URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO

Nr 2/04/23

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo!

Za nami konferencja pod hasłem „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa". Temat ten nie jest przypadkowy. W kwietniu br. obchodzimy ćwierćwiecze systemu ochrony danych osobowych w Polsce, co pozwala wskazać na kluczowe wyzwania dla systemu ochrony danych osobowych w świetle 25 lat jego obowiązywania w naszym kraju.
Głównym zadaniem organu nadzorczego jest zapewnienie skutecznej ochrony danych osobowych obywateli i realizacja ich prawa do prywatności. Urząd Ochrony Danych Osobowych od chwili powołania stał po stronie człowieka. Z przykrością jednak widzimy, kiedy podstawowe prawa człowieka nie są respektowane przez niektórych administratorów. Osoby dotknięte naruszeniem często muszą mierzyć się z konsekwencjami błędu administratora. Jednak równie niezrozumiałe jest to, że sądy wydają coraz więcej wyroków niekorzystnych dla obywateli. Nie sposób się nie odnieść do jednej z głośniejszych spraw w ostatnim czasie, czyli wyroku Naczelnego Sądu Administracyjnego w sprawie wycieku danych w Morele.net, który zapadł 9 lutego 2023 r.
W uzasadnieniu wyroku NSA, wskazując powody uchylenia decyzji UODO, nakładającej karę pieniężną, podważa kompetencje i doświadczenie pracowników Urzędu w istocie uderzają w niezależność organu nadzorczego. Prezes UODO, nie mogąc się z tym zgodzić, skierował list do Prezesa NSA, w którym wyraża głębokie zaniepokojenie niebezpiecznym kierunkiem, w jakim zmierza dokonana przez NSA interpretacja kompetencji i pozycji ustrojowej organu nadzorczego w świetle praw osób, których dane osobowe zostały naruszone. To nie pierwszy przypadek, kiedy UODO musi bronić swojej niezależności. W innym wyroku WSA w Warszawie (wyrok z 28 września 2021 r., sygn. akt II SA/Wa 474/21), uchylając decyzję UODO, uznał, że w sprawie zaniechano zwrócenia się do innego organu właściwego w sprawach związanych m.in. z badaniem zdolności kredytowej i analizą ryzyka kredytowego, co w jego ocenie było bezwzględnie konieczne. Tak jak wtedy, korzystając z instrumentu prawnego w postaci skargi kasacyjnej, zwracaliśmy uwagę na konieczność zapewnienia niezależności organowi ds. ochrony danych osobowych, tak i teraz również to robimy. UODO nie ugnie się w swoich działaniach i będzie zawsze podkreślać swoją niezależność i autonomię, zagwarantowaną przepisami RODO, zgodnie z którymi każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień działa w sposób w pełni niezależny.
Aby jeszcze bardziej dbać o ochronę danych osobowych i prawa do prywatności obywateli, czyli praw gwarantowanych każdemu człowiekowi, UODO podejmuje liczne działania edukacyjno-informacyjne. Do takich z pewnością można zaliczyć podpisanie porozumienia o współpracy z Krajową Izbą Radców Prawnych. Cieszy nas fakt, że tak nowoczesny samorząd zawodowy, który korzysta ze swojego długoletniego doświadczenia, potrafi wskazywać aktualne wyzwania, z jakim sam się mierzy w zakresie ochrony danych osobowych. To jest odpowiedzialne podejście.

Proszę Państwa, podjęliśmy temat trudny, ale bardzo ważny z perspektywy obywatela i ochrony praw jednostki.
Konferencja „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa” rozpoczęła szeroką dyskusję na temat wyzwań dla ochrony danych osobowych obywateli w świetle orzecznictwa sądów i w efekcie doprowadzi do wzmocnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Już otrzymujemy sygnały, że zorganizowane wydarzenie przyczyniło się do poważnej, merytorycznej dyskusji na temat skutecznej realizacji prawa ochrony danych osobowych i poszanowania prywatności. Liczę na współpracę wymiaru sprawiedliwości z polskim organem właściwym w sprawie ochrony danych osobowych, na rzecz zagwarantowania realnej ochrony danych osobowych obywateli i pewność prawną w tym obszarze.

Jakub Groszkowski
Zastępca Prezesa UODO

Drodzy Czytelnicy!

W kwietniu tego roku obchodzimy 25 lat obowiązywania systemu ochrony danych osobowych w Polsce. To bardzo ważna rocznica, która jednocześnie przypomina nam, że ochrona danych osobowych czy prawo do prywatności nie są niczym nowym i nie zostały wprowadzone rozporządzeniem o ochronie danych (RODO). Pomimo ćwierćwiecza systemu ochrony danych nadal zauważamy problemy ze zrozumieniem kwestii podstawowych w tej materii jak np. definicji danych osobowych czy niezależności organu nadzorczego. Szerzej na ten temat wypowiadali się prelegenci debaty pt. „System ochrony danych osobowych w pracach regulatorów na rzecz obywatela" podczas konferencji pod hasłem „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów". Co ciekawe do samego końca organizowanej przez UODO konferencji, liczba uczestników była bardzo wysoka. Uczestniczyło w niej za pośrednictwem Internetu kilkaset osób, co świadczy o tym jak ten temat jest ważny i aktualny. Pragnę też zwrócić Państwa uwagę, że o znaczeniu ochrony danych osobowych w codziennej działalności regulatorów dyskutowano przy udziale przedstawicieli UKE, UOKiK oraz przedstawicieli przedsiębiorców, np. KRD, i organizacji pozarządowych. Tym samym przedstawiliśmy szerokie spektrum problemów, z jakimi się mierzymy wszyscy. Organ nadzorczy każdego dnia dzieli się swoją wiedzą i doświadczeniem z monitorowania i przestrzegania RODO, rozpatrywania skarg od osób, których dane dotyczą w zakresie sposobu przetwarzania tych danych czy wspomagania administratorów i inspektorów ochrony danych w realizacji ich zadań. Urząd co roku wydaje wiele decyzji. Ich liczba na przestrzeni lat stale rośnie. W roku 2021 Prezes Urzędu Ochrony Danych Osobowych wydał prawie 2100 decyzji administracyjnych, prawie o 20 proc. więcej niż rok wcześniej. I choć decyzje nakładające administracyjne kary pieniężne, stanowią kilka procent wszystkich wydawanych przez organ nadzorczy, a przypomnę, że łącznie było ich 65, to nadal cieszą się one największym zainteresowaniem i opinii publicznej, jak i samych administratorów. Urząd stale podkreśla, że nakładane kary administracyjne nie są celem samym w sobie. Warto podkreślić, że RODO to niekończący się proces, nieustanne dostosowywanie przyjętych rozwiązań do stale zmieniających się warunków – także prawnych i technologicznych. UODO wielokrotnie sygnalizował, że ustawodawca, projektując przepisy przewidujące przetwarzanie danych osobowych powinien precyzyjnie określić role, obowiązki i uprawnienia podmiotów. Tak jest i tym razem, o czym przeczytacie Państwo w „Biuletynie UODO", kiedy UODO zwraca uwagę, że ustawodawca powinien precyzyjnie regulować korzystanie z rozwiązań informatycznych. W zakresie ochrony danych osobowych jest też przed nami wiele wyzwań, z którymi w najbliższym czasie trzeba będzie się zmierzyć. Pożądane jest również ujednolicenie podejścia do ochrony danych osobowych i prawa do prywatności, czy to przez ustawodawcę czy sądownictwo.

O tym, jaką rolę odgrywa orzecznictwo sądów administracyjnych w kształtowaniu praktyki przetwarzania danych osobowych i o tym, jak wydawane wyroki mają bezpośredni wpływ na bezpieczeństwo danych osobowych nas Polaków przeczytacie Państwo w wywiadzie z Jackiem Młotkiewiczem, dyrektorem Departamentu Kontroli i Naruszeń w UODO.
Rolą UODO jest wskazanie właściwej ścieżki postępowania i pożądanych kierunków działania, a także budowanie odpowiednich postaw obywateli oraz określonej praktyki stosowania przepisów RODO przez administratorów. UODO pozostaje otwarty na współpracę z podmiotami faktycznie zainteresowanymi ochroną danych osobowych. Do takich można zaliczyć spotkania przedstawicieli UODO, jakie odbywają się z inicjatywami pracującymi nad kodeksami postępowania czy podpisanie porozumienia o współpracy z Krajową Izbą Radców Prawnych.
W działalności UODO ważne miejsce zajmuje edukacja, która jest przede wszystkim ukierunkowana na popularyzowanie wiedzy o prawie ochrony danych tak, aby podnosić świadomość społeczeństwa w tym zakresie i zachęcać do odpowiedzialnego posługiwania się danymi. Działania te obejmują także podnoszenie świadomości Polaków nt. bezpiecznego posługiwania się danymi osobowymi podczas korzystania np. z nowych technologii. Obecnie musimy nieustannie radzić sobie z natłokiem informacji. Coraz trudniej jest nam odróżnić prawdziwe i rzetelne treści od tzw. fake newsów, które celowo wprowadzają odbiorcę w błąd. Więcej na ten temat w materiale „Deepfake. Czy wiesz, jak nie dać się oszukać, oglądając zdjęcia lub filmy wideo".
W tym numerze „Biuletynu UODO" znajdziecie Państwo także wiele innych ciekawych materiałów, które odnoszą się do ochrony danych osobowych i prawa do prywatności każdego z nas.
Udanej lektury!

Adam Sanocki
Rzecznik Prasowy UODO
Dyrektor Departamentu
Komunikacji Społecznej UODO

1 ROZMOWA Z EKSPERTEM

DOROBEK ORZECZNICZY POWINIEN KSZTAŁTOWAĆ STANDARDY, MAJĄC NA UWADZE TROSKĘ O OBYWATELA

Jacek Młotkiewicz, dyrektor Departamentu Kontroli i Naruszeń w UODO w rozmowie z Eweliną Janczylik-Foryś o administracyjnych karach pieniężnych i wpływie orzecznictwa sądów administracyjnych w ich zakresie na skuteczność ochrony danych osobowych w Polsce.

Panie Dyrektorze, nie milkną echa konferencji UODO pod hasłem „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów". Dlaczego ta konferencja była tak ważna z punktu widzenia UODO?

Chcieliśmy zabrać głos w tej niezwykle ważnej dyskusji i wskazać, jak orzecznictwo ma wpływ na bezpieczeństwo danych każdego Polaka. Mimo iż nie zawsze zgadzamy się z sądem co do powodów uchylenia decyzji, np. nakładającej administracyjną karę pieniężną, czego efektem są składane przez nas skargi kasacyjne w przypadku wyroków WSA, to do każdego orzeczenia podchodzimy z szacunkiem, wiedząc, jak ważną rolę odgrywa orzecznictwo sądów administracyjnych w kształtowaniu właściwej praktyki przetwarzania danych osobowych. Wierzymy, że dorobek zarówno nasz – UODO, jak i sądów administracyjnych przyczynia się obecnie do budowania w tym obszarze coraz lepszych i efektywnych standardów na miarę trzeciej dekady 21. wieku i ma bezpośredni wpływ na bezpieczeństwo danych osobowych nas Polaków.

W swoim wystąpieniu wiele miejsca poświęcił Pan omawianiu „najgłośniejszych" administracyjnych kar pieniężnych.

Nie ulega wątpliwości, że do najważniejszych działań organu nadzorczego należy monitorowanie przestrzegania RODO i reagowanie w sytuacji naruszenia przepisów tego aktu prawnego. I choć organ nadzorczy podejmuje szereg działań edukacyjnych, budując tym samym pewną określoną praktykę stosowania przepisów RODO i wskazując pożądany kierunek postępowania w ramach określonego zagadnienia związanego z ochroną danych osobowych, to są jednak działania, które nie mają charakteru władczego. Najbardziej dobitnym przykładem monitorowania przestrzegania przepisów rozporządzenia są oczywiście decyzje nakładające administracyjną karę pieniężną.

UODO powtarza, że nakładanie kar nie jest celem samym w sobie.

Administracyjne kary pieniężne to narzędzie, w jakie prawodawca unijny wyposażył organy nadzorcze w celu zapewnienia prawidłowej realizacji obowiązków wynikających z RODO i efektywnej ochrony praw osób fizycznych. Miały one spowodować, że RODO będzie faktycznie przestrzegane, bo wcześniej obowiązujące w obszarze ochrony danych osobowych rozwiązania okazały się nieskuteczne. Wobec tego nie tylko przewidziano takie uprawnienie dla organów nadzorczych, ale i wyznaczano górną granicę kar na odpowiednio wysokim poziomie, tj. do 20 mln euro. Administracyjna kara pieniężna według RODO musi być nie tylko proporcjonalna, ale też odstraszająca.

Wszystko po to, aby administrator nie unikał inwestycji w bezpieczeństwo przetwarzanych przez siebie danych osobowych i nie wkalkulowywał ewentualnych niskich kar w koszty prowadzonej przez siebie działalności. Nie można jednak nie wskazać, że nakładanie kar ma skłonić administratorów do przekonania, że wywiązywanie się z ich obowiązków, m.in. w zakresie zapewnienia danym właściwego poziomu bezpieczeństwa, jest koniecznością wynikającą z potrzeby ochrony osób, których dane osobowe, w swojej działalności te podmioty wykorzystują, a także że leży i w ich interesie, bowiem coraz większa grupa świadomych swoich praw osób także i przez ten pryzmat ocenia podmioty, którym chce przekazać swoje dane osobowe.

Z wystąpień udzielonych podczas konferencji „Wyzwania dla ochrony danych osobowych w świetle orzecznictwa sądów" można wywnioskować, że im wyższa kara pieniężna nakładana przez organ nadzorczy, tym większe prawdopodobieństwo, że zostanie wniesiona skarga na decyzję Prezesa UODO. Czy zgadza się Pan z tym stwierdzeniem?

Od początku stosowania RODO, Prezes Urzędu wydał 65 decyzji nakładających administracyjną karę pieniężną, z których 33 zostało zaskarżonych do Wojewódzkiego Sądu Administracyjnego w Warszawie. Dotychczas WSA rozpatrzył 27 spraw, w 19 oddalając skargę. Z tych 19 wyroków do NSA zaskarżonych zostało 13, który do tej pory zajął się jedną sprawą – uchylając zarówno wyrok WSA, jak i decyzję organu nadzorczego. Chodzi o sprawę Morele.net. Odpowiadając na Pani pytanie, rzeczywiście taki wniosek się nasuwa, ponieważ wyroki uchylające nasze decyzje dotyczą przede wszystkim tych decyzji, w których wysokość nałożonej administracyjnej kary pieniężnej wynosiła około 1 mln zł i więcej.

Nie sposób nie odnieść się do sprawy sprzed kilku tygodni, czyli do wyroku Morele.net. Jakie jest stanowisko UODO w tym zakresie?

Naczelny Sąd Administracyjny zakwestionował naszą decyzję z powodów trudnych dla nas do zaakceptowania. Wyrok, do którego się Pani odnosi, został wydany w sprawie związanej z bardzo głośnym wyciekiem danych, jaki miał miejsce w Morele.net, za co podmiot ten został ukarany przez Prezesa Urzędu administracyjną karą pieniężną w wysokości prawie 3 mln zł. Podstawowy zarzut sądu, który spowodował uchylenie zarówno korzystnego dla organu nadzorczego wcześniejszego wyroku WSA w Warszawie, jak i samej decyzji, związany był z nieuwzględnieniem wniosku strony o przeprowadzenie dowodu z opinii biegłego. Sąd stwierdził, że skorzystanie z opinii biegłego było konieczne, ponieważ pracownicy UODO nie dysponują wystarczającą wiedzą do dokonania prawidłowej oceny zgromadzonego w sprawie materiału dowodowego dotyczącego zabezpieczeń. Swój pogląd w tym zakresie sąd uzasadnił zbyt krótkim czasem, jaki upłynął od momentu rozpoczęcia stosowania RODO (maj 2018 roku) do czasu wydania decyzji nakładającej administracyjną karę pieniężną (wrzesień 2019 roku), przez co pracownicy nie mogli nabyć niezbędnego doświadczenia. Szczególnie trudno nam zaakceptować, że NSA nie przyjął naszej argumentacji, iż doświadczenie pracowników Urzędu wynika również z okresu obowiązywania poprzednich przepisów o ochronie

danych osobowych, na podstawie których przez lata oceniane były przez nas środki bezpieczeństwa z uwzględnieniem takich elementów, jak kategorie danych osobowych i zagrożenia dla nich. Trudno zgodzić się, że wieloletnie doświadczenie organu ds. ochrony danych jest bez znaczenia tylko dlatego, że zostało wprowadzone RODO.
Po drugie, zarzut ten jest niezrozumiały jeszcze z jednego istotnego względu. Skoro pracownicy UODO przeprowadzający kontrolę w siedzibie Morele.net oraz opracowujący projekt decyzji w sprawie tego wycieku danych nie mieli wystarczającego doświadczenia jedynie z uwagi na krótki czas, jaki upłynął od maja 2018 roku do wystąpienia naruszenia w tej spółce i jego oceny przez Urząd, czyli zbyt krótki okres stosowania RODO, to taka sama ocena powinna dotyczyć przecież doświadczenia jakiegokolwiek biegłego, który miałby się zająć oceną tego przypadku. W praktyce wyrok NSA oznacza, że w tym czasie nie było nikogo, kto miałby i kompetencje i doświadczenie do oceny tej sprawy.

Sprawa Morele.net i postępowania sądowego, nie była jedyną, na jaką zwracał Pan uwagę podczas konferencji. Jakie inne postępowania także Pan omówił?

Innym, kwestionującym decyzję UODO wyrokiem sądu, do którego się odniosłem, jest wyrok dotyczący decyzji nakładającej administracyjną karę pieniężną na Cyfrowy Polsat. W tym przypadku zarzucono, że Urząd nie wziął pod uwagę okoliczności, która w ogóle nie była przedmiotem jakiegokolwiek sporu, czy wątpliwości w toku postępowania. Chodziło o brak wystarczającego wykazania w decyzji, że podmiot ten jest administratorem danych. Cyfrowy Polsat wysunął twierdzenie, że nie jest administratorem dopiero w złożonej skardze na decyzję i sąd do tego twierdzenia się przychylił. Tymczasem w toku postępowania administracyjnego Cyfrowy Polsat nie kwestionował w ogóle tej okoliczności, a ponadto cała jego wcześniejsza działalność związana z obsługą naruszeń ochrony danych osobowych, których zbyt późna identyfikacja spowodowała wszczęcie postępowania, potwierdzała, że uznaje się on za administratora. W materiale dowodowym znajdowały się zgłoszenia naruszenia ochrony danych osobowych dokonane przez Cyfrowy Polsat wraz z treścią skierowanych przez niego zawiadomień do osób, których dane dotyczą, co przecież jest obowiązkiem właśnie administratora. Ponadto w materiale dowodowym była umowa, na podstawie której Cyfrowy Polsat powierzył przetwarzanie danych osobowych innemu podmiotowi – firmie kurierskiej, który w jego imieniu dostarczał dokumenty związane ze świadczeniem usług telekomunikacyjnych abonentom Cyfrowego Polsatu w celu ich podpisania. Charakter tych dokumentów nie pozostawiał żadnych wątpliwości, że to właśnie Cyfrowy Polsat jest administratorem danych tych osób, dla których przecież świadczy usługi telekomunikacyjne. Tych okoliczności sąd jednak w ogóle nie wziął pod uwagę. Nie chciałbym jednak, aby powstało wrażenie, że sądy mają w większości odmienne zdanie niż UODO.
W postępowaniu administracyjnym zapada wiele wyroków utrzymujących w mocy decyzje UODO, w których sądy w pełni przychylają się do ustaleń organu nadzorczego.

Jakie to wyroki?

Wśród wyroków sądów potwierdzających słuszność przyjętej przez nas oceny, a dotyczących naruszeń przepisów RODO odnoszących się do bezpieczeństwa danych, można wyróżnić te, które wpływają na utrwalenie określnych stanowisk w świadomości administratorów i znacząco wpływają na praktykę. Kilka wyroków, oddalających skargę, potwierdzało nasze stanowisko, że środki techniczne i organizacyjne mające zapewnić odpowiednią ochronę danych osobowych powinny być dobrane przez administratora danych w wyniku uprzednio przeprowadzonej analizy ryzyka, a następnie poddawane ciągłemu monitorowaniu pod kątem ich skuteczności. Inna grupa orzeczeń potwierdza prezentowane przez nas stanowisko, że ryzyka związane z wystąpieniem naruszeń ochrony danych osobowych w organizacji administratora nie muszą się zmaterializować, by po stronie administratora danych powstały określone obowiązki związane z obsługą tych naruszeń, w tym obowiązek zgłoszenia naruszenia organowi nadzorczemu oraz zawiadomienia osób, których ono dotyczyło, jeżeli ryzyko naruszenia praw lub wolności tych osób było wysokie. Chcę także powiedzieć, że korzystanie z takiego instrumentu, jakim są administracyjne kary pieniężne, było i jest dla nas dużym wyzwaniem, zadaniem wymagającym odwagi i ciężkiej pracy. Ta trudna praca jest po naszej stronie i po stronie sądów weryfikujących nasze decyzje. Niemniej dzięki administracyjnym karom pieniężnym odpowiedniej wysokości w każdym szczegółowo uzasadnionym przez nas przypadku możemy dużo lepiej wypełniać naszą misję i przyczyniać się do zapobiegania zdarzeniom, które mogą mieć dla osób fizycznych bardzo doniosłe i trudne do zaakceptowania skutki. Bardzo zależy nam na tym, aby dorobek orzeczniczy ukształtował pewne standardy, dzięki którym administratorzy zawsze podczas przetwarzania danych osobowych będą mieli na względzie dobro obywateli.

wniosek

Administracyjna kara pieniężna według RODO musi być nie tylko proporcjonalna, ale też odstraszająca. Wszystko po to, aby administrator nie unikał inwestycji w bezpieczeństwo przetwarzanych przez siebie danych osobowych i nie wkalkulowywał ewentualnych niskich kar w koszty prowadzonej przez siebie działalności.

Panie Dyrektorze, jedną z najbardziej interesujących spraw na przestrzeni tego roku były także pytania skierowane przez UODO do administratorów.

Tak, pewnie chodzi Pani o „słynne” 27 pytań, które miały na celu kompleksową weryfikację przestrzegania obowiązków administratorów związanych z wyznaczeniem i funkcjonowaniem inspektorów ochrony danych i objęły wszystkie kluczowe kwestie w tym zakresie.

Dokładnie. Proszę powiedzieć, czy są już jakieś pierwsze efekty w tej sprawie?

Pytania zostały skierowane do ponad 20 administratorów danych, zarówno z sektora publicznego, jak z sektora prywatnego, do administratorów korzystających z tzw. zewnętrznego inspektora ochrony danych, jak i tych, którzy takiego inspektora zatrudniają na podstawie umowy o pracę. Obecnie za wcześnie jest mówić o kompletnych wynikach tej akcji, ale faktycznie pierwsze efekty są już zauważalne. Nie ukrywam, że skoro niektóre z tych pism zostały skierowane do administratorów korzystających z usług zewnętrznego inspektora ochrony danych, świadczonych przez podmioty zajmujące się profesjonalnie tego typu działaniami od dłuższego czasu, to spodziewaliśmy się również profesjonalnych, a przede wszystkim wyczerpujących odpowiedzi na zadane pytanie. Niestety, część z tych administratorów podeszła w sposób bardzo lekceważący do tych pytań, udzielając bardzo lakonicznych odpowiedzi i nie popierając ich żadnym dokumentem, pomimo wyraźnego wezwania do przedstawienia dowodów potwierdzających składane wyjaśnienia. Oczywiście nasza reakcja mogła być tylko jedna, czyli ponowne wezwanie w tym zakresie do złożenia wyjaśnień wraz z dowodami, a są też przypadki, w których zdecydowaliśmy się na przeprowadzenie kontroli u takiego administratora, oczywiście w zakresie objętym treścią pytań. Na ten moment u czterech administratorów zostały przeprowadzone kontrole stacjonarne wynikające z lakoniczności przesłanych odpowiedzi.

wniosek

Listę 27 pytań administratorzy wykorzystywali do autokontroli w zakresie realizacji swoich obowiązków odnoszących się do zagwarantowania IOD właściwej pozycji i prawidłowego wykonywania zadań. Z kolei inspektorzy uznali je - zgodnie z intencją UODO - za zwracające uwagę na ich szczególną rolę, a jednocześnie będące dla nich wsparciem i mające przełożenie na efektywne wypełnianie przez nich funkcji.

W czasie prowadzonych postępowań stwierdzono liczne nieprawidłowości dotyczące powołania i funkcjonowania inspektorów ochrony danych, które dotyczą takich kwestii, jak np.: niewłaściwe włączanie IOD w sprawy dotyczące ochrony danych osobowych, niepodejmowanie działań mających na celu zapewnienie inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej, brak procedur zapewniających niezależność inspektora ochrony danych, w szczególności dotyczących zakazu otrzymywania instrukcji, wydawania poleceń, jak również zapewnienia, że w ramach wykonywania zadań inspektora ochrony danych nie będzie on odwoływany ani karany. Wiele z naszych zastrzeżeń związanych też było z nałożeniem na inspektorów ochrony danych zadań, które należą do obowiązków administratorów, jak np. prowadzenie rejestru czynności przetwarzania, rejestru naruszeń ochrony danych osobowych czy tworzenia wewnętrznych polityk. Inspektor nie może bowiem być obciążony działaniami, które ma oceniać pod kątem ich zgodności z przepisami prawa i regulacjami wewnętrznymi administratora.

Urząd wielokrotnie wskazywał na to w materiałach publikowanych na swojej stronie internetowej. Wobec jednego z administratorów zostało wszczęte postępowanie administracyjne. Przygotowywane są również zawiadomienia o wszczęciu postępowania w stosunku do kolejnych administratorów. Pozostałe wyjaśnienia złożone przez administratorów są sukcesywnie poddawane analizie.

Faktycznie, te dane nie napawają optymizmem.

Proszę jednak zwrócić uwagę, że byli również i tacy administratorzy, którzy do tematu podeszli rzetelnie i przekazali do UODO nie tylko odpowiedzi, które stanowiły pełne i szczegółowe odniesienie się do poruszonych kwestii, ale wsparli je odpowiednimi dowodami, np. wdrożoną u nich kompleksową dokumentacją potwierdzającą składane wyjaśnienia. W taki sposób powinna działać jedna z najważniejszych zasad przyjęta w RODO – zasada rozliczalności. W największym skrócie sprowadza się ona do tego, że jeśli prawo nakłada na mnie określone obowiązki i ja się z nich wywiązuję, mam wdrożone w danym obszarze odpowiednie rozwiązania, to szybko i w przekonujący sposób potrafię to wykazać. Pozytywne jest to, że dla niektórych podmiotów, do których skierowaliśmy nasze pytania, istota tej zasady była od dawna jasna, a to przyczyniło się z kolei do właściwego zareagowania na wezwania naszego urzędu. Mam nadzieję, że na dalszych etapach prowadzenia tej akcji świadomość administratorów co do obowiązku sumiennego wykazania, że przepisy dotyczące inspektorów są przestrzegane, będzie coraz lepsza. Tym bardziej, że rozpoczęta w marcu 2022 r. weryfikacja dotycząca IOD nie jest przecież – jak już informowaliśmy – akcją jednorazową. Ponadto to, co mnie bardzo cieszy, to postrzeganie i wpływ tych działań organu nadzorczego. Administratorzy wspomnianą listę 27 pytań wykorzystywali do autokontroli w zakresie realizacji swoich obowiązków odnoszących się do zagwarantowania IOD właściwej pozycji i prawidłowego wykonywania zadań. Z kolei inspektorzy uznali je – zgodnie z intencją UODO – za zwracające uwagę na ich szczególną rolę, a jednocześnie będące dla nich wsparciem i mające przełożenie na efektywne wypełnianie przez nich ich funkcji. Warto też wspomnieć, że rozpoczęta w zeszłym roku przez UODO weryfikacja obecnie doskonale wpisuje się w podjęte przez EROD działanie w zakresie ram skoordynowanego egzekwowania prawa "CEF 2023". W 2023 r. dotyczy ono wyznaczania i pozycji inspektorów ochrony danych. UODO bierze udział w tym działaniu wraz z innymi organami nadzorczymi.

Czy mógłby Pan więcej powiedzieć o działaniach UODO w ramach „CEF 2023”?

Inicjatywy CEF mają na celu usprawnienie egzekwowania przepisów i współpracy między organami nadzorczymi. W tym roku działania EROD dotyczą przepisów o ochronie danych osobowych związanych z wyznaczeniem i funkcjonowaniem inspektorów ochrony danych i na poziomie krajowym mogą przybierać różne formy, w tym związane z korzystaniem przez organy z uprawnień nadzorczych. W przypadku organów, które – tak jak UODO – już wcześniej rozpoczęły postępowania w tym zakresie, współdziałanie będzie polegać na kontynuowaniu postępowań lub przeanalizowaniu ich wyników, by następnie wymienić się z innymi organami wnioskami płynącymi z tych działań.

USTAWODAWCA POWINIEN PRECYZYJNIE REGULOWAĆ KORZYSTANIE Z ROZWIĄZAŃ INFORMATYCZNYCH

Ustawodawca, projektując przepisy przewidujące przetwarzanie danych osobowych przy użyciu aplikacji, portali, wspólnych systemów czy innych rozwiązań informatycznych, powinien precyzyjnie określić role, obowiązki i uprawnienia podmiotów korzystających z tych narzędzi.

Przepisy RODO wskazują, że każde przetwarzanie danych osobowych powinno być planowane z uwzględnieniem koncepcji ochrony danych (i prywatności) w fazie projektowania (privacy by design). Zatem gdy ustawodawca przewiduje, że przetwarzanie danych osobowych będzie prowadzone z wykorzystaniem określonych rozwiązań informatycznych, to od samego początku, na każdym etapie projektowania ich wykorzystywania, pod uwagę powinien brać wpływ, jaki ich stosowanie wywrze na sferę prywatności. Uwzględniać przy tym musi stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych, a jednocześnie tak projektować planowane cyfrowe rozwiązania, by były odpowiednie dla konkretnego przypadku. Dodatkowo ważone powinno być przy tym wynikające z przetwarzania ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Ustawodawca powinien też przewidywać mogące pojawić się problemy związane z wykonywaniem tworzonych przepisów. Oprócz uwzględniania ochrony danych w fazie projektowania (art. 25 ust. 1 RODO) równie istotne jest też wdrożenie mechanizmów zapewniających stosowanie zasady domyślnej ochrony danych (art. 25 ust. 2 RODO). Zasadę tę należy rozumieć jako postulat uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego mają być zbierane (minimalizacja danych). Pożądane jest, aby ten aspekt brać pod uwagę już na etapie projektowania rozwiązań prawnych. To one powinny być skonstruowane tak, by z jednej strony umożliwiały spełnianie wskazanych w RODO zasad, a z drugiej strony pozwalały na zachowanie gwarantowanej w RODO neutralności technologicznej.

2 UODO SYGNALIZUJE

Tymczasem polski ustawodawca, projektując przepisy przewidujące przetwarzanie danych osobowych przy użyciu różnego rodzaju rozwiązań informatycznych, w wielu przypadkach zdaje się zapominać o tych zasadach. Przyjmuje rozwiązania powodujące niepewność prawa, nieodpowiadające wymogom RODO, a przecież projektodawca (ustawodawca) nie może dopuszczać do wystąpienia problemów w zrozumieniu i interpretacji przepisów, a także tworzyć przepisów niezapewniających stosowania RODO czy pozostających z nim w sprzeczności, które powodują potencjalne istotne ryzyka w zakresie przetwarzania danych osobowych. Rozwiązania obarczone tego rodzaju brakami są nieczytelne zarówno dla osób, których dane mają być przetwarzane, jak i dla wykonawców tych norm, mogą budzić ich uzasadnione wątpliwości i powodować brak pewności prawa, co również zagraża zasadzie zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a RODO).

Wymagania dla systemu

Problemy zaczynają się już w momencie przyjmowania niekonkretnych, blankietowych przepisów, przewidujących i poprzestających na stwierdzeniu, że przetwarzanie danych osobowych będzie realizowane przy wykorzystaniu aplikacji bądź systemu informatycznego, bez odpowiedniego ich zdefiniowania. Wprowadzane niekiedy odesłanie jedynie do definicji systemu teleinformatycznego zawartej w ustawie z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne jest niewystarczające. Prowadzi to bowiem do pozostawienia wykonawcom norm prawnych zupełnej dowolności przy dokonywaniu wyboru odpowiednich środków technicznych i organizacyjnych, a niekiedy nawet rodzajów aplikacji mających służyć realizacji określonych zadań.

Podkreślić przy tym należy, że RODO nie stoi na przeszkodzie wolności technologicznej. Wręcz odwrotnie, wskazuje w motywie 15, że „aby zapobiec poważnemu ryzyku obchodzenia prawa ochrona osób fizycznych powinna być neutralna pod względem technicznym oraz że nie powinna zależeć od stosowanych technik".

Jednak pełna dowolność i niedookreśloność rozwiązań nie powinna mieć miejsca w przypadku regulacji odnoszących się do realizacji zadań publicznych, niezależnie od tego, przez jakie podmioty jest ono dokonywane. Powoduje to ryzyko korzystania z rozwiązań, które uniemożliwiają spełnienie określonych w RODO (w tym jego art. 24 i 32) wymogów i nie dają gwarancji bezpieczeństwa dla przetwarzanych danych osobowych.

Określenie ról i odpowiedzialności

Równie istotne jest precyzyjne określenie:
- ról podmiotów korzystających z konkretnych systemów i narzędzi informatycznych w procesach /operacjach/ zestawach operacji przetwarzania danych osobowych,
- praw i obowiązków poszczególnych podmiotów w zakresie prowadzenia, funkcjonowania i wykorzystywania konkretnych rozwiązań informatycznych, w których są przetwarzane dane osobowe,
- procedur związanych z przetwarzaniem danych osobowych przy użyciu projektowanych systemów/narzędzi,
- norm odnoszących się do obowiązku zapewnienia poufności i integralności przetwarzania danych osobowych,
- okresu retencji danych.

Nie może się to jednak odbyć w oderwaniu od jasnego i precyzyjnego określenia zadań i celów, dla których dane osobowe mają być przetwarzane.
Przepisy ustawowe powinny również określać, jakie dane osobowe mają być przetwarzane i jakich kategorii podmiotów będą dotyczyć. Istotne jest również określenie, kto, komu, na jakich zasadach i w jakim trybie udostępniać będzie dostępne dane. Jeżeli zamierza się przekazywać dane osobowe do państw trzecich i organizacji międzynarodowych, to niezbędne jest spełnianie przesłanek z art. 46–49 RODO. Jest to szczególnie istotne w przypadku podmiotów publicznych, które zobowiązane są, by działać na podstawie i w granicach prawa, a także centralnych systemów zarządzanych przez odrębnych administratorów czy współadministratorów.

2 UODO SYGNALIZUJE

Dzięki szczegółowemu określeniu wskazanych wyżej kwestii w przepisach ustaw, możliwe jest zapewnienie zgodności wszystkich działań na danych osobowych z wymogami RODO, w tym z zasadami zgodności z prawem, rzetelności i przejrzystości, minimalizacji danych, ograniczenia przechowywania, integralności i poufności (art. 5 ust. 1), a jednocześnie uniknięcie niebezpieczeństwa domniemywania kompetencji organów.

Szczególna rola administratora

Ustalenie ról w procesie przetwarzania danych osobowych ma kluczowe znaczenie z punktu widzenia odpowiedzialności za realizację praw i obowiązków wynikających z przepisów RODO. Szczególna rola w tym zakresie przypada zaś administratorowi. To on bowiem jest adresatem licznych obowiązków w zakresie ochrony danych osobowych.
Odpowiada m.in. za:

- zgodność przetwarzania danych osobowych z określonymi w RODO zasadami,
- realizację praw osób, których dane dotyczą (wskazanych w art. 13 i 14 oraz 15–22 RODO),
- bezpieczeństwo danych osobowych,
- zgłaszanie naruszeń ochrony danych osobowych i – gdy to uzasadnione – kontaktowanie się w tej sprawie z osobami, których dane dotyczą,
- zgodne z prawem przetwarzanie danych osobowych, które prowadzi samodzielnie, lub które prowadzone jest w jego imieniu (motyw 74 RODO).

Przepisy powinny więc być skonstruowane tak, by wyznaczały administratorowi cele i sposoby przetwarzania danych niezbędne dla realizacji celów regulacji, a jednocześnie umożliwiały mu sprawowanie faktycznej kontroli nad przetwarzaniem danych osobowych.

2 UODO SYGNALIZUJE

Właściwe wyznaczenie praw i obowiązków z zakresu przetwarzania danych osobowych dla konkretnych potrzeb regulacji ma podstawowe znaczenie w przypadku podmiotów publicznych czy wykonujących zadania publiczne, zakresu kompetencji, których nie można domniemywać. Istotna jest także zupełność, kompletność regulacji w całym procesie przetwarzania danych – od ich pozyskania po zaprzestanie przetwarzania (w tym ich usunięcie). Niedopuszczalne jest uzupełnianie nieistniejących czy niedoskonałych przepisów rangi ustawy przepisami rangi rozporządzenia, a tym bardziej pozostawianie tych kwestii do uregulowania w formie porozumień. To w ustawie powinny być przewidziane wszelkie istotne aspekty procesów przetwarzania danych osobowych, a rozporządzenie może jedynie określać sposób wykonania przepisów ustawowych.

Dobre przykłady istnieją

W polskim ustawodawstwie istnieją akty prawne precyzyjnie opisujące role w procesie przetwarzania danych przy pomocy systemu teleinformatycznego czy aplikacji. Dobrym przykładem tego typu klarownych rozwiązań są przepisy dotyczące ewidencji ludności czy dokumentów paszportowych, w których bardzo dokładnie określono wszystkie kwestie związane z używaniem wspólnego systemu informatycznego, m.in. takie jak zasilanie, przekazywanie danych prawidłowych czy zadbanie o bezpieczeństwo. Przyjmowanie tak skonstruowanych rozwiązań jest istotne dla ustalania odpowiedzialności za przetwarzane dane osobowe, m.in. tego, kto jest odpowiedzialny za zgłaszanie naruszeń, za nadawanie upoważnień itp.

Na każdym poziomie

Powyższe uwagi i zalecenia można również odnieść do projektowania i wdrażania rozwiązań informatycznych na poziomie poszczególnych firm i instytucji, co jest szczególnie istotne w dobie powszechnej ich cyfryzacji oraz świadczenia usług na odległość z wykorzystaniem narzędzi cyfrowych.

PLACÓWKI MEDYCZNE MOGĄ JUŻ PRZYSTĘPOWAĆ DO KODEKSU POSTĘPOWANIA

Każdy podmiot leczniczy należący do Federacji Porozumienie Zielonogórskie, który w swoich strukturach ma poradnię podstawowej opieki zdrowotnej (POZ) lub ambulatoryjnej opieki specjalistycznej (AOS), może przystąpić do „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych". Nie ma przy tym znaczenia wielkość placówki ani liczba obsługiwanych pacjentów.

O uruchomieniu zapisów poinformował na swojej stronie internetowej współautor kodeksu (tj. Jamano sp. z o.o.). Przystąpienie do stosowania kodeksu możliwe jest za pośrednictwem strony internetowej podmiotu monitorującego **www.kodeksrodo.pl**, na której zamieszczono dedykowany formularz zgłoszeniowy. Na tej stronie można również znaleźć treść kodeksu, a także informacje dotyczące zarówno samego przystąpienia do kodeksu, jak i procedury jego stosowania.
Organ nadzorczy zachęca podmioty lecznicze do przystępowania do stosowania kodeksu.
Kodeks, który jest właściwie przygotowany (m.in. nie jest jedynie powtórzeniem przepisów RODO, a przede wszystkim doprecyzowuje problemowe kwestie z uwzględnieniem specyfiki danej branży), administratorom i podmiotom przetwarzającym będącym jego członkami przynosi wiele korzyści:

- daje gwarancję pewności stosowania określonych rozwiązań zatwierdzonych przez organ nadzorczy,
- ułatwia dostosowanie się do wymogów przepisowych i wypełnianie wielu obowiązków, gdyż wskazuje właściwe rozwiązania, tam gdzie istnieją dylematy,
- zapewnia nadzór nad procesami przetwarzania danych osobowych przez niezależny podmiot monitorujący kodeks; oznacza to w praktyce, że np. kontrola podmiotu czy rozpatrywanie skarg osób, których dane dotyczą, mogą odbywać się bez udziału organu nadzorczego,
- jego stosowanie jest brane pod uwagę przy nakładaniu administracyjnej kary pieniężnej.

Stosowanie kodeksu jest korzystne również dla osób, których dane są przetwarzane, gdyż mogą one liczyć na zbliżony standard ochrony ich danych osobowych oraz realizacji wynikających z RODO praw przez daną branżę. Przypomnijmy, że organ nadzorczy zatwierdził „Kodeks postępowania dotyczący ochrony danych osobowych przetwarzanych w małych placówkach medycznych" 14 grudnia 2022 r., wydając stosowną decyzję administracyjną. Tego samego dnia udzielił on również akredytacji RS Jamano sp. z o.o. sp.k., do monitorowania jego przestrzegania przez podmioty, które do niego przystąpią (więcej informacji na ten temat można znaleźć na naszej **stronie internetowej** oraz w Newsletterze UODO dla IOD 1/2023).

BRANŻA HOTELARSKA PRACUJE NAD KODEKSEM POSTĘPOWANIA

Izba Gospodarcza Hotelarstwa Polskiego kontynuuje prace nad projektem kodeksu postępowania dla przedsiębiorców prowadzących działalność hotelarską. Stan ich zaawansowania wskazuje, że jeszcze w tym roku może rozpocząć się postępowanie o jego zatwierdzenie.

W odpowiedzi na prośbę Izby Gospodarczej Hotelarstwa Polskiego (IGHP) w siedzibie Urzędu Ochrony Danych Osobowych 21 lutego 2023 r. odbyło się spotkanie dotyczące projektu kodeksu postępowania dla branży hotelarskiej, nad którym pracuje IGHP.

Informacje o Izbie Gospodarczej Hotelarstwa Polskiego (IGHP)
Izba Gospodarcza Hotelarstwa Polskiego jest największą organizacją samorządu gospodarczego zrzeszającą podmioty prowadzące działalność w zakresie usług hotelarskich i gastronomicznych oraz podmioty prowadzące działalność na rzecz branży hotelarskiej i gastronomicznej na terytorium Rzeczypospolitej Polskiej.
Do zadań Izby należy m.in.:
- reprezentowanie interesów gospodarczych zrzeszonych w niej podmiotów w zakresie ich działalności gospodarczej, zwłaszcza wobec organów państwowych i samorządu terytorialnego oraz organów wymiaru sprawiedliwości,
- organizowanie pomocy w rozwiązywaniu problemów ekonomicznych, organizacyjnych i prawnych związanych z podejmowaniem i prowadzeniem przez członków Izby działalności gospodarczej w dziedzinie hotelarstwa i gastronomii,
- prowadzenie działalności promocyjnej na rzecz członków oraz pomoc w nawiązywaniu kontaktów z partnerami w kraju i za granicą.

IGHP jest reprezentantem polskiej branży hotelarskiej w HOTREC (Konfederacja Narodowych Organizacji Hoteli, Restauracji, Kawiarni w krajach UE i europejskiego obszaru ekonomicznego), a także w Hotelstars Union (HSU).
Więcej informacji o IGHP dostępnych jest na stronie: **www.ighp.pl**.

Szeroka inicjatywa

Przedstawiciele IGHP wskazali, że kontynuują prace nad projektem kodeksu postępowania, który miałby zastosowanie do przetwarzania danych osobowych przez przedsiębiorców prowadzących działalność hotelarską. Ma to być kodeks krajowy, a przystąpienie do niego nie będzie uzależnione od członkostwa w Izbie. Doprecyzowanie i ustandaryzowanie przetwarzania danych osobowych w branży hotelarskiej przyczyniłoby się do zapewnienia wyższego poziomu ochrony danych osobowych jej klientów, a dla członków kodeksu miałoby wymiar marketingowy.

Prowadzenie prac i ich zaawansowanie

Tematem wspólnych rozmów była również kwestia konsultacji projektu kodeksu postępowania przygotowanego przez Izbę, których przeprowadzenie jest elementem niezbędnym w procedurze zatwierdzania projektu kodeksu przez organ nadzorczy.

Odnosząc się do doświadczeń innych inicjatyw kodeksowych, przedstawiciel UODO wskazał na przykładowe możliwe do zastosowania rozwiązania wspierające przygotowanie projektu kodeksu, jak:

- utworzenie strony internetowej, za pośrednictwem której twórcy projektu kodeksu mogliby przeprowadzić jego konsultacje z właściwymi środowiskami, zwłaszcza z osobami, których dane dotyczą,
- umieszczenie informacji o takich konsultacjach na stronie internetowej UODO,
- udział przedstawicieli UODO w wydarzeniach promujących kodeks.

Osoby reprezentujące IGHP przedstawiły swoją propozycję polegającą na informowaniu klientów hoteli o możliwości wypowiedzenia się na temat projektu kodeksu przy okazji dokonywania rezerwacji (pobytu czy innych usług) albo meldowania się w hotelu. Spotkanie z inicjatywą pracującą nad kodeksem było również okazją do przypomnienia procedury zatwierdzania projektów kodeksów postępowania przez organ nadzorczy, która jest uregulowana w przepisach RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także w Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z RODO. Przedstawiciel UODO podkreślił, że bardzo ważne jest prawidłowe przeprowadzenie konsultacji dotyczących treści kodeksu i właściwe przedstawienie ich wyniku (o czym pisaliśmy m.in. w Newsletterze UODO dla IOD 11/2021). Zwracał też uwagę na konieczność zawarcia w kodeksie mechanizmów umożliwiających monitorowanie przestrzegania jego przepisów przez członków kodeksu. W projekcie kodeksu, który obejmuje czynności przetwarzania prowadzone przez podmioty prywatne, należy również wskazać podmiot monitorujący i określić mechanizmy umożliwiające mu wykonywanie jego działań zgodnie z art. 41 RODO. Stan zaawansowania prac nad projektem kodeksu postępowania IGHP wskazuje, że jeszcze w tym roku może rozpocząć się postępowanie o jego zatwierdzenie.

Urząd otwarty na spotkania

Spotkania przedstawicieli UODO z inicjatywami pracującymi nad kodeksami postępowania, mające na celu omówienie zasad i procedur związanych z tworzeniem tych dokumentów, to jeden ze sposobów realizacji przez organ nadzorczy zadania, jakim jest zachęcanie do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO. Wszystkie inne tego typu inicjatywy również mogą skorzystać z tej formy pomocy. Jednocześnie warto przypomnieć, że na stronie internetowej UODO dostępne są aktualne informacje zarówno o środowiskach pracujących **nad projektami** kodeksów postępowania, jak i o projektach kodeksów postępowania, które zostały **przedłożone organowi nadzorczemu** do zatwierdzenia.

3 WYBRANE DECYZJE UODO

PRAWIDŁOWE POINFORMOWANIE O PRZETWARZANIU DANYCH MA ZNACZENIE

Organ nadzorczy nakazał bankowi zaprzestania przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

Do Urzędu Ochrony Danych Osobowych wpłynęła skarga na nieprawidłowości w procesie przetwarzania danych osobowych przez jeden z banków, które polegały na przetwarzaniu danych osobowych skarżącego bez podstawy prawnej w związku z zobowiązaniami wynikającymi z umowy zawartej z bankiem, w tym na udostępnianiu ich na rzecz Biura.

Skarżący wskazał, że mimo ustania jego relacji z bankiem po całkowitej spłacie zobowiązania, bank nadal przetwarza jego dane osobowe bez podstawy prawnej oraz udostępnia je w zewnętrznej bazie instytucji utworzonej na podstawie prawa bankowego, na co skarżący swoją zgodę wycofał. W związku z tym, skarżący wniósł o usunięcie jego danych osobowych przetwarzanych przez bank w bazie tej instytucji. W trakcie prowadzonego postępowania instytucja wskazała, że przetwarza dane osobowe skarżącego w zakresie danych przekazanych przez bank – dotyczyły umowy.
Jak zaznaczono, przetwarza dane osobowe dotyczące zobowiązań wynikających z umów, w tym historii ich spłaty w celu oceny zdolności kredytowej i analizy ryzyka kredytowego na podstawie art. 105a ust. 3 Prawa bankowego, ze względu na przekazanie przez bank do biura informacji o spełnieniu warunków, o których mowa w tym przepisie dających podstawę do przetwarzania danych bez zgody skarżącego. Co do zasady, podstawą prawną przetwarzania danych osobowych klientów przez bank w instytucji utworzonej na podstawie prawa bankowego może być art. 6 ust. 1 f RODO, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Wskazania wymaga, że przetwarzanie danych osobowych odbywa się w oparciu o umowę zawartą pomiędzy bankiem i tą instytucją.

3 WYBRANE DECYZJE UODO

Przetwarzanie danych bez zgody osoby, której dane dotyczą

Art. 105 ust. 4 Prawa bankowego stanowi, że banki mogą, wspólnie z bankowymi izbami gospodarczymi, utworzyć instytucje upoważnione do gromadzenia, przetwarzania i udostępniania bankom informacji stanowiących tajemnicę bankową. Zakres przetwarzanych danych przez tę instytucję dotyczy sytuacji związanych z wykonywaniem czynności bankowych innym instytucjom, które m.in. są upoważnione do udzielania kredytów, pożyczek pieniężnych, gwarancji bankowych i poręczeń. Co równie ważne, dotyczy to także oceny zdolności kredytowej konsumenta czy analizy ryzyka kredytowego. Ponadto także istotne jest, że na podstawie prawa bankowego mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank o zamiarze przetwarzania dotyczących jej tych informacji, bez jej zgody.

Bieg terminu

Jak wynika ze zgromadzonego materiału dowodowego, skarżący dopuścił się zwłoki w spłacie zadłużenia trwającej dłużej niż 60 dni. Istotnym jednakże jest to, że bank nie poinformował go skutecznie o zamiarze przetwarzania dotyczących go informacji stanowiących tajemnicę bankową, bez jego zgody po wygaśnięciu zobowiązań wynikających z przedmiotowych umów. Sam fakt, iż skarżący nie wykonał zobowiązania lub spóźnił się z jego wykonaniem co najmniej 60 dni, nie upoważnia Banku do przetwarzania jego danych na warunkach określonych w art. 105a ust. 3 Prawa bankowego.

Jak liczyć terminy?
Moment, od którego należy liczyć 60-dniowy termin, w którym osoba, której informacje dotyczą dopuszcza się zwłoki w wykonaniu zobowiązania, to termin wykonania zobowiązania. Dopiero po upływie 60 dni zaczyna biec termin 30 dni.

Termin 30 dni biegnie od momentu, w którym osoba, której informacje dotyczą zostanie skutecznie poinformowana przez instytucję o zamiarze przetwarzania danych po wygaśnięciu zobowiązania. Ostatecznie to bezskuteczny upływ 30 dni od momentu poinformowania stanowi wypełnienie przesłanek z art. 105a ust. 3 Prawa bankowego.

3 WYBRANE DECYZJE UODO

Prawidłowe poinformowanie

Bank, przetwarzając dane klienta na podstawie art. 105a, musi wykazać, że osoba ta została poinformowana o zamiarze przetwarzania jego danych bez jego zgody. Samo sporządzenie i wysłanie takiego pisma zwykłym listem, nie jest równoznaczne z udowodnieniem ich prawidłowego doręczenia, skutkującego poinformowaniem klienta o zamiarze przetwarzania danych stanowiących tajemnicę bankową, bez jego zgody na podstawie art. 105a ust. 3 Prawa bankowego.
Badając sprawę, Prezes UODO nie stwierdził okoliczności uprawniających bank do przetwarzania danych osobowych skarżącego w oparciu o art. 105a ust 3 Prawa bankowego, który umożliwia bankowi przetwarzanie informacji stanowiących tajemnicę bankową dotyczącą osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy bez ich zgody w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Dlatego korzystając z przysługujących mu uprawnień, nakazał bankowi zaprzestania przetwarzania danych osobowych w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

art. 105a ust. 3

Banki, instytucje oraz podmioty, o których mowa w ust. 1, mogą przetwarzać informacje stanowiące tajemnicę bankową i informacje udostępnione przez instytucje pożyczkowe oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, dotyczące osób fizycznych po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem, inną instytucją ustawowo upoważnioną do udzielania kredytów, instytucją pożyczkową lub podmiotem, o którym mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem, inną instytucją ustawowo upoważnioną do udzielania kredytów, instytucją pożyczkową lub podmiotem, o którym mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, a po zaistnieniu tych okoliczności upłynęło co najmniej 30 dni od poinformowania tej osoby przez bank, inną instytucję ustawowo upoważnioną do udzielania kredytów, instytucję pożyczkową albo podmiot, o którym mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, o zamiarze przetwarzania dotyczących jej tych informacji, bez jej zgody.

4 NARUSZENIA I KONTROLE

JUŻ DZIAŁA ZMODERNIZOWANY SYSTEM SIS

W ramach pakietu reform Systemu Informacyjnego Schengen (SIS Recast) 7 marca 2023 r. zaczęły obowiązywać zmienione unijne rozporządzenia regulujące sposób funkcjonowania Systemu Informacyjnego Schengen (SIS)*. To największy system wymiany informacji w zakresie bezpieczeństwa wewnętrznego i zarządzania granicami w Europie.

SIS dostarcza informacji na temat osób poszukiwanych lub zaginionych, obywateli państw trzecich nieposiadających prawa do pobytu w Unii Europejskiej oraz zagubionych lub skradzionych przedmiotów (np. samochodów, broni palnej, łodzi i dokumentów tożsamości).

Zmodernizowany SIS jest podstawą będącego w trakcie przygotowywania najbardziej zaawansowanego systemu zarządzania granicami na świecie. Wraz z systemem wjazdu/wyjazdu (EES) oraz europejskim systemem informacji o podróży oraz zezwoleń na podróż(ETIAS), SIS będzie częścią architektury interoperacyjności.

Nowości w systemie SIS

Nowy SIS wzbogacano o nowe kategorie wpisów, dane biometryczne, takie jak odciski dłoni, ślady palców i zapisy DNA w przypadku osób zaginionych, oraz dodatkowe narzędzia do walki z przestępczością i terroryzmem. Dokonanie modernizacji ma niebagatelne znaczenie, ponieważ umożliwi również dokonywanie wpisów prewencyjnych w celu ochrony osób szczególnie zagrożonych i powstrzymania nielegalnej migracji. Celem tych zmian jest zapewnienie organom krajowym bardziej kompletnych i wiarygodnych informacji w celu zwiększenia bezpieczeństwa i zarządzania granicami w Europie. W związku z dokonanymi zmianami System Informacyjny Schengen został objęty zakresem kompetencji Komitetu Skoordynowanego Nadzoru. Komitet zrzesza krajowe organy ochrony danych, w tym polski organ oraz Europejskiego Inspektora Ochrony Danych (EIOD) w celu zapewnienia skoordynowanego nadzoru nad wielkoskalowymi systemami informatycznymi oraz nad organami

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich;

i jednostkami organizacyjnymi Unii Europejskiej, zgodnie z art. 62 rozporządzenia (UE) 2018/1725** lub – jak w przypadku SIS – z aktem prawnym UE ustanawiającym wielkoskalowy system informatyczny lub unijny organ, urząd lub agencję***. Skoordynowany nadzór nad systemami UE niesie za sobą wiele wyzwań. Należy upewnić się, że działania monitorujące są odpowiednie i skuteczne, w szczególności w obszarze, w którym przetwarzanie danych ma ogromny wpływ na prawa osób fizycznych. Dzięki nowym ramom prawnym SIS został wzbogacony o nowe funkcje i szersze cele przetwarzania danych, które będą wymagały dodatkowego monitorowania i kontroli na szczeblu krajowym, w szczególności w odniesieniu do wpisów, czy zostały dokonane zgodnie z prawem, jakości danych oraz dostępu do danych i ich wykorzystywania przez organy korzystające z SIS. Należy podkreślić, że osoby, których dane dotyczą, częściej korzystają ze swoich praw w ramach SIS niż w innych systemach.

Nowe rodzaje wpisów do SIS objęte nadzorem

Mając na uwadze powyższe, Komitet Skoordynowanego Nadzoru uwzględnił w swoim programie prac na lata 2022–2024 działania nadzorcze dotyczące nowego rodzaju wpisu do SIS. W poprzednich latach Komitet przeprowadził skoordynowane inspekcje wpisów dotyczących kontroli niejawnych i szczególnych zgodnie z art. 36 decyzji w sprawie SIS II oraz opublikował zaktualizowany przewodnik dotyczący wykonywania praw osób, których dane dotyczą. Ponadto Komitet przeprowadzi wspólne działanie nadzorcze nad nowymi wpisami, które dotyczyć będą również Europolu. Ten rodzaj wpisów budzi pewne obawy i dlatego od początku Komitet postanowił śledzić jego praktyczne wdrożenie. Podejście horyzontalne Komitetu pozwoli uzyskać kompleksowy przegląd całego przetwarzania danych przez systemy Unii Europejskiej, a tym samym umożliwi lepsze monitorowanie przepływów danych między systemami i wzmocni nadzór nad tą złożoną strukturą. Jest to dość ważne, zwłaszcza w przypadku osiągnięcia interoperacyjności sześciu wielkoskalowych systemów informatycznych (System Informacyjny Schengen (SIS), System Wjazdu/Wyjazdu (EES), System informacji o podróży oraz zezwoleń na podróż (ETIAS), scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN), Wizowy System Informacyjny (VIS) i system Eurodac do porównywania odcisków palców). Jednocześnie Komitet umożliwia większą synergię i wzmocnioną współpracę między organami ochrony danych, w tym na szczeblu krajowym i europejskim, którą zamierza w pełni zbadać. W tym celu będzie opierać się na doświadczeniu, korzystać z metod pracy i skupiać się na kluczowych kwestiach.

** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE

*** Art. 57 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006

5 NOWE TECHNOLOGIE

DEEPFAKE. CZY WIESZ, JAK NIE DAĆ SIĘ OSZUKAĆ, OGLĄDAJĄC ZDJĘCIA LUB FILMY WIDEO?

Rozwiązania takie jak sztuczna inteligencja, uczenie maszynowe, czy Internet rzeczy rozwijają się w szybkim tempie i mają bardzo duży wpływ na naszą codzienność. Mogą one również nieść ze sobą pewne zagrożenia dla ochrony danych i prywatności, z którymi będziemy musieli coraz częściej mierzyć się w przyszłości, zarówno w pracy, jak i w życiu osobistym. Jednym ze zjawisk, które wymaga szczególnej uwagi jest technologia deepfake.

Coraz częściej z możliwości sztucznej inteligencji korzystają również cyberprzestępcy w celu zwiększenia skuteczności kampanii socjotechnicznych, manipulowania informacjami, szerzenia dezinformacji, czy szantażowania. Niestety, w świecie zdominowanym przez Internet i media społecznościowe musimy nieustannie radzić sobie z natłokiem informacji. Coraz trudniej jest nam je filtrować, poddając źródła analizie i weryfikacji w celu odróżnienia wartościowych i rzetelnych treści od fake newsów, które celowo wprowadzają odbiorcę w błąd. Jednym z najnowszych osiągnięć przyczyniających się do tego problemu jest deepfake, czyli zmanipulowany obraz lub nagranie video, powstające przy wykorzystaniu sztucznej inteligencji (SI).

Technologia deepfake, czyli co?

Pojęcie deepfake to połączenie dwóch słów: deep – skrót od głębokiego uczenia (ang. deep learning), oraz fake, czyli fałszywy. Inną formą oszustwa jest technologia deepfake audio, która korzystając z próbki głosu może go sklonować, odwzorowując tonację, akcent, czy inne unikalne cechy. Może ona stanowić jeszcze większe zagrożenie, ponieważ ludzie często komunikują się werbalnie, np. telefonicznie, czy za pomocą nagrań głosowych, co znacznie rozszerza możliwości wykorzystania przez cyberprzestępców technologii deepfake.
Rozwój zaawansowanych głębokich sieci neuronowych i dostępność dużej ilości danych (np. w postaci obrazu i wideo udostępnionych w Internecie) sprawiły, że sfałszowane obrazy i filmy są prawie nie do odróżnienia, co stwarza nie tylko zagrożenia społeczne, czy prawne, ale przede wszystkim cybernetyczne, takie jak wymuszenia, oszustwa, czy kradzież tożsamości, która może przybierać różne formy, np. użycie głosu ofiary.

Warto zapamiętać!
Cyberprzestępca podszywając się pod kogoś znanego lub zaufanego może uzyskać dostęp do poufnych informacji, takich jak dane osobowe (często również wrażliwe), hasła, czy numery kart kredytowych. Istnieją jednak sposoby, które mogą pomóc w ustaleniu, czy nagranie jest prawdziwe. Warto zwrócić uwagę na mimikę twarzy, ruch gałek ocznych, brak emocji podczas wypowiedzi, czy nienaturalny ruch ciała. Istnieją również narzędzia, które w sposób automatyczny potrafią wykryć nieprawidłowości.

5 NOWE TECHNOLOGIE

Czy Europa poradzi sobie z dezinformacją?

Walka z dezinformacją to wspólny wysiłek wszystkich instytucji europejskich, dlatego UE współpracuje z platformami internetowymi, aby zachęcić je do usuwania nieprawdziwych treści oraz promowania wyłącznie wiarygodnych źródeł. Ponadto w 2018 roku został ogłoszony plan działania przeciwko dezinformacji, w którym określono kluczowe działania, mające stanowić odpowiedź na ten problem.*

Systemy deepfake podlegają szczególnym obowiązkom w zakresie przejrzystości określonym w art. 52 ust. 3 projektowanego aktu o sztucznej inteligencji: „Użytkownicy systemu sztucznej inteligencji, który generuje obrazy, treści dźwiękowe lub treści wideo, które łudząco przypominają istniejące osoby, obiekty, miejsca lub inne podmioty lub zdarzenia, lub który tymi obrazami i treściami manipuluje, przez co osoba będąca ich odbiorcą mogłaby niesłusznie uznać je za autentyczne lub prawdziwe („deepfake"), ujawniają, że dane treści zostały wygenerowane lub zmanipulowane przez system sztucznej inteligencji". **

Przepis ten pozwoli na dokonywanie świadomych wyborów lub na wycofanie się z danej sytuacji i ma na celu ochronę osób fizycznych przed ryzykiem podszywania się pod inne osoby lub wprowadzenia w błąd, gdy system sztucznej inteligencji generuje lub manipuluje treściami graficznymi, dźwiękowymi lub wideo. Ponadto Komitet Rady Europy do spraw Sztucznej Inteligencji na początku lutego 2023 roku opublikował „zerowy" projekt Konwencji w sprawie sztucznej Inteligencji, praw człowieka, demokracji i praworządności, który ma na celu zapewnić odpowiedni stopień ochrony praw człowieka w dobie dynamicznego rozwoju nowych technologii opartych o systemy sztucznej inteligencji. Jesteśmy jeszcze na początku rozwoju technologii deepfake i często jesteśmy w stanie odróżnić autentyczne nagranie od zmanipulowanego, ale nie zawsze tak będzie. Wraz z rozwojem tej technologii może stać się nie do odróżnienia i dostępna bardziej niż kiedykolwiek, dlatego niezwykle istotne jest stałe podnoszenie świadomości społeczeństwa na temat zagrożeń związanych z dezinformacją.

* https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52018JC0036&from=nl
** https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52021PC0206

6 SPRAWY MIĘDZYNARODOWE

WĘGRY: PRZETWARZANIE DANYCH OSOBOWYCH NA STRONACH INTERNETOWYCH TYLKO W ZGODZIE Z RODO

Węgierski organ nadzorczy nałożył na TV2 Média Csoport Zrt. administracyjną karę pieniężną w forintach węgierskich w wysokości równej ok. 25 tys. euro. Powodem decyzji było stwierdzenie, że firma niezgodne z prawem zarządzała zgodami na pliki cookies na swoich stronach internetowych.

Administrator – TV2 Média Csoport Zrt., prowadzący strony internetowe „tenyek.hu" i „tv2play.hu" udostępniał na nich publicznie własne treści medialne, w tym reklamy. Mimo że administrator ten zawierał umowy z osobami trzecimi na obsługę stron i materiałów promocyjnych, reklamy wybierał na podstawie własnej wyłącznej decyzji, co oznacza, że był administratorem w odniesieniu do wszystkich funkcji stron internetowych.

Na podstawie pkt 102 wyroku TSUE w sprawie C-40/17 osoba sprawująca decydującą kontrolę nad stronami internetowymi jest odpowiedzialna za wszystkie informacje, które należy przekazać osobom, których dane dotyczą, nawet jeśli informacje te odnoszą się do przetwarzania danych osobowych, gromadzonych w późniejszym czasie przez osobę trzecią.

Zgodność stosowania systemu zarządzania zgodami na pliki cookies z wymogami RODO stanowiła główny przedmiot postępowania prowadzonego przed wegierskim organem nadzorczym. Ustalono, że strony internetowe wykorzystują ten sam system zarządzania treścią CMS, a po wypełnieniu jednego formularza CMS pojawia się następny, co może wprowadzać w błąd. Ponadto drugi z wykorzystywanych formularzy – po zapytaniu o zgodę – nie przyjmował „nie" za odpowiedź, mimo że wyraźnie kierował prośbę o wyrażenie zgody.

Ponieważ pliki cookies mogą być wykorzystywane do indywidualnego śledzenia i profilowania, informacja o nich dla osób, których dane dotyczą, była niewystarczająca i trudno dostępna ze względu na wadliwie skonstruowany interfejs użytkownika. W trakcie kilkumiesięcznego postępowania administrator oświadczył, że rozwiąże zidentyfikowane problemy z CMS, jednak wprowadził jedynie niewielkie zmiany, które nie miały wpływu na meritum sprawy.

Węgierski organ nadzorczy stwierdził w swojej decyzji, że administrator powinien kontynuować przetwarzanie danych na stronach internetowych tylko wtedy, gdy przetwarzanie to będzie zgodne z wymaganiami RODO.

Administrator wszczął postępowanie sądowe przeciwko tej decyzji.

Źródło: **decyzja organu nadzorczego**

FINLANDIA: KARA DLA ADMINISTRATORA, KTÓRY NIE WYKONAŁ NAKAZU ORGANU NADZORCZEGO

Fiński organ nadzorczy nałożył na Suomen Asiakastieto Oy administracyjną karę pieniężną w wysokości 440 tys. euro. Podstawą nałożenia kary było to, że administrator nie usunął nieprawidłowych wpisów o zaległościach w płatnościach z powodu nieodpowiednich praktyk zapisanych w rejestrze informacji kredytowych. Organ wskazał, że wpis o zaległościach w płatnościach ma istotny wpływ na prawa i wolności osoby fizycznej.

W 2021 roku fiński organ nadzorczy badał przetwarzanie przez Suomen Asiakastieto Oy informacji o zaległościach w płatnościach opartych na prawomocnych orzeczeniach. Stwierdzono wówczas, że informacje oparte na orzeczeniach wydanych w sprawach cywilnych były błędnie przechowywane jako wpisy dotyczące zaległości w płatnościach.

Fiński organ nakazał administratorowi dostosowanie praktyk w zakresie rejestrowania wpisów dotyczących zaległości w płatnościach opartych na prawomocnych orzeczeniach. Zobligował go również do usunięcia wszystkich nieprawidłowych wpisów odnoszących się do zaległości w płatnościach, które były wynikiem takich działań. Administrator nie odwołał się od tej decyzji. Ostatecznie sprawę zakończyła decyzja o nałożeniu administracyjnej kary pieniężnej w wysokości 440 tys. euro.

Źródło: **decyzja organu nadzorczego**

7 EDUKACJA

WSKAZÓWKI DLA PROJEKTANTÓW GIER. JAK PRZESTRZEGAĆ „KODEKSU DLA DZIECI"

„Kodeks dla dzieci" przyjęty przez brytyjski organ nadzorczy (ICO) określa, w jaki sposób usługi online, z których mogą korzystać dzieci, powinny chronić je w cyfrowym świecie.

ICO przeprowadził audyt firm zajmujących się projektowaniem gier, aby lepiej zrozumieć, w jaki sposób „Kodeks dla dzieci" ma zastosowanie w sektorze gier i – co ważne – jakie kroki mogą podjąć firmy zajmujące się grami, aby upewnić się, że działają w zgodzie z kodeksem. Oto najważniejsze wskazówki:

1. Wyszukuj zagrożenia.

Dokonaj oceny ryzyka. Ustal proces, który pomoże zidentyfikować i zminimalizować ryzyko związane z ochroną danych w grach, tak by chronić prawa i wolności dzieci.

2. Wzmocnij gwarancję wieku.

Poznaj wiek swoich graczy. Przedział wiekowy Twoich graczy oraz różne potrzeby dzieci w różnym wieku i na różnych etapach rozwoju powinny leżeć u podstaw projektowania gier i stosowania kodeksu postępowania.

3. Dbaj o przejrzystość.

Niedopracowany projekt informacji o prywatności nie przestrzega odpowiednio przed zagrożeniami i wzmaga nieufność między dziećmi, rodzicami i dostawcami gier.

4. Zapobiegaj szkodliwemu wykorzystaniu danych dzieci.

Przetwarzaj dane osobowe dzieci wyłącznie w sposób, który nie jest szkodliwy dla ich zdrowia lub dobrego samopoczucia.

5. Domyślnie ustawiaj wysoki poziom prywatności i kontroli rodzicielskiej.

Należy projektować gry w taki sposób, aby promować interakcje rodzica lub opiekuna z dzieckiem przy jednoczesnym domyślnym ustawieniu wysokiego poziomu prywatności i zapewnieniu szeregu odpowiednich kontroli rodzicielskich.

6. Scouting, czyli profiluj odpowiedzialnie.

Daj dzieciom kontrolę nad ich danymi. Informuj zarówno o tym, czy wykorzystujesz ich dane osobowe, jak i o tym, jak je wykorzystujesz. Jest to szczególnie ważne, gdy profilowanie nie jest niezbędne do gry.

7. Zapobiegaj FOMO.

FOMO to skrót od ang. fear of missing out i oznacza strach przed tym, co nas omija.
Podczas projektowania gier nie wykorzystuj technik nakłaniania dzieci do podejmowania niekorzystnych decyzji dotyczących ich prywatności.

Szczegółowy opis wskazówek

8 WSPÓŁPRACA Z UODO

URZĄD OCHRONY DANYCH OSOBOWYCH I KRAJOWA IZBA RADCÓW PRAWNYCH Z POROZUMIENIEM O WSPÓŁPRACY

Porozumienie o współpracy zawarto 5 kwietnia 2023 roku. Obie instytucje będą się wspierać w działaniach na rzecz promowania i ochrony ważnych dla siebie wartości, a także uczestniczyć razem w projektach oraz podejmować wspólne inicjatywy.

– Mam dużą satysfakcję w związku z tym, że zacieśniamy i formalizujemy współpracę pomiędzy Krajową Izbą Radców Prawnych a Urzędem Ochrony Danych Osobowych. Jest ona niezwykle ważna w kontekście wyzwań, jakie stawia zarówno profesjonalnym pełnomocnikom, jak i obywatelom rzeczywistość społeczno-gospodarcza i prawna w ostatnich latach. Ochrona danych osobowych jest od wielu lat zagadnieniem obecnym w programie szkolenia i doskonalenia radców prawnych, dlatego jesteśmy odpowiednio przygotowani do zabezpieczenia interesów naszych klientów w tym zakresie. Niestety świadomość obywateli w obszarze ochrony danych osobowych jest ciągle niewystarczająca, a zagrożenia, choćby w obszarze nowych technologii, rosną. Dlatego odpowiedzialnością nas - ekspertów - jest prowadzenie skutecznej edukacji prawnej, także wokół zagadnienia danych osobowych. Taka edukacja z pewnością będzie lepsza, szersza, bardziej efektywna, jeśli będziemy ją realizować z tak istotnym partnerem jak UODO. Z drugiej strony jako bardzo obiecującą widzę współpracę pomiędzy naszymi instytucjami w wypracowaniu nowoczesnych, spójnych rozwiązań legislacyjnych dotyczących ochrony danych osobowych w obszarach związanych z wykonywaniem przez radców prawnych zawodu oraz funkcjonowaniem samorządu. Tego typu przepisów brakuje i mam głęboką nadzieję, że wspólnie opracujemy tu użyteczne regulacje. Jestem przekonany, że przed nami nie miesiące, a lata dobrej współpracy i działania na rzecz ochrony praw obywatelek i obywateli naszego państwa – powiedział Włodzimierz Chróścik, Prezes Krajowej Rady Radców Prawnych.

Czym jest i czym zajmuje się samorząd radców prawnych?

Samorząd radców prawnych to samorząd zawodowy. Stanowi wspólnotę radców prawnych wykonujących zawód zaufania publicznego. Podstawowym zadaniem samorządu zawodowego jest tworzenie warunków do wykonywania zawodu i sprawowanie nadzoru nad jego wykonywaniem w zakresie obywateli – odbiorców pomocy prawnej oraz w interesie publicznym. Samorząd prowadzi szkolenie zawodowe kandydatów do zawodu (aplikantów radcowskich), a także doskonalenie zawodowe radców prawnych. Dzięki temu radcowie prawni uzyskują uprawnienia i ciągle doskonalą swoje kompetencje zawodowe, by zapewnić wysoki poziom świadczonej pomocy prawnej.

Jak jest zorganizowany samorząd radców prawnych?

Jednostkami organizacyjnymi samorządu są okręgowe izby radców prawnych i Krajowa Izba Radców Prawnych (KIRP).

8 WSPÓŁPRACA Z UODO

W Polsce funkcjonuje 19 okręgowych izb radców prawnych: w Białymstoku, Bydgoszczy, Gdańsku, Katowicach, Kielcach, Koszalinie, Krakowie, Lublinie, Łodzi, Olsztynie, Opolu, Poznaniu, Rzeszowie, Szczecinie, Toruniu, Wałbrzychu, Warszawie, Wrocławiu, Zielonej Górze.
KIRP jest zrzeszona m.in. w radzie Adwokatur i Stowarzyszeń Prawniczych Europy (CCBE) oraz w Międzynarodowym Stowarzyszeniu Prawników (IBA). Działalnością KIRP kieruje Krajowa Rada Radców Prawnych, zaś organem wykonawczym Rady jest Prezydium (Prezes, Wiceprezesi, Sekretarz, Skarbnik i członkowie). Na czele Rady stoi Prezes. Samorząd liczy ponad 50 000 radców prawnych, ponad 6400 aplikantów radcowskich i jest największym samorządem zawodów prawniczych w Polsce. Radcowie prawni to osoby aktywne zawodowo, stale pogłębiające swoją wiedzę i doskonalące umiejętności zawodowe, nowoczesne, aktywne społecznie, w tym w społecznościach lokalnych.

W czym może ci pomóc radca prawny?

Radca prawny ma pełen zakres uprawnień zawodowych, tzn. może pełnić rolę obrońcy w sprawach karnych lub innych o charakterze represyjnym, pełnomocnika procesowego w postępowaniach sądowych, zastępcy prawnego w postępowaniach i sprawach pozasądowych, konsultanta, negocjatora, legislatora, mediatora lub arbitra. Radca prawny udziela porad, konsultacji, sporządza dokumenty mające znaczenie prawne (np. opinie prawne, umowy, akty prawne, oświadczenia woli lub wiedzy), zapewnia zastępstwo procesowe lub prawne. Jeżeli poszukujesz dla siebie radcy prawnego w konkretnej sprawie, możesz skorzystać z udostępnianej przez KIRP wyszukiwarki www.szukajradcy.pl.

Fot. UODO.. od lewej: Włodzimierz Chróścik, Prezes Krajowej Rady Radców Prawnych i Jakub Groszkowski, Zastępca Prezesa UODO

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl