uzasadnionego interesu administratora lub osoby trzeciej można było uznać za zgodne z prawem, dane te muszą być absolutnie niezbędne, a oceny w tym zakresie należy dokonywać łącznie z zasadą minimalizacji ustanowioną w art. 5 ust. 1 lit. c) RODO. Zgodnie z nią dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Z kolei co do warunku, że interesy lub podstawowe prawa i wolności osoby objętej ochroną danych nie mają pierwszeństwa przed prawnie uzasadnionym interesem administratora lub osoby trzeciej,

Trybunał wskazał, że dokonując w każdym konkretnym przypadku szczegółowego wyważenia tych praw i interesów, pod uwagę należy brać

• przede wszystkim racjonalne oczekiwania osoby, której dane dotyczą, że jej dane mogą być przetwarzane przez danego administratora

• oraz zakres tej operacji przetwarzania i jej wpływ na tę osobę. Jednocześnie udzielił wskazówek, na jakich etapach i jakie aspekty należy uwzględniać.

TSUE zaznaczył, że przetwarzanie przez prywatne biuro informacji kredytowej danych dotyczących przyznanego zwolnienia z pozostałej części długu, takie jak

• przechowywanie,

• analiza

• i ujawnianie tych danych osobie trzeciej,

stanowi poważną ingerencję w prawa podstawowe osoby, której dane dotyczą. Takie dane są bowiem wykorzystywane jako czynnik wpływający negatywnie na ocenę jej zdolności kredytowej, a zatem stanowią szczególnie chronione informacje na temat jej życia prywatnego, których przetwarzanie może poważnie zaszkodzić jej interesom. Co więcej, im dłuższy jest okres przechowywania takich danych, tym znaczniejszy ma to wpływ na interesy i życie prywatne osoby, której dane dotyczą, i tym bardziej rygorystyczne są wymogi w zakresie zgodności przechowywania tych informacji z prawem.

Trybunał zauważył, że za gromadzenie i przechowywanie danych w krajowych bazach danych odpowiadają państwa członkowskie, dlatego to one powinny również ustalić okres przechowywania tych danych.

W niniejszym przypadku prawodawca krajowy uznał, że po upływie sześciu miesięcy prawa i interesy osoby, której dane dotyczą, mają pierwszeństwo przed prawem i interesem ogółu w zakresie dysponowania tą informacją. Co więcej, zwolnienie z pozostałej części długu ma umożliwić osobie, której takie zwolnienie przyznano, ponowny udział w życiu gospodarczym i ma ono zwykle dla tej osoby znaczenie egzystencjalne. Osiągnięcie tego celu byłoby zaś zagrożone, gdyby odnoszące się do tego zwolnienia informacje mogły być przechowywane i wykorzystywane po ich usunięciu z publicznego rejestru upadłości. W związku z tym Trybunał stwierdził, że interes sektora kredytowego w dysponowaniu informacjami dotyczącymi zwolnienia z pozostałej części długu nie może uzasadniać przechowywania danych po upływie okresu przechowywania w publicznym rejestrze upadłości.

Trybunał dodał, że przechowywanie danych przez sześć miesięcy również stanowi ingerencję w prawa podstawowe osoby, której dane dotyczą. W tym względzie do sądu odsyłającego należy ocena, czy równoległe przechowywanie tych danych przez prywatne biura można uznać za ograniczone do tego, co absolutnie niezbędne.

Wreszcie co do istnienia kodeksu postępowania przewidującego usuwanie danych z upływem trzech lat, Trybunał zauważył, że o ile taki kodeks ma pomagać we właściwym stosowaniu RODO, o tyle przesłanki zgodności z prawem przetwarzania danych osobowych określone w takim kodeksie nie mogą różnić się od przesłanek przewidzianych w RODO. W związku z tym nie można uwzględnić kodeksu postępowania, który prowadzi do oceny innej niż ta wynikająca z zastosowania RODO.

Analizując zaś obowiązki administratora w zakresie usuwania danych osobowych, Trybunał zauważył, po pierwsze, że administrator musi usunąć dane, które poddano niezgodnemu z prawem przetwarzaniu, takiemu jak rozpatrywane w niniejszym przypadku przetwarzanie danych przez biuro po upływie sześciomiesięcznego okresu przechowywania w rejestrze publicznym. Po drugie, nawet gdyby sąd odsyłający doszedł do wniosku, że przetwarzanie danych przez sześć miesięcy jest zgodne z prawem, osobie, której dane dotyczą, przysługuje prawo do wniesienia sprzeciwu wobec takiego przetwarzania oraz do uzyskania usunięcia dotyczących jej danych, jeżeli biuro nie udowodni występowania nadrzędnych prawnie uzasadnionych podstaw, które mają pierwszeństwo przed interesami oraz prawami i wolnościami tej osoby.

Analiza UODO

Analiza tego wyroku TSUE dokonana przez polski organ nadzorczy z uwzględnieniem krajowego systemu prawnego zaowocowała powstaniem opinii dla rządu. **UODO zwraca w niej uwagę, że w przepisach prawa polskiego nie ma zakazu pozyskiwania z publicznych rejestrów danych osobowych dłużnika na potrzeby oceny jego zdolności kredytowej.**

Zgodnie z art. 105 ust. 4 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe banki mogą, wspólnie z bankowymi izbami gospodarczymi, utworzyć instytucje upoważnione do gromadzenia, przetwarzania i udostępniania określonych informacji podmiotom wymienionym w tym przepisie. Na tej podstawie działają takie instytucje, jak Biuro Informacji Kredytowej oraz Bankowy Rejestr prowadzony przez Związek Banków Polskich. Z kolei art. 28 ust. 1 ustawy z dnia 9 kwietnia 2010 r. o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych określa źródła pozyskiwania danych przez biuro informacji gospodarczej.

Powołane przepisy nie regulują jednak sytuacji, której dotyczy omawiany wyrok TSUE. Czyli przypadku, gdy informacja o dłużniku zostaje wykreślona z rejestru publicznego, z którego została pozyskana, ale nadal przetwarzana jest w biurze informacji kredytowej (gospodarczej).

Tymczasem TSUE uznał, że „w tych okolicznościach interes sektora kredytowego w dysponowaniu informacjami dotyczącymi zwolnienia z pozostałej części długu nie może uzasadniać przetwarzania danych osobowych takiego jak rozpatrywane w postępowaniach głównych po upływie okresu przechowywania danych w publicznym rejestrze upadłości, w związku z czym przechowywanie tych danych przez biuro informacji kredytowej nie może być oparte na art. 6 ust. 1 akapit pierwszy lit. f) rozporządzenia 2016/689 w okresie następującym po usunięciu wspomnianych danych z publicznego rejestru upadłości" (pkt 99 orzeczenia).

Zatem w przepisach Prawa bankowego oraz w ustawie o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych należałoby wprowadzić uregulowania odnoszące się do tego, że dane nie powinny być przetwarzane w biurze informacji kredytowej (gospodarczej) dłużej niż jest to dopuszczalne w rejestrze, z którego zostały pozyskane.

Prezes UODO zwrócił też uwagę na to, że przepisy ustawy Prawo bankowe w ogóle pomijają kwestię dopuszczalnych źródeł pozyskania danych osobowych dotyczących stanu majątkowego osoby wnioskującej o zawarcie umowy z bankiem lub posiadającej już zobowiązanie finansowe.

W opinii organu nadzorczego sfera dotycząca przetwarzania danych przez podmioty gromadzące informacje odnoszące się do zobowiązań kredytowych i pożyczkowych powinna zostać szczegółowo uregulowana przepisami ustawy, gdyż godzi to w prawa i wolności dłużnika związane z zaspokajaniem przez niego podstawowych potrzeb w kontekście badania zdolności do zaciągnięcia zobowiązania.

Podsumowując – w ocenie Prezesa UODO – analizowany wyrok TSUE powinien być podstawą do podjęcia rozważań nad zmianą stosownych przepisów ustawy Prawo bankowe oraz w ustawy o udostępnianiu informacji gospodarczych i wymianie danych gospodarczych.

UDOSTĘPNIANIE PACJENTOM ICH SUROWYCH DANYCH GENETYCZNYCH

Administratorzy – stosownie do art. 15 ust. 3 RODO – mają obowiązek dostarczenia osobie, której dane dotyczą, kopii przetwarzanych danych osobowych. Spełnienie tego obowiązku przez podmioty z sektora opieki zdrowotnej może polegać m.in. na wydaniu pacjentowi kopii informacji, niezależnie od tego, czy stanowią one część jego dokumentacji medycznej.

Pewien podmiot leczniczy, który wykonał badania genetyczne, nie chciał udostępnić pacjentowi jego surowych danych genetycznych. Tymczasem pacjent ten chciał przekazać je do reanalizy w innym ośrodku. Spotkawszy się z odmową, zwrócił się o pomoc do Rzecznika Praw Pacjenta.

Ten zaś, powołując się na obowiązujące przepisy i zawarte porozumienie o współpracy, poprosił Urząd Ochrony Danych Osobowych o opinię, czy dane takie stanowią część dokumentacji medycznej i czy muszą podlegać udostępnieniu.

W odpowiedzi organ nadzorczy przekazał wskazówki co do wzajemnej relacji uprawnień pacjenta (podmiotu danych) określonych w art. 15 RODO i jego prawa do pozyskania kopii dokumentacji medycznej, o którym mowa w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

Zaznaczył, że art. 4 pkt 13 ogólnego rozporządzenia o ochronie danych (RODO) definiuje „dane genetyczne" jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

Zakres tego pojęcia obejmuje dane konkretnych osób o różnym charakterze i jest szeroki.

W motywie 34 RODO doprecyzowano, że dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu

dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji.

Dodatkowo z motywu 35 powołanego rozporządzenia wynika, że do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą.

Do danych takich należą

• informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej,

• numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;

• informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;

• oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Należy także pamiętać, że dane genetyczne należą do danych szczególnych kategorii. Zgodnie z art. 9 ust. 1 RODO ich przetwarzanie jest co do zasady zabronione, chyba że podmiot wykonujący operacje na nich spełnia jedną z przesłanek przewidzianych w ust. 2 tego przepisu. Wówczas to ona będzie podstawą uprawniającą do przetwarzania takich danych. Jednocześnie stosownie do art. 9 ust. 4 RODO państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania m.in. danych genetycznych.

Biorąc to pod uwagę UODO uznał, że surowe dane genetyczne pacjentów będą podlegały ochronie wynikającej z przepisów RODO, o ile będą pochodzić z analizy próbki biologicznej, na podstawie której będzie można uznać, że dotyczy konkretnej osoby.

Oceniając obowiązek udostępnienia pacjentom surowych danych genetycznych należy wskazać, że uregulowane w art. 15 RODO prawo dostępu osoby do dotyczących jej danych nie jest ograniczone tym, czy dane te zostały włączone do dokumentacji medycznej, o której mowa w art. 25 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Określone w art. 26 tej ustawy zasady udostępniania

dokumentacji medycznej nie wyłączają także uprawnienia osób, których dane dotyczą, do uzyskania od administratora na podstawie art. 15 ust. 1 RODO potwierdzenia, czy przetwarza on dane osobowe tej osoby, a jeżeli ma to miejsce, uprawnienia do uzyskania dostępu do nich oraz do informacji określonych w tym przepisie. W wytycznych Europejskiej Rady Ochrony Danych 01/2022 w sprawie praw osób, których dane dotyczą – Prawo dostępu podkreślono, że zakres prawa dostępu określa zakres pojęcia danych osobowych w rozumieniu art. 4 pkt 1 RODO.

Stosownie do art. 15 ust. 3 RODO administrator ma też obowiązek dostarczenia osobie, której dane dotyczą, kopii danych osobowych podlegających przetwarzaniu.

fot. Pexels.com

UPOMNIENIE DLA PZU ZA PRZETWARZANIE NIEWŁAŚCIWYCH DANYCH KLIENTA

Prezes UODO upomniał PZU SA za sposób, w jaki potraktował klienta, który zalegał z opłatami za OC samochodu. Przekazał jego dane do Krajowego Rejestru Długów, bowiem pomylił jego adresy i całą korespondencję o długu kierował na niewłaściwy adres.

Sprawa kończy się upomnieniem, bo spółka naprawiła pomyłkę w swojej bazie i po spłacie zadłużenia usunęła wpis w rejestrze dłużników.

Problem wziął się stąd, że PZU dysponował dwoma adresami klienta. Starym, archiwalnym, z polisy zawartej przed 2006 roku i nowym, z polisy OC na samochód z 2020 roku. Tej ostatniej polisy klient nie zamierzał przedłużać. Niestety, wypowiedzenie umowy złożył już po wygaśnięciu polisy. A zgodnie z ustawą o ubezpieczeniach obowiązkowych (art. 28 ust. 1) PZU musiał tę polisę wznowić automatycznie. W efekcie powstało zadłużenie w wysokości ok. 400 zł.

PZU wpisał więc swego klienta (pod niewłaściwym adresem) do Krajowego Rejestru Długów Biura Informacji Gospodarczej SA (zwanego dalej: BIG). W postępowaniu przed UODO Zakład wyjaśnił, że sam klient, kiedy dowiedział się o sprawie zadłużenia, odpisał też z tego adresu.

Prezes UODO wydając decyzję o upomnieniu wskazał, że

• PZU samowolnie wykorzystał adres archiwalny do przedłużenia umowy ubezpieczenia, podczas gdy w umowie pierwotnej wskazany został przez Skarżącego inny adres.

• To, że Skarżący podał potem ten stary adres w korespondencji z PZU, nie ma znaczenia. Skarżący zrobił to po to, by PZU go prawidłowo zidentyfikował.

• Każdy ma prawo do wskazania swojego adresu do korespondencji, gdyż ponosi odpowiedzialność za późniejsze odbieranie korespondencji. Na administratorze ciąży natomiast obowiązek przetwarzania prawidłowych i aktualnych danych adresowych.

• W przedmiotowej sprawie doszło do naruszenia przez PZU przepisów o ochronie danych osobowych polegających na przetwarzaniu nieprawidłowych danych osobowych Skarżącego w zakresie jego nieaktualnego adresu.

3 WYBRANE DECYZJE UODO

• Konsekwencją przetwarzania, w związku z kolejną polisą, nieaktualnych danych osobowych Skarżącego w zakresie adresu, było nieprawidłowe udostępnienie danych osobowych Skarżącego do BIG. Stosownie do art. 14 ust. 1 pkt 3 ustawy o BIG dane można przekazać, gdy upłynął co najmniej miesiąc od wysłania wezwania do zapłaty na adres do doręczeń wskazany przez dłużnika będącego konsumentem. Tymczasem PZU wysyłał korespondencję na nieaktualny adres.

Sygnatura sprawy: DS.523.2993.2021

fot. pixabay

ROLA KIEROWNICTWA ADMINISTRATORA W PROCESIE WYKONYWANIA PRZEPISÓW RODO

RODO, które obowiązuje już sześć lat, nakłada na administratorów szereg rozmaitych obowiązków mających na celu ochronę osób fizycznych w związku z przetwarzaniem ich danych osobowych. Niestety, bezpieczeństwo danych wciąż nie jest traktowane priorytetowo przez organy kierownicze wielu organizacji.

Administrator jako organizacja

„Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Cele i sposoby przetwarzania mogą też zostać określone bezpośrednio w prawie europejskim lub krajowym – wówczas administratora lub kryteria jego wyznaczania również można ustanowić poprzez normy prawne.

RODO zasadniczo nie stwarza ograniczeń dotyczących rodzaju podmiotu, który może pełnić funkcję administratora. Zazwyczaj jednak, choć nie zawsze, **za administratora uznajemy organizację jako taką, a nie związaną z nią osobę fizyczną (np. pracownika, dyrektora lub prezesa zarządu spółki).**

Znaczenie kierownictwa administratora

Istotą roli administratora jest rzeczywista decyzyjność dotycząca kluczowych aspektów przetwarzania, dlatego szczególne znaczenie w tym procesie odgrywają organy kierownicze. Mimo to wciąż zdarza się, że ścisłe kierownictwo administratora przejawia daleko idącą nieświadomość w zakresie obowiązujących w tym obszarze regulacji, a także niebezpieczeństw, jakie w przypadku ich nieprzestrzegania mogą grozić osobom, których dane dotyczą.

Jest to duży problem, ponieważ aby instrumenty ochrony danych osobowych były rzeczywiście skuteczne, wymagają one systemowego i wielowymiarowego podejścia. Często może je zagwarantować wyłącznie inicjatywa posiadająca poparcie najwyższego kierownictwa organizacji.

Konsekwencje, których można uniknąć

W 2023 r. do Prezesa UODO wpłynęło ponad 14 tysięcy zgłoszeń naruszeń ochrony danych osobowych, czyli naruszeń bezpieczeństwa rodzących ryzyko wystąpienia negatywnych skutków dla

osób fizycznych[1] . Wśród najczęstszych przyczyn takich zdarzeń można wymienić m.in.

• błędy pracowników,
• nieznajomość lub brak stosownych procedur i polityk ochrony danych
• oraz nieodpowiednie zabezpieczenia techniczne.

Administratorzy nie byli w stanie zapobiec wszystkim odnotowanym incydentom, jednakże w przypadku większości z nich dało się uniknąć albo przynajmniej znacznie ograniczyć konsekwencje dla osób, których dane przetwarzano. **W tym kontekście fundamentalne znaczenie mają przemyślane i proporcjonalne inwestycje w ochronę danych osobowych oraz skuteczne mechanizmy zaradcze.** Tymczasem niechęć kierownictwa wielu organizacji do akceptacji dodatkowych wydatków sprzyja urzeczywistnianiu się ryzyka w sytuacjach, w których można się przed nim uchronić.

Pozorna oszczędność

Pamiętajmy zatem, że przedkładanie korzyści biznesowych ponad bezpieczeństwo również może kosztować.

Najlepszym tego dowodem jest wyposażenie organów nadzorczych, takich jak Prezes UODO, w możliwość nakładania administracyjnych kar pieniężnych w przypadku naruszania przepisów RODO. Te zaś mogą sięgać nawet wielu milionów euro. Co więcej, osobom, które ponoszą szkody w wyniku takich naruszeń, przysługuje prawo do uzyskania odszkodowania.

Nie trzeba jednak powoływać się na argument sankcji administracyjnych, aby uzasadnić, jak pozorna i krótkowzroczna może się okazać tego rodzaju oszczędność.

Według raportu CERT Polska w ubiegłym roku zarejestrowano przeszło 80 tysięcy unikalnych incydentów cyberbezpieczeństwa. To ponad stuprocentowy przyrost w stosunku do 2022 r. Co więcej, same ataki typu ransomware liczy się już na całym świecie w setkach milionów. Objęte nimi systemy informatyczne gromadzą nie tylko dane osobowe, ale także inne cenne i wrażliwe aktywa administratorów.

Przykłady te pokazują, że adekwatne gwarancje bezpieczeństwa informacji, również tych dotyczących osób fizycznych, stały się po prostu niezbędne we współczesnym świecie gospodarki opartej na danych.

Rola inspektora ochrony danych

Przedsiębiorstwa i organy publiczne często wyznaczają konkretną osobę do realizacji zadań dotyczących przetwarzania danych osobowych. Nie zapominajmy natomiast, że to na administratorze, a nie na osobie działającej w jego imieniu, spoczywa ciężar odpowiedzialności za prawidłowe wykonywanie przepisów RODO.

4 NARUSZENIA I KONTROLE

Niezwykle ważną częścią systemu ochrony danych osobowych są w tym kontekście inspektorzy ochrony danych.

Wśród ich głównych zadań można wskazać budowanie świadomości administratorów, a zatem przede wszystkim najwyższego kierownictwa, na temat spoczywających na nich obowiązków. Monitorują oni także przestrzeganie przepisów RODO wewnątrz organizacji oraz doradzają poszczególnym jednostkom w tym zakresie.

Powszechnym zjawiskiem jest jednak przypisywanie inspektorom nieadekwatnych, nadmiarowych funkcji. Prowadzi to do obarczania ich zadaniami, za których wykonanie w świetle RODO odpowiada wyłącznie administrator. Skutkuje to również niedopuszczalnymi sytuacjami, w których inspektorzy w rzeczywistości nadzorują sami siebie.

Niezrozumienie roli inspektora ochrony danych oraz uchylanie się przez kadrę kierowniczą od obowiązków wynikających z RODO może zatem przesądzić o zaistnieniu konfliktu interesów i naruszeniu przepisów. Niewłaściwą praktyką jest więc np. obarczanie inspektorów odpowiedzialnością za stwierdzanie, kwalifikowanie i zgłaszanie naruszeń ochrony danych osobowych czy też łączenie pracy inspektora ochrony danych z funkcją pełnomocnika administratora lub innym stanowiskiem, w ramach którego inspektor uczestniczy w podejmowaniu decyzji o celach i sposobach przetwarzania.

Perspektywa zmian

Pomimo niepokojących zjawisk warto też zauważyć, że proces budowania świadomości w zakresie przetwarzania i ochrony danych osobowych postępuje. Liczne inicjatywy Prezesa UODO, niezwykle ważna aktywność inspektorów ochrony danych oraz całego środowiska osób zajmujących się tą tematyką, a także generalny wzrost zainteresowania cyberbezpieczeństwem wynikający z upowszechniania się rozmaitych technologii cyfrowych pozwalają żywić nadzieję na większe zaangażowanie decydentów w realizację zadań wynikających z RODO.

Należy również wspomnieć o wielu zakończonych niedawno oraz toczących się jeszcze na szczeblu unijnym procesach legislacyjnych, których efektem będzie rozbudowa całokształtu regulacji dotyczących przetwarzania danych, a także podniesienie rangi przepisów obejmujących szeroko pojęte sprawy bezpieczeństwa cyfrowego.

Niezależnie od tego w najbliższych miesiącach i latach wciąż pozostaje jeszcze wiele do zrobienia w kierunku podniesienia jakości zarządzania naszymi danymi osobowymi oraz zwiększenia poziomu ich bezpieczeństwa.

[1] Więcej na temat definicji „naruszenia ochrony danych osobowych" w „Biuletynie UODO" nr 1/03/23 na str. 13-14.

DZIEŃ DZIECKA W ERZE CYFROWEJ: JAK W KILKU KROKACH ZADBAĆ O PRYWATNOŚĆ I BEZPIECZEŃSTWO NAJMŁODSZYCH ONLINE?

W Dzień Dziecka oprócz tradycyjnych zabawek, rodzice coraz częściej decydują się na kupno prezentu w postaci nowoczesnych gadżetów czy abonamentów do serwisów streamingowych. Jednak z tą cyfrową ekscytacją przychodzi również odpowiedzialność – ochrona prywatności i bezpieczeństwa naszych dzieci w sieci.

1. Zrozumienie zagrożeń

Aby dzieci były bezpieczne, dorośli powinni zdobyć podstawową wiedzę o ich funkcjonowaniu w sieci. Pierwszym krokiem jest zrozumienie potencjalnych zagrożeń. Cyberprzestępczość, cyberprzemoc, niewłaściwe treści, czy narażenie na nadmierną reklamę to tylko niektóre z nich. Ważne jest, by rodzice byli świadomi, co ich dzieci robią w internecie oraz jakie aplikacje i strony odwiedzają.

• Cyberprzestępczość, czyli w tym wypadku – różnorodne ataki, które mogą dotknąć młodych użytkowników: phishing, wyłudzanie danych czy złośliwe oprogramowanie. Dzieci mogą nieświadomie kliknąć w szkodliwe linki lub pobrać zainfekowane aplikacje, co może prowadzić do kradzieży poufnych danych osobowych lub finansowych całej rodziny.

• Cyberprzemoc: To zjawisko obejmuje działania takie jak cyberbullying, stalking czy hejt, które mają miejsce na platformach społecznościowych, w komunikatorach czy podczas gier online. Ofiary tych zabiegów mogą doświadczać stresu, lęku i innych negatywnych skutków.

• Niewłaściwe treści: Dzieci mogą natknąć się na treści nieodpowiednie dla ich wieku, takie jak przemoc czy materiały o charakterze seksualnym. Wystawienie na nie może wywoływać dezorientację i niezdrowe wzorce myślenia.

• Nadmierna reklama: Dzieci są szczególnie podatne na manipulację, co może prowadzić do niechcianych zakupów lub kształtowania niewłaściwych postaw. Aplikacje i gry często są zaprojektowane tak, aby maksymalizować zaangażowanie i wydatki poprzez mikrotransakcje, szczególnie kuszące dla młodszych użytkowników.

2. Edukacja jest kluczowa

O bezpieczeństwie cyfrowym trzeba z dziećmi rozmawiać. Zaczynając te dyskusje możliwie jak najwcześniej, rodzice wyposażą swoje dzieci w narzędzia niezbędne do bezpiecznego i świadomego korzystania z internetu. Podczas rozmów warto wziąć pod uwagę kilka kluczowych aspektów:

Początek edukacji

Można zacząć od prostych zasad, takich jak nieudostępnianie osobistych informacji (np. imię, adres, numer telefonu) osobom trzecim w sieci.

Nauka rozpoznawania zagrożeń

Dzieci powinny znać różne formy zagrożeń w internecie, takie jak phishing, fałszywe strony internetowe czy niebezpieczne linki. Ucząc je, jak rozpoznawać podejrzane wiadomości i oferty, znacząco zwiększamy ich bezpieczeństwo online.

Rozwijanie krytycznego myślenia

Bardzo ważne jest, aby nauczyć dzieci, że nie wszystko, co czytają czy widzą w internecie, jest prawdziwe. Należy rozwijać ich umiejętności krytycznego myślenia, pytając o źródła informacji i ich wiarygodność. To przygotuje je do rozsądnego podejścia do treści online w przyszłości.

Wyjaśnienie, jak szukać pomocy

Dzieci muszą wiedzieć, że zawsze mogą zwrócić się o pomoc do zaufanej osoby dorosłej – rodzica, nauczyciela czy innego opiekuna – gdy natrafią na coś niepokojącego lub niezrozumiałego w internecie.

Bezpieczne zachowania online

Nauka o bezpiecznych praktykach, takich jak korzystanie z silnych, unikalnych haseł, regularne ich aktualizowanie oraz nieklikanie w nieznane linki, to podstawy, które każde dziecko powinno znać. Równie ważne jest uświadomienie dzieciom, że w sieci nie powinny podejmować działań, które mogłyby być szkodliwe lub nieodpowiednie w świecie rzeczywistym.

Ustalanie jasnych reguł

Rodzice powinni ustalić jasne reguły korzystania z internetu, które są dostosowane do wieku dziecka. Obejmuje to ograniczenia czasowe, dopuszczalne typy treści oraz zrozumiałe dla dziecka wyjaśnienia tych ograniczeń.

3. Narzędzia do kontroli rodzicielskiej

Na rynku dostępnych jest wiele narzędzi do kontroli rodzicielskiej, które mogą pomóc w monitorowaniu i ograniczaniu czasu spędzanego przez dzieci w internecie. Pozwalają one na blokowanie dostępu do nieodpowiednich treści, zarządzanie czasem spędzanym przed ekranem, a także śledzenie lokalizacji w przypadku urządzeń mobilnych. Choć niewątpliwie wykorzystanie tych narzędzi wynika z troski o bezpieczeństwo, stawia jednak przed rodzicami szereg pytań dotyczących prywatności, zaufania, a także technicznych i prawnych aspektów ich stosowania. O tym czy i z jakich urządzeń informujących o miejscu pobytu dziecka korzystać oraz jak działają i jakie ryzyka trzeba wziąć pod uwagę pisaliśmy w artykule pt. „Dzieci pod cyfrową opieką: geolokalizacja w służbie rodzicielskiej czujności?", który pojawił się w nr 04/04/24 Biuletynu UODO.

4. Prywatność przede wszystkim

Aby zapewnić odpowiednią ochronę danych dzieci, konieczne jest regularne przeglądanie i aktualizowanie ustawień prywatności na urządzeniach i w kontach online, które dzieci używają. Należy upewnić się, że ustawienia te są skonfigurowane w sposób, który ogranicza dostęp do informacji osobistych i zwiększa kontrolę nad tym, co jest udostępniane i komu.

Warto również zainwestować czas w rozmowy z dziećmi na temat prywatności. Ważne jest, aby zrozumiały, jakie informacje uznaje się za prywatne i dlaczego nie powinny ich udostępniać publicznie lub osobom, które nie są zaufane. Istotne jest także uświadomienie, że takie działania mogą prowadzić do niebezpiecznych sytuacji lub nadużyć.

Dodatkowo, dobrą praktyką jest nauczanie dzieci, jak rozpoznawać sytuacje, w których mogą być proszone o podanie danych osobowych, oraz jak reagować, gdy coś wydaje się podejrzane. Można również wytłumaczyć dzieciom, w jaki sposób technologie takie jak cookies śledzą ich działania online i jak można zarządzać tymi ustawieniami w przeglądarkach internetowych.

5. Bezpieczeństwo urządzeń

Bezpieczeństwo urządzeń, na których dzieci korzystają z dostępu do Internetu, jest kluczowe dla ich ogólnego bezpieczeństwa online. Zapewnienie, że wszystkie urządzenia są odpowiednio zabezpieczone, może znacznie zminimalizować ryzyko wystąpienia zagrożeń takich jak wirusy, malware czy nieautoryzowany dostęp.

• Podstawą zabezpieczenia urządzeń jest regularne aktualizowanie oprogramowania. Producent urządzenia często wydaje aktualizacje, które mają na celu naprawienie znanych luk bezpieczeństwa.

Dlatego ważne jest, aby zawsze instalować najnowsze dostępne aktualizacje systemu operacyjnego oraz aplikacji.

• Instalacja oprogramowania antywirusowego jest kolejnym krokiem w kierunku zapewnienia bezpieczeństwa cyfrowego dzieci. Antywirusy skanują urządzenia w poszukiwaniu szkodliwego oprogramowania i chronią przed jego instalacją. Choć żaden antywirus nie zapewnia stuprocentowej ochrony, jego obecność znacząco zwiększa poziom bezpieczeństwa.

• Również uważne korzystanie z sieci Wi-Fi ma ogromne znaczenie. Należy upewnić się, że dzieci używają tylko zaufanych, zabezpieczonych sieci Wi-Fi. Korzystanie z otwartych, publicznych sieci bez odpowiednich zabezpieczeń może być ryzykowne, gdyż często są one celem dla osób próbujących wykradać dane.

• Rodzice mogą rozważyć włączenie dodatkowych funkcji bezpieczeństwa, takich jak firewall (zapora sieciowa), które mają na celu dalszą ochronę przed nieautoryzowanymi próbami dostępu do urządzenia.

W Dniu Dziecka, warto poświęcić czas na sprawdzenie i zaktualizowanie wszelkich zabezpieczeń na urządzeniach używanych przez dzieci. To doskonała okazja do edukacji najmłodszych o znaczeniu bezpieczeństwa online oraz o tym, jak mogą chronić swoje cyfrowe ślady. Troska o bezpieczeństwo urządzeń to fundament, który pozwala dzieciom bezpiecznie eksplorować cyfrowy świat.

6. Gry i aplikacje

Warto zwrócić uwagę na aplikacje i gry, które dzieci instalują na swoich urządzeniach. Aplikacje często wymagają dostępu do obszernych ilości danych osobowych, co może stanowić potencjalne zagrożenie dla prywatności i bezpieczeństwa młodych użytkowników. Kontrolowanie tego, jakie aplikacje są instalowane na urządzeniach dzieci, jest kluczowe. Rodzice powinni aktywnie uczestniczyć w procesie wyboru i instalacji aplikacji, sprawdzając jakie uprawnienia są przez nią wymagane i oceniając, czy są one rzeczywiście niezbędne do jej funkcjonowania. Również oceny i recenzje innych użytkowników dostarczają cennych informacji na temat bezpieczeństwa i przydatności aplikacji dla dzieci.

7. Promowanie zdrowych nawyków

Dzień Dziecka to doskonała okazja do promowania zdrowych nawyków cyfrowych. Może to obejmować ustalanie konkretnych godzin korzystania z urządzeń, zachęcanie do aktywności fizycznej oraz promowanie treści edukacyjnych, które wzbogacają i rozwijają młode umysły.

5 NOWE TECHNOLOGIE

Zadbanie o bezpieczeństwo dzieci online jest procesem ciągłym, który wymaga współpracy, edukacji i odpowiedzialności zarówno ze strony dzieci, jak i ich opiekunów. Dzień Dziecka jest świetnym momentem na wprowadzenie nowych zasad bezpieczeństwa lub odświeżenia istniejących, gwarantującym, że cyfrowy świat będzie dla najmłodszych miejscem bezpiecznym i przyjaznym.

fot. pixabay

DNI OTWARTE UNII EUROPEJSKIEJ 2024

W dniu 4 maja 2024 r. Komisja Europejska zorganizowała Dzień Otwarty w swojej siedzibie – budynku Berlaymont w Brukseli.

To coroczne wydarzenie jest częścią obchodów Dnia Europy 9 maja, kiedy Unia Europejska upamiętnia podpisanie Deklaracji Schumana w 1950 roku. Tego dnia instytucje europejskie otwierają swoje drzwi dla odwiedzających, aby mogli z bliska przyjrzeć się ich działalności. Dni Otwarte to również wspaniała okazja do odświeżenia swojej wiedzy na temat Unii Europejskiej, jej powstania, rozwoju oraz wyzwań, z którymi obecnie się zmaga.

Dni Otwarte są dla każdego, wejście jest bezpłatne, a spacer po stanowiskach poszczególnych instytucji to tak naprawdę zaproszenie do dobrej zabawy i wzięcia udziału w szeregu angażujących aktywności. W tym roku powierzchnia wystawowa w budynku Berlaymont została podzielona na sześć tzw. wiosek (ang. villages), z których każda skupiała instytucje unijne odpowiedzialne za realizacje określonych polityk. W sumie obejmowały one tak szerokie spektrum zagadnień jak kwestie społeczne, migracyjne, środowiskowe, językowe, gospodarcze, polityczne, kulturowe, i… wiele wiele innych, co zresztą dobrze obrazuje z jak wieloma zadaniami zmagają się na co dzień pracownicy unijnych instytucji.

Tematy z zakresu ochrony danych osobowych, prywatności, a także rozwoju technologii prezentowane były w wiosce „Nasza silna cyfrowa Europa” (ang. Our strong digital Europe). Obok agencji unijnych odpowiedzialnych za rozwój technologiczny i cyfrowy (w tym rozwój europejskiej przestrzeni kosmicznej), znajdowało się wspólne stanowisko Europejskiej Rady Ochrony Danych oraz Europejskiego Inspektora Ochrony Danych, które swoją działalność zaprezentowały w ramach trzech aktywności: quizu, systemu SI do rozpoznawania twarzy w czasie rzeczywistym oraz narzędzia SI do generowania obrazów (tzw. deepfake).

Quiz składał się z sześciu pytań dot. podstawowych zagadnień z zakresu ochrony danych osobowych i prywatności, a także działalności EROD i EIOD. Zasady wzięcia udziału były bardzo proste. Wystarczyło za pomocą telefonu zeskanować kod QR umieszczony w kilku miejscach, który automatycznie odsyłał do strony z pytaniami dostępnymi w trzech wersjach językowych: angielskiej, francuskiej i niderlandzkiej. Quiz był przeprowadzany anonimowo i nie wymagał dokonywania żadnej dodatkowej rejestracji. Jedyną informacją, która mogła pośrednio identyfikować użytkownika był kod IP urządzenia, zapisywany ze względów technicznych i bezpieczeństwa

na lokalnym serwerze. Zaraz po zakończeniu wydarzenia również ta informacja była jednak usuwana.

Zazwyczaj wyniki były bardzo dobre (5-6 pkt). W quizie brały udział osoby z różnych narodowości i we wszystkich przedziałach wiekowych, w tym rodzice z dziećmi. Chociaż nie da się ukryć, że w tym układzie rodzic najczęściej rozwiązywał quiz, a dziecko wybierało nagrodę – gadżet z logiem EROD/EIOD. Specjalnie dla dzieci przewidziany był również ilustrowany komiks.

Narzędzie do rozpoznawania twarzy w czasie rzeczywistym wymagało ustawienia się przed kamerą, która rejestrowała rysy twarzy i odtwarzała na ekranie uchwycony wizerunek uczestnika. Po paru sekundach algorytm urządzenia podawał przetworzone parametry dot. płci, wieku oraz rozpoznanych emocji. Wyniki jakie pojawiały się na ekranie bywały zresztą, ku radości albo ku rozpaczy „zarejestrowanego", bardzo zaskakujące. Wystarczyło bowiem założyć okulary, by zostać automatycznie postarzonym o kilka lat, kolor włosów z kolei był zupełnie ignorowany. Przy określaniu wieku algorytm brał bowiem pod uwagę przede wszystkim takie parametry jak kształt twarzy czy wygląd skóry.

Dużo radości budziło również eksperymentowanie z mimiką twarzy. Urządzenie wychwytywało takie podstawowe emocje jak radość, smutek, złość. Co istotne, neutralny wyraz twarzy nie powodował żadnej albo jedynie minimalną zmianę na wykresie emocji i konieczne było przybranie bardziej ekspresyjnej miny, żeby sprowokować algorytm do wyraźnej reakcji. Trzeba przyznać, że zwłaszcza dzieci świetnie radziły sobie z tym zadaniem.

Trzecia aktywność miała za zadanie zwrócenie uwagi na tzw. technologię deepfake. Na czterech ekranach wyświetlone zostały zdjęcia czterech sławnych, nieżyjących już osób: Marilyn Monroe, Johna Lennona, Whitney Houston oraz Luciano Pavarottiego. Każdy uczestnik mógł wydać do opisu wizerunku wybranej osoby tzw. prompt, a więc polecenie, w jaki sposób chciałby przekształcić jej wygląd. Efekt takiego wpisu wyświetlał się następnie na ekranie. Niektóre prompty były zresztą bardzo zabawne np. „John Lennon w hawajskiej koszuli, grający na ukulele przed budynkiem Berlaymont". Nieco mniej zabawne było to, że wyniki „kolażu" były w wielu wypadkach zaskakująco trafne i realistyczne.

Aktywności zorganizowane przez EROD i EIOD świetnie wpisywały się w filozofię „nauki przez zabawę", która towarzyszyła całemu wydarzeniu. Ochrona danych osobowych i działania obu instytucji, zwrócenie uwagi na kwestię biometrycznego przetwarzania danych w czasie rzeczywistym czy zagrożeń związanych z technologią deepfake, to zagadnienia, z którymi na co dzień zmagają się europejskie i krajowe organy ochrony danych. Tutaj jednak, zamiast konieczności konfrontowania się z rozbudowanymi wytycznymi, odwiedzający w ramach kilkuminutowej zabawy,

mogli przekonać się, jak kwestie te mogą bezpośrednio przekładać się na ich codzienne życie. A po wszystkim mogli jeszcze napić się kawy zrobionej przez robota i jeżeli tylko mieli ochotę, pogawędzić chwilę na mniej lub bardziej poważne tematy z którymś z pracowników, również zadowolonym, że chociaż raz w roku, może wystąpić w mniej formalnej roli.

Nic dziwnego, że wydarzenie cieszy się bardzo dużą popularnością. Od rana odwiedzający ustawiali się w kolejce, a przez korytarze i sale Berlaymont, aż do końca wydarzenia do godz. 18:00 przewijały się setki gości.

Autorka materiału, Karolina Jastalska, specjalistka w Departamencie Komunikacji Społecznej UODO, była wolontariuszką podczas Dni Otwartych KE.

Odwiedzający na stanowisku EROD i EIOD w trakcie Dni Otwartych UE. Zdjęcie udostępnione na stronie Komisji Europejskiej

SPRAWOZDANIE ROCZNE EROD ZA 2023 R.: OCHRONA PRAW CYFROWYCH OSÓB FIZYCZNYCH

Europejska Rada Ochrony Danych (EROD) opublikowała sprawozdanie roczne za rok 2023. Zawiera ono przegląd przeprowadzonych prac i podsumowuje kluczowe osiągnięcia.

Są to:

• uruchomienie pierwszego projektu informacyjnego EROD dla ogółu odbiorców: „Przewodnika po ochronie danych EROD dla małych przedsiębiorstw";
• przyjęcie dwóch wiążących decyzji i jednej pilnej wiążącej decyzji, dostarczających wspólnej interpretacji prawa o ochronie danych i kluczowych zasad prawnych, które będą kształtować cyfrowy krajobraz; oraz
• wybór Anu Talus na przewodniczącą EROD.

Sprawozdanie zawiera też przykłady egzekwowania prawa przez organy ochrony danych na szczeblu krajowym.

Przewodnicząca EROD, Anu Talus, powiedziała: „Zbudowaliśmy imponujące kompendium wytycznych, stworzyliśmy nowe metody współpracy dla organów ochrony danych i przyjęliśmy istotne wiążące decyzje, które pomogą kształtować usługi cyfrowe. Ciężko pracowaliśmy również nad zwiększeniem świadomości na temat RODO na poziomie europejskim i międzynarodowym, aby osoby fizyczne znały swoje prawa i korzystały z nich, a przedsiębiorstwa, nawet te małe, mogły zrozumieć, jak przestrzegać ciążących na nich obowiązków prawnych".

Źródło: komunikat EROD

GRECKI ORGAN NADZORCZY NAŁOŻYŁ NA TAMTEJSZE MINISTERSTWO MIGRACJI I AZYLU ADMINISTRACYJNĄ KARĘ PIENIĘŻNĄ I NAKAZAŁ PRZESTRZEGANIA RODO

Chodzi o dwa programy: „Centaur" i „Hyperion", które były wdrażane na terenie Zamkniętych Centrów Kontrolowanego Dostępu oraz Centrów Recepcji i Identyfikacji dla obywateli państw trzecich. Jak ustalił grecki organ ochrony danych osobowych (HDPA) pod koniec 2021 r., rząd grecki postanowił te programy wdrożyć, by kontrolować przyjmowanie i zakwaterowanie obywateli państw trzecich na wyspach Morza Egejskiego.

„Centaur" to zintegrowany cyfrowy system zarządzania bezpieczeństwem elektronicznym i fizycznym, a „Hyperion" – zintegrowany system kontroli wejścia - wyjścia z czytnikiem w połączeniu z odciskiem palca. Przetwarzał on dane biometryczne gości, pracowników i certyfikowanych członków organizacji pozarządowych.

Dodatkowo grecki organ dostał trzy wnioski:
• Z komisji LIBE Parlamentu Europejskiego (Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych) trafił wniosek o udzielenie informacji na temat technologii nadzoru granic.
• W lutym 2022 r. organizacje społeczeństwa obywatelskiego złożyły wniosek o zbadanie i wydanie opinii w sprawie zamówień i wdrażania systemów „Hyperion" i „Centaur" w ośrodkach przyjmowania i zakwaterowania osób ubiegających się o azyl.
• W lipcu 2022 r. urząd otrzymał również pismo od Przedstawicielstwa UNHCR w Grecji w sprawie tych systemów.

Po zbadaniu sprawy grecki organ nadzorczy stwierdził brak współpracy ze strony ministerstwa jako administratora danych. Uznał też, że analiza ryzyka była niekompletna, a RODO nie jest właściwie przestrzegane.

HDPA nałożył na Ministerstwo Migracji i Azylu karę pieniężną w wysokości 175 000 euro za te naruszenia, a jednocześnie nakazał wypełnienie w ciągu trzech miesięcy obowiązków wynikających z RODO.

Źródło: komunikat greckiego organu nadzorczego (HDPA)

HISZPAŃSKI ORGAN NADZORCZY TRZECI ROK Z RZĘDU OTRZYMUJE NAJWIĘKSZĄ LICZBĘ SKARG W SWOJEJ HISTORII

Hiszpański organ nadzorczy (AEPD) w sprawozdaniu za rok 2023 r. informuje o rosnącej liczbie skarg. W 2023 r. wpłynęło ich 21 590, czyli 43% więcej niż w 2022 r. i 55% więcej w porównaniu z 2021 r.

Skargi dotyczyły najczęściej otrzymywania niechcianych reklam (+114%), usług internetowych (+30%), nadzoru wideo (+29%), handlu, transportu i hotelarstwa (+66%) oraz tych związanych z instytucjami finansowymi/kredytodawcami (+78%).

Jeśli chodzi o procedury nakładania kar pieniężnych, zakończono ich 419, przy czym najczęstsze obszary to nadzór wideo (33%), usługi internetowe (14%), procedury związane z administracją publiczną (6%) i reklama (spam e-mail/SMS) (6%).

W sprawach transgranicznych AEPD prowadził 25 spraw w 2023 r. jako organ wiodący. Współpracowała jako organ nadzorczy, którego sprawa dotyczy, w ponad 300 sprawach. W sprawozdaniu wyszczególniono główne transgraniczne postępowania w sprawie nałożenia sankcji, w których AEPD była organem wiodącym (OpenBank, GlovoApp23, The Mail Track Company) oraz w których była organem nadzorczym, którego sprawa dotyczy (Facebook, TikTok, Instagram i Whatsapp).

Utworzona w 2015 r. jednostka AEPD ds. nieletnich kontynuowała pracę nad kanałem młodzieżowym, który odpowiada za kwestie związane z ochroną dzieci i młodzieży. W 2023 r. zgłoszono ponad 4000 spraw, co stanowi wzrost o ponad 70% w porównaniu z 2022 r. Na pierwszym miejscu znalazły się zapytania rodziców (52%) dotyczące przetwarzania danych ich dzieci. W sprawach rodzinnych najczęstsze zapytania odnosiły się do publikacji zdjęć w sieciach społecznościowych.

Na uwagę zasługują również sprawy związane z przetwarzaniem danych nieletnich w dziedzinie sportu, zwłaszcza w przypadkach rejestrowania i rozpowszechniania obrazów podczas uprawiania sportu w zawodach organizowanych zwykle przez federacje sportowe.

Źródło: komunikat hiszpańskiego organu nadzorczego (AEPD)

EIOD BADA FRONTEX I EUROPOL

Europejski inspektor ochrony danych (EIOD) Wojciech Wiewiórowski przedstawił roczne sprawozdanie przed Komisją Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego (LIBE).

EIOD w zaprezentowanym sprawozdaniu podkreślił znaczenie:

• humanocentrycznego podejścia do sztucznej inteligencji,
• ochrony prywatności migrantów,
• obaw związanych z przetwarzaniem danych przez Frontex (Europejską Agencję Straży Granicznej i Przybrzeżnej) na Lesbos w Grecji,
• a także ryzyko i istotne niedociągnięcia proponowanego rozporządzenia w sprawie materiałów przedstawiających seksualne wykorzystywanie dzieci.

EIOD powiedział, że choć jest organem egzekwującym ustawę o sztucznej inteligencji dla instytucji UE, to jego biuro nie ma na to wystarczających zasobów.

EIOD zajmował się sprawą Frontexu, ponieważ od 2020 r. organ nadzorczy miał obawy dotyczące przetwarzania danych migrantów. Chociaż Frontex poprawił sposób działania, nadal istnieją wątpliwości co do podstaw prawnych przetwarzania danych. Inspektor wyda decyzję w najbliższych tygodniach – powiedział Wojciech Wiewiórowski.

EIOD prowadzi również dochodzenie w sprawie naruszenia danych Europolu dotyczącego brakujących akt osobowych – EIOD ma zastrzeżenia co do wewnętrznych procesów Europolu.

Jeśli chodzi o skargę organizacji NOYB (Europejskiego Centrum Praw Cyfrowych), odnoszącą się do mikrotargetowania Komisji Europejskiej na X (dawniej Twitter), Wojciech Wiewiórowski wyjaśnił, że EIOD nadal zbiera informacje i na tym etapie nie może udzielić dalszych komentarzy. Sprawa ma związek z proponowanym rozporządzeniem UE w sprawie kontroli czatów, szyfrowanej komunikacji online i pozyskiwania publicznego poparcia dla wniosku. NOYB twierdzi, że Komisja Europejska atakowała użytkowników na podstawie ich poglądów politycznych.

Źródło: sprawozdanie EIOD

OBCHODY 20-LECIA ISTNIENIA INSTYTUCJI EUROPEJSKIEGO INSPEKTORA OCHRONY DANYCH

Europejski Inspektor Ochrony Danych świętuje 20-lecie powstania swojej instytucji i z tej okazji organizuje szereg wydarzeń.

EIOD zachęca do udziału w czterech rocznicowych inicjatywach:

• Historia EIOD: Książka i oś czasu

Książka i interaktywna oś czasu pokazują kamienie milowe w ochronie danych i wkładu EIOD w ochronę prywatności. Ważni eksperci opowiadają o przyszłości ochrony danych i wyzwaniach, które przed nami stoją.

• 20 Rozmów

To seria rozmów na temat prywatności i ochrony danych z 20 ekspertami i wpływowymi osobistościami z różnych dziedzin.

• 20 Inicjatyw

W ciągu całego roku EIOD przedstawi 20 inicjatyw ilustrujących jego dążenie do bycia nowoczesnym organem ochrony danych. Będzie promować nowe podejścia i innowacje w swojej pracy, które wzmocnią prawa osób fizycznych do prywatności i ochrony danych.

• Europejski Szczyt Ochrony Danych – „Rethinking Data in a Democratic Society"

20 czerwca 2024 r. odbędzie się Europejski Szczyt Ochrony Danych – debata na temat roli państw w czasach stale rosnącego gromadzenia informacji o obywatelach oraz roli, jaką ochrona danych powinna odgrywać we współczesnych demokracjach. Dyskusja będzie dotyczyć roli ochrony danych, jej możliwości i ograniczeń, sukcesów i straconych szans, w przyczynianiu się do rozwoju fundamentów demokratycznych społeczeństw.

Link do rejestracji dostępny jest tutaj.

Źródło: strona poświęcona obchodom 20-lecia EIOD

WYROK TSUE W SPRAWIE C-61/22 | LANDESHAUPTSTADT WIESBADEN

Według Trybunału Sprawiedliwości UE obowiązek umieszczania dwóch pełnych odcisków palców w nośniku danych dowodów osobistych stanowi ograniczenie prawa do poszanowania życia prywatnego i prawa do ochrony danych osobowych, ponieważ obowiązek ten został przyjęty na niewłaściwej podstawie prawnej.

Obowiązkowe umieszczenie w dowodach osobistych dwóch odcisków palców jest zgodne z prawami podstawowymi. Ponieważ jednak rozporządzenie w tej sprawie zostało wydane w oparciu o złą podstawę prawną, Trybunał Sprawiedliwości UE stwierdził jego nieważność i postanowił, że może być ono stosowane najpóźniej do 31 grudnia 2026. To czas, który pozwoli prawodawcy przyjąć nowe rozporządzenie.

Obywatel niemiecki zaskarżył do niemieckiego sądu odmowę miasta Wiesbaden wydania obywatelowi nowego dowodu osobistego bez umieszczenia w nim jego odcisków palców.

Sąd krajowy zwrócił się do TSUE o zweryfikowanie ważności rozporządzenia UE przewidującego obowiązek umieszczania dwóch odcisków palców na nośniku danych dowodów osobistych. Po wnikliwym zbadaniu sprawy TSUE stwierdził, że obowiązek umieszczania dwóch pełnych odcisków palców w nośniku danych dowodów osobistych stanowi ograniczenie prawa do poszanowania życia prywatnego i prawa do ochrony danych osobowych, gwarantowanych w Karcie Praw Podstawowych UE.

Obowiązek jest jednak uzasadniony celami interesu ogólnego polegającymi na zwalczaniu wytwarzania fałszywych dowodów osobistych i oszustw dotyczących tożsamości, a także na zapewnieniu interoperacyjności systemów weryfikacji. Przetwarzanie jest właściwe i konieczne do realizacji tych celów, a także w stosunku do tych celów proporcjonalne.

W szczególności w zakresie, w jakim umieszczenie dwóch odcisków palców umożliwia zwalczanie wytwarzania fałszywych dowodów osobistych i oszustw dotyczących tożsamości, zabieg ten może się przyczynić zarówno do ochrony życia prywatnego osób, których dane dotyczą, jak i – szerzej – do zwalczania przestępczości i terroryzmu. Ponadto, umożliwiając obywatelom UE wykazanie swej tożsamości w wiarygodny sposób, ułatwia to wykonywanie ich prawa do swobodnego

przemieszczania się i pobytu w UE. Cele takiego rozwiązania mają więc szczególne znaczenie nie tylko dla UE i państw członkowskich, lecz również dla obywateli UE.

Samo umieszczenie wizerunku twarzy stanowiłoby mniej skuteczny środek identyfikacji niż umieszczenie, oprócz tego wizerunku, dwóch odcisków palców. Starzenie się, styl życia, choroba lub zabiegi chirurgiczne mogą bowiem zmienić cechy anatomiczne twarzy.

Trybunał stwierdził nieważność rozporządzenia 2019/1157(1) w sprawie poprawy zabezpieczeń dowodów osobistych obywateli Unii, ponieważ zostało ono wydane na błędnej podstawie prawnej. Stwierdzenie nieważności rozporządzenia ze skutkiem natychmiastowym mogłoby jednak wywołać poważne negatywne konsekwencje dla znacznej liczby obywateli UE i dla ich bezpieczeństwa w przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Z tego powodu Trybunał utrzymał skutki rozporządzenia do czasu wejścia w życie, w rozsądnym terminie i najpóźniej do 31 grudnia 2026 r., nowego rozporządzenia, przyjętego na właściwej podstawie prawnej.

Źródło: Wyrok TSUE

fot. pexels

WYROK ETPC W SPRAWIE ZÖLDI PRZECIWKO WĘGROM (NR 49049/18)

Według ETPC zastosowanie ochrony prawa do poszanowania życia prywatnego i rodzinnego, zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka, i zrównoważenie go z prawami wnioskodawcy, wynikającymi z art. 10, czyli przepisami dotyczącymi wolności wyrażania opinii, nie było zasadne.

Sprawa dotyczy wykorzystania środków publicznych i wysiłków podejmowanych w 2015 r. przez Blankę Zöldi, dziennikarkę śledczą, w celu uzyskania informacji na temat finansów dwóch fundacji utworzonych przez Węgierski Bank Narodowy.

Skarżąca chciała poznać nazwiska osób, które otrzymały dotacje od tych dwóch fundacji. Te odmówiły, a sąd odmowę podtrzymał. W tamtym czasie nie istniał żaden konkretny przepis zezwalający na ujawnienie takich danych osobowych.

Utworzenie i finansowanie fundacji Banku znajdowało się wówczas w centrum debaty publicznej. Powołując się na Art. 10 (Wolność wyrażania opinii) Europejskiej Konwencji Praw Człowieka, pani Zöldi wniosła skargę do Europejskiego Trybunału Praw Człowieka, stwierdzając w niej, że nie mogła uzyskać informacji na temat tożsamości odbiorców dotacji z fundacji utworzonych przez Węgierski Bank Narodowy.

ETPC uznał, że doszło do naruszenia Art. 10 (Wolność wyrażania opinii) Europejskiej Konwencji Praw Człowieka.

Zasądzone zostało zadośćuczynienie:

- szkoda niemajątkowa: 1 000 euro;
- koszty i wydatki: 3 600 euro.

Źródło: Wyrok ETPC

ROZMOWĘ TRZEBA ZACZĄĆ OD SŁUCHANIA

Z dr Joanną Hałoń-Gnutek, lauretką Nagrody im. Michała Serzyckiego rozmawiała Marta Mikołajczyk z Departamentu Współpracy Międzynarodowej i Edukacji UODO, Koordynator Programu „Twoje dane – Twoja sprawa”.

Program „Twoje dane – Twoja sprawa” tworzą ludzie kreatywni, zaangażowani, pełni pasji i chęci do działania. To oni są duszą i motorem programu, dzięki nim idea ochrony prywatności i danych osobowych staje się nie tylko coraz powszechniejsza, ale również naprawdę ważna.

Korzystając z okazji jeszcze raz serdecznie gratuluję Pani otrzymania Nagrody im. Michała Serzyckiego. To jedno z najważniejszych wyróżnień przyznawanych przez Prezesa UODO.

Pierwsze emocje już opadły i mogę na spokojnie zebrać myśli. Czuję wzruszenie i radość nie do opisania. I wdzięczność za zaufanie, którym mnie Państwo obdarzyli. Informacja o otrzymanym wyróżnieniu była dla mnie ogromnym zaskoczeniem. Nie sądziłam, że podejmowane przeze mnie inicjatywy edukacyjne na rzecz ochrony danych osobowych i prawa do prywatności mogą być dla innych nie tylko przydatne, ale także inspirujące. To bardzo mnie cieszy, wręcz dodaje skrzydeł do dalszej pracy. Raz jeszcze z serca dziękuję za wszelkie słowa uznania i gratulacji, które popłynęły w moją stronę.

Program ma na celu uświadomić uczniom, jakie są konsekwencje nierozważnego udostępniania danych osobowych; przekazać wiedzę o sposobach zabezpieczenia swoich danych i tego jak rozsądnie dysponować informacjami o sobie i umiejętnie korzystać z przysługujących praw. Czy dostrzega Pani potrzebę dalszej edukacji uczniów w zakresie ochrony danych osobowych?

Zdecydowanie tak. Edukacja w tym zakresie jest kluczową sprawą, bo warunkuje stworzenie przez młodych ludzi bezpiecznej przestrzeni życia dla siebie i swoich bliskich, zarówno w wymiarze wirtualnym, jak i rzeczywistym. Wiedza, a przede wszystkim praktyczne umiejętności ochrony danych determinują przecież nasze codzienne decyzje, wybory, a nawet życiowe postawy. Pozwalają na asekuracyjne zaangażowanie się w otaczający nas świat. Placówki oświatowe muszą

więc być w forpoczcie działań na rzecz ochrony prywatności.

O czym warto rozmawiać z uczniami? W jaki sposób to robić, aby edukacja była skuteczna?

Zabrzmi to może banalnie: rozmowę trzeba zacząć od słuchania. To najlepszy znany mi sposób, aby nakreślić sobie obraz tego, z czym zmagają się młodzi ludzie, co ich faktycznie interesuje.
Ci, z którymi na co dzień mam kontakt, już dużo wiedzą na temat danych osobowych. Spora w tym zasługa rodziców. Taki punkt wyjścia daje nam szansę na wszechstronne zgłębianie tematu.
Co najbardziej interesuje uczniów? W mojej ocenie regulacje prawne i faktyczne konsekwencje popełnienia lub zaniechania danego czynu, również te odroczone. Chcą sprawnie poruszać się w świecie wirtualnym, a ponieważ tam ryzyko utraty danych czy naruszenia prywatności jest wyższe, potrzebują algorytmu działania w sytuacjach problemowych. Biorąc pod uwagę potrzeby uczniów, najczęściej rozpoczynam zajęcia zaproszeniem do analizy autentycznego lub zaczerpniętego z wartościowej literatury case study, czyli osadzam zagadnienie w konkretnej, bliskiej uczniom czasoprzestrzeni. Dzięki temu natychmiast niwelują się pytania typu „po co mi to?", a budzi się zainteresowanie i otwartość na współpracę. A jeśli podczas ewaluacji lekcji o ochronie danych osobowych wybrzmi użyteczność poznanej wiedzy w codziennym życiu, co więcej – wzrośnie sprawczość uczestników zajęć w zakresie bezpieczeństwa, a także świadomość konsekwencji każdej podjętej decyzji, to przestaję się martwić o ich przyszłość.

Kolejny rok realizuje Pani wspaniałe, innowacyjne projekty edukacyjne w ramach programu „Twoje dane – Twoja sprawa", angażując w nie uczniów. Co Panią motywuje do działania na rzecz upowszechniania wiedzy o ochronie danych osobowych?

Mimo że często podkreślam użyteczność tej wiedzy, nie to jest dla mnie najistotniejsze. Jeśli edukacja ustąpiłaby działaniom podporządkowanym jedynie pragmatycznym celom, stałaby się karykaturą, pseudopracą z uczniami. Szkoła powinna przyczyniać się do lepszego rozumienia siebie samego, uczyć relacji ze światem oraz kontroli własnych zachowań. Inaczej mówiąc, zadbać o wieloaspektowy rozwój człowieka. Zagadnienia związane z ochroną danych osobowych i prawa do prywatności doskonale wpisują się w model edukacji opartej na wartościach. Nie sposób przecież omawiać te tematy bez odwołania się do głębszego, aksjologicznego sensu danego modelu postępowania. Taka idea pracy dydaktyczno - wychowawczej jest mi po prostu bardzo bliska.

Jak stworzyć most i angażować uczniów w działania, skutecznie działać na rzecz zwiększenia ich świadomości, gdy to jednak oni są bardziej biegli w obsłudze

urządzeń, znajomości programów i aplikacji?

Oczywiście zdarza się, że uczniowie sprawniej niż my, dorośli korzystają z komputera, lepiej odnajdują się w gąszczu programów czy aplikacji. Nie zmienia to jednak faktu, że prócz technicznych umiejętności potrzebują jeszcze tego, co nabywa się z wiekiem i doświadczeniem: uważności na szczegóły i przekaz „między słowami", odróżniania faktów od opinii, umiejętności przetwarzania i krytycznej selekcji informacji, rozpoznawania związków przyczynowo-skutkowych i przewidywania konsekwencji swoich działań. Aranżując określone sytuacje podczas zajęć, można dać im bezpieczną przestrzeń na kształtowanie właściwych zachowań. Można po prostu dać im czas na rozmowę o sprawach ważniejszych niż pilne. Skoro człowiek najlepiej uczy się z innymi, warto jak najczęściej umożliwiać im korzystanie z siebie nawzajem jako zasobów edukacyjnych. Jeśli to nie nauczyciel, lecz uczniowie znajdą się w centrum uwagi, istnieje szansa, że staną się odpowiedzialnymi autorami procesu swojego uczenia się. Most zostanie przerzucony na drugi brzeg.

Z jakimi problemami spotyka się Pani na co dzień w swojej pracy?

Staram się być refleksyjnym nauczycielem, a to – jak się okazuje w praktyce – prowadzi do wielu dylematów w obszarze tego, czego i jak nauczać we współczesnym świecie. Realizować podstawę programową, czy stawiać akcent na kompetencje kluczowe? Być tradycyjnym nauczycielem czy partnerem młodego człowieka w jego procesie uczenia się? Pracować według dotychczasowych schematów czy zaryzykować i postawić na innowację? Jak rozciągnąć czas, by sprostać wszystkim formalnym wymaganiom, a jednocześnie realizować z uczniami takie przedsięwzięcia, które zapadną im w pamięć na całe życie, bo uruchamiają emocje i tworzą więzi.

Co my – dorośli – przedstawiciele urzędów, organizacji i szkół, rodzice powinniśmy robić, aby ochrona danych osobowych i dbanie o siebie w obszarze bezpieczeństwa stała się dla uczniów kwestią priorytetową?

Nasuwają mi się na myśl trzy sprawy. Po pierwsze, dawać dobry przykład. Po drugie, być blisko młodego człowieka, obserwować go i uważnie słuchać. Po trzecie, zadbać o profilaktykę pozytywną w zakresie ochrony danych osobowych – wzmacniać i promować dobre wzorce.

Dziękuję za rozmowę.

Kolejna edycja jubileuszowa programu „Twoje dane – Twoja sprawa" startuje 1 września 2024 roku. Zapraszamy szkoły podstawowe i ponadpodstawowe do wspólnych działań na rzecz ochrony prywatności dzieci.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl