URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 01/01/24

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo!

Co roku, w styczniu z okazji Dnia Ochrony Danych Osobowych w całej Europie odbywają się liczne konferencje, warsztaty i inne spotkania towarzyszące temu wydarzeniu. Są one okazją do pogłębienia wiedzy na temat ochrony danych osobowych przez społeczeństwo oraz wymiany poglądów między osobami zawodowo zajmującymi się tym tematem. To wyjątkowo intensywny dla europejskich organów nadzorczych okres, w którym staramy się zaadresować realne problemy i potrzeby z korzyścią dla naszych wszystkich interesariuszy.

Dzień Ochrony Danych Osobowych (DODO) został ustanowiony na dzień 28 stycznia przez Komitet Ministrów Rady Europy. Obchodzony jest w rocznicę sporządzenia najstarszego aktu prawnego o zasięgu międzynarodowym, który reguluje zagadnienia związane z ochroną danych osobowych – Konwencji nr 108 RE o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych podpisanej w Strasburgu dn. 28 stycznia 1981 r.

Urząd Ochrony Danych Osobowych aktywnie uczestniczy w DODO od 2007 roku. W tym roku spotkania składające się na obchody 18. Edycji tego święta trwają od 8 stycznia do 12 lutego i koncentrują się przede wszystkim na zagadnieniach związanych ze stosowaniem RODO, w związku z intensywnym rozwojem technologicznym.

Tegoroczne obchody DODO organizowane przez Urząd Ochrony Danych Osobowych zainaugurowały warsztaty dla seniorów na temat tego, jak bezpiecznie korzystać ze zdobyczy nowych technologii podczas codziennych czynności. Za nami również warsztaty dla studentów dot. bezpieczeństwa w cyberprzestrzeni, podczas których eksperci UODO rozmawiali ze słuchaczami o aplikacjach mobilnych, a także szansach i zagrożeniach, jakie płyną z korzystania z nowoczesnych technologii.

Nie zapominając o najmłodszych – szkoły i placówki oświatowe, które uczestniczą w programie „Twoje dane – Twoja sprawa” podejmą w ramach naszego święta liczne aktywności, inicjujące dyskusję na temat kluczowej roli ochrony prywatności w cyfrowym świecie. Przygotowaliśmy nawet grę terenową współorganizowaną z warszawskimi harcerzami. Ponadto uczniowie szkół ponadpodstawowych wezmą udział w zajęciach online – #ODOlekcja pt. „Deepfake: fałszywa rzeczywistość w sieci – czy jesteś na to gotowy?”.

Wzorem lat ubiegłych do współorganizacji tego święta włączyły się szkoły wyższe, z którymi Prezes Urzędu zawarł porozumienia o współpracy. W uczelniach odbywają się spotkania i konferencje z udziałem specjalistów UODO. W tym roku są to między innymi cykl debat dotyczących ochrony danych osobowych w sektorze zdrowia w dobie rozwoju nowych technologii w Warszawskiej AEH, Konferencję Naukową na WPiA UMK w Toruniu czy X Dzień Otwarty UODO w Akademii WSB

dobrych praktyk w zakresie ochrony danych osobowych. Ważnym punktem obchodów naszego święta są konsultacje dla Inspektorów Ochrony Danych oraz porady prawne z zakresu ochrony danych, podczas których eksperci Urzędu podzielą się swoją wiedzą z odwiedzającymi siedzibę organu nadzorczego.

Dzień Ochrony Danych Osobowych został ustanowiony by uwrażliwić obywateli na ochronę danych oraz poinformować ich o przysługujących im prawach i dobrych praktykach. Cieszę się, że Urząd aktywnie wypełnia te cele. Po więcej szczegółów na temat aktywności związanych z obchodami 18. Dnia Ochrony Danych Osobowych zapraszam na **stronę Urzędu**.

.

Jakub Groszkowski

Zastępca Prezesa

Urzędu Ochrony Danych Osobowych

Drodzy Czytelnicy!

Styczniowe aktywności europejskich organów nadzorczych skupiają się wokół Dnia Ochrony Danych Osobowych. To święto, któremu zawsze w UODO poświęcamy wiele uwagi. Tegoroczne obchody upływają głównie pod znakiem zagadnień dotyczących stosowania RODO, w związku z rozwojem technologicznym. To kwestie, które w ostatnim czasie bardzo nas zajmowały, szczególnie że to właśnie do bezpieczeństwa naszych danych w sieci odnoszą się główne wyzwania, czekające ochronę danych w tym roku. O trendach i wyzwaniach w 2024 roku przeczytacie Państwo w kolejnej porcji opinii zaproszonych ekspertów.

Modele AI oparte na przetwarzaniu olbrzymiej ilości danych to domena, która wymaga szczególnej uwagi ze strony specjalistów od prywatności. Urząd Ochrony Danych Osobowych jest świadomy, że troska o dane obywateli w erze cyfrowej powinna odzwierciedlać najwyższe standardy i w tym zadaniu polski organ nadzorczy wspierany jest przez Departament Nowych Technologii. Więcej nt. jego aktywności i dlaczego jest tak potrzebny dla efektywnych działań Urzędu w dzisiejszym świecie dowiecie się z wywiadu z Natalią Misiuk, Dyrektor Departamentu Nowych Technologii UODO i Tomaszem Ochmińskim – jej zastępcą.

Kontakty SDN (Software Defined Network) – nowoczesnej generacji technologii telekomunikacyjnej -zamieszczone na karcie SIM mogą zostać uznane za prowadzenie marketingu bezpośredniego. Zdecydowana odmowa ponownego kontaktu telefonicznego stanowi sprzeciw na przetwarzanie danych osobowych w celach marketingowych. Takie rozstrzygnięcia przyjął Prezes UODO po rozpatrzeniu skargi na niezgodne z prawem przetwarzanie danych osobowych przez jednego z popularnych operatorów telefonii komórkowej. Polecam lekturę szczegółów tej decyzji.

W tym numerze nie zabraknie również orzeczeń innych europejskich regulatorów. Francuski organ nadzorczy przeprowadził postępowanie, w wyniku którego stwierdził, że Minister Transformacji i Służby Publicznej dopuścił do naruszenia ochrony danych. Polityk wykorzystał przechowywane w systemie do komunikacji z urzędnikami dane do wysłania im komunikatu o tematyce politycznej. Z kolei włoski organ nadzorczy nałożył administracyjną karę pieniężną w wysokości 18 tys. euro na firmę świadczącą usługi szkoleniowe dla lekarzy za publikację informacji dotyczących wrażliwych danych zmarłego.

Styczniowe wydanie „Biuletynu UODO" to ogromna dawka przydatnych i ciekawych informacji, a także mała zapowiedź tego, co czeka nas w tym roku. Życzę miłej lektury!

Adam Sanocki
Dyrektor Departamentu Komunikacji Społecznej,
Rzecznik Prasowy UODO

WAŻNE, BY REGULACJE NADĄŻAŁY ZA ROZWOJEM NOWYCH TECHNOLOGII

Z Natalią Misiuk, Dyrektorem Departamentu Nowych Technologii UODO oraz Tomaszem Ochmińskim, Zastępcą Dyrektora Departamentu Nowych Technologii UODO rozmawiał Karol Witowski, Zastępca Rzecznika Prasowego UODO

Czym zajmuje się Departament Nowych Technologii UODO (DNT)?

Natalia Misiuk: Jednym z istotnych tematów związanych z działalnością Departamentu Nowych Technologii UODO jest budowanie kultury ochrony danych osobowych w obszarze rozwoju technologicznego. Do jego innych zadań należy m.in. przygotowywanie opinii, również w ramach zespołów międzynarodowych, odnoszących się do przetwarzania danych osobowych w systemach informatycznych oraz dotyczących nowych rozwiązań technologicznych. Ponadto jesteśmy zaangażowani w działania edukacyjne i podnoszenie świadomości społecznej, co jest bardzo ważną częścią działalności Urzędu Ochrony Danych Osobowych. Bierzemy również czynny udział w organizacji konferencji, webinariów, debat i innych spotkań mających na celu podniesienie świadomości społeczeństwa na temat nowych technologii i ich wpływu na ochronę danych. Występujemy również jako prelegenci na tych wydarzeniach, prezentując aktualne trendy i zasady bezpieczeństwa. Stworzyliśmy wiele materiałów pokonferencyjnych, które stanowią doskonałe źródło niezbędnej wiedzy z zakresu nowych technologii w obszarze ochrony danych osobowych.

Czy DNT zajmuje się również zagadnieniami związanymi z cyberbezpieczeństwem ?

Tomasz Ochmiński: Jednym z zadań Departamentu Nowych Technologii UODO jest weryfikacja zabezpieczeń technicznych w różnych rozwiązaniach technologicznych – to nic innego jak zagadnienia związane z cyberbezpieczeństwem. Pamiętajmy jednak, że cyberbezpieczeństwo to bardzo rozległa dziedzina wiedzy, która obejmuje wiele warstw różnych rozwiązań technologicznych i ich zabezpieczeń. Warto przy tym wiedzieć, że cyberbezpieczeństwo jest zarówno szerokie, jak i głębokie. Dla uproszczenia możemy je podzielić na trzy główne obszary tj. corporate security, network security i application security. O tym podziale informowaliśmy również na wspólnym wystąpieniu z Panią Dyrektor Natalią Misiuk, podczas konferencji, która odbyła się 22 listopada 2023 roku w siedzibie Zakładu Ubezpieczeń Społecznych, a tematem były „Nowe technologie a ochrona

danych osobowych – konferencja UODO i ZUS". Gorąco zachęcam do zapoznania się z materiałem video, dostępnym na kanale Youtube ZUS. Ponadto prowadzimy szkolenia wewnętrzne dotyczące zagadnień z zakresu cyberbezpieczeństwa dla naszych pracowników, głównie osób zajmujących się zagadnieniami technicznymi, pracujących w Departamencie Kontroli i Naruszeń.

Technologie cyfrowe bazują na ogromnych zbiorach danych, sztuczna inteligencja nie byłaby w stanie generować żadnych odpowiedzi czy rozwiązań, gdyby nie dane. Jak w tym kontekście wygląda ochrona danych osobowych i innych danych wrażliwych?

Natalia Misiuk: Technologie cyfrowe rzeczywiście polegają na dużych zbiorach danych, które mogą zawierać dane osobowe, w tym również wrażliwe, dlatego ich ochrona jest kluczowa, co niestety wiąże się z wieloma wyzwaniami. Na szczęście ustawodawcy, zarówno krajowi jak i unijni, dążą do zapewnienia poczucia bezpieczeństwa i na bieżąco regulują najważniejsze kwestie. Istnieje więc wiele mechanizmów i praktyk, których celem jest zapewnienie prywatności i bezpieczeństwa danych w tym kontekście. Chociażby RODO, które nakłada ścisłe wymogi dotyczące gromadzenia, przechowywania i przetwarzania danych osobowych. Rosnąca liczba cyberzagrożeń podkreśla znaczenie skutecznych strategii bezpieczeństwa danych w każdej dziedzinie - od biznesu po korzystanie z aplikacji czy usług online. Istotne jest również, aby firmy i organizacje stosowały zasady minimalizacji danych, ograniczając zbieranie informacji do tego, co niezbędne do realizacji konkretnego celu. Ponadto na kwestie związane bezpośrednio ze sztuczną inteligencją zwraca uwagę projektowany akt o sztucznej inteligencji, który ma na celu uregulowanie jej zastosowań, wprowadzając zasady dotyczące transparentności, odpowiedzialności i bezpieczeństwa.

W jaki sposób generatywna sztuczna inteligencja, taka jak GPT-4, wpływa na kwestie ochrony danych osobowych, i jakie środki są podejmowane, aby zapewnić, że takie systemy nie naruszają prywatności użytkowników?

Generatywna sztuczna inteligencja przetwarza ogromne ilości danych, w tym potencjalnie dane osobowe, aby uczyć się i generować odpowiedzi. W kontekście ochrony danych osobowych, istnieje kilka kluczowych aspektów i środków zapobiegawczych, które powinny być podejmowane, w tym chociażby przestrzeganie obowiązujących przepisów o ochronie danych, takich jak RODO w Unii Europejskiej. Obejmuje to m.in. zapewnienie przejrzystości w zakresie tego, jakie dane są zbierane i w jakim celu, oraz uzyskanie zgody użytkowników tam, gdzie jest to wymagane. Mimo to, wciąż istnieją wyzwania związane z zapewnieniem pełnej ochrony danych osobowych w kontekście szybko rozwijającej się technologii generatywnej AI, co wymaga ciągłej uwagi i dostosowywania podejść zarówno od twórców technologii, jak i organów regulacyjnych. W tym miejscu warto przypomnieć, że Urząd Ochrony Danych Osobowych rozpatruje skargę dotyczącą ChatGPT, w której skarżący zarzuca twórcy tego narzędzia przetwarzanie danych w sposób niezgodny z prawem, nierzetelny z wykorzystaniem nieprzejrzystych zasad. Dlatego niezwykle ważne jest, aby rozwój tej technologii

odbywał się z poszanowaniem praw osób fizycznych wynikających m.in. z RODO, w tym ograniczał zbieranie i przetwarzanie danych do tego, co jest konieczne, oraz zapewniał przejrzystość i odpowiedzialność w działaniu systemów AI.

Czy w dobie powszechnego dostępu do mediów społecznościowych możliwe jest zapewnienie bezpieczeństwa danych osobowych?

Natalia Misiuk: Zapewnienie bezpieczeństwa danych osobowych w świecie powszechnego dostępu do mediów społecznościowych jest dużym wyzwaniem. Social media generują ogromne ilości danych, często zawierających wrażliwe informacje. Chociaż firmy działające w tym sektorze podejmują środki ochronne, takie jak ulepszanie polityk prywatności czy wprowadzanie zaawansowanych technologii zabezpieczających, użytkownicy również muszą mieć świadomość ryzyka i być odpowiedzialni za ochronę swoich danych, na przykład poprzez korzystanie z silnych haseł oraz zarządzanie ustawieniami bezpieczeństwa i prywatności na swoich kontach.

Bez wątpienia era mediów społecznościowych stwarza również szereg wyzwań dla organów ochrony danych. Należą do nich: monitorowanie i egzekwowanie przestrzegania RODO oraz reagowanie w sytuacji naruszenia przepisów tego aktu prawnego. Ponadto, organy te muszą stale monitorować ciągłe zmiany w technologii i sposobach wykorzystania danych przez platformy społecznościowe.

W kontekście mediów społecznościowych nie sposób nie wspomnieć o tzw. zwodniczych wzorcach projektowych w interfejsach platform mediów społecznościowych, które mogą skłaniać użytkowników do nieświadomego wyrażania zgody na zbieranie lub udostępnianie swoich danych osobowych. Są to praktyki, które mogą naruszać nie tylko przepisy RODO, ale również aktu o usługach cyfrowych (DSA), w którym przyjęto zakaz ich wykorzystywania do wprowadzania w błąd. Ponadto Europejska Rada Ochrony Danych (EROD) przyjęła Wytyczne 03/2022 zawierające zalecenia i wskazówki dla dostawców mediów społecznościowych dotyczące projektowania zwodniczych wzorców projektowych, które naruszają wymogi RODO.

Urząd Ochrony Danych Osobowych, zdając sobie sprawę z tego jak ważne jest podnoszenie poziomu świadomości w tym zakresie, organizuje szereg wydarzeń poświęconych zagadnieniom ochrony danych - również w kontekście mediów społecznościowych. Przykładowo w ramach 18. Dnia Ochrony Danych Osobowych odbyły się warsztaty dla studentów „Bezpieczna droga przez cyberprzestrzeń: od deepfake'ów po bezpieczeństwo aplikacji mobilnych", podczas których również poruszaliśmy istotę ochrony danych w mediach społecznościowych. Dostrzegając te wszystkie problemy UODO systematycznie opracowuje również specjalne wskazówki i porady związane z bezpiecznym użytkowaniem Internetu, w tym również w odniesieniu do kwestii udostępniania i ochrony danych osobowych w mediach społecznościowych oraz prawa do prywatności.

1 ROZMOWA Z EKSPERTEM

Czy RODO skutecznie chroni użytkowników przed social mediachmi czy sztuczną inteligencją w kontekście niebezpieczeństw związanych z udostępnianiem wizerunku i wykorzystaniem danych osobowych ?

Tomasz Ochmiński: RODO nakłada na podmioty przetwarzające dane osobowe szereg obowiązków, takich jak informowanie użytkowników o celach i sposobach przetwarzania, uzyskiwanie ich zgody, zapewnianie bezpieczeństwa i poufności danych, umożliwianie dostępu, sprostowania, usunięcia lub przeniesienia danych, a także respektowanie praw użytkowników do sprzeciwu, ograniczenia lub cofnięcia zgody. Sztuczna inteligencja, czyli zbiór technologii umożliwiających maszynom wykonywanie zadań takich jak generowanie i rozpoznawanie obrazów, mowy czy tekstu, uczenie się, wnioskowanie czy podejmowanie decyzji, jest coraz częściej stosowana w różnych dziedzinach życia, w tym w social mediach. Sztuczna inteligencja może przynosić wiele korzyści, takich jak poprawa jakości usług, personalizacja treści, optymalizacja procesów czy tworzenie nowych możliwości, jednak wiąże się także z wieloma wyzwaniami i zagrożeniami, takimi jak naruszenie prywatności, dyskryminacja, manipulacja, nadużycie, brak przejrzystości, odpowiedzialności czy kontroli.
W związku z tym, nie można jednoznacznie stwierdzić, że RODO skutecznie chroni użytkowników przed zagrożeniami jakie mogą wiązać się z korzystaniem z social mediów i sztuczną inteligencją, ponieważ to jakie informacje będą przetwarzane przez wymienione rozwiązania technologiczne w znacznej mierze zależy od samych użytkowników i informacji, które wprowadzają do poszczególnych serwisów społecznościowych. Pamiętajmy więc, że wszystkie systemy dostępne publicznie mogą w jakiś sposób zostać przełamane, a tym samym może dojść do wycieku przetwarzanych w nich danych. Dlatego bezpieczniej jest przyjąć założenie, że wszystko co wprowadzamy do takich systemów może zostać upublicznione, a co za tym idzie nie powinniśmy wprowadzać żadnych poufnych danych do tego typu rozwiązań technologicznych.

Jak wygląda kwestia bezpieczeństwa danych dotyczących aktywności fizycznej i zdrowia gromadzonych w licznych aplikacjach obsługujących urządzenia osobiste typu wearables?

Natalia Misiuk: Wearables to jedna z najbardziej popularnych i ogólnodostępnych kategorii urządzeń, które zaliczane są do koncepcji Internetu Rzeczy. Oferują szeroki wachlarz możliwości, które bez wątpienia mogą poprawić komfort naszego życie w wielu obszarach. Jednak wraz z rozwojem tej technologii pojawiają się zagrożenia związane z ochroną danych osobowych i prywatnością użytkowników, ponieważ ilość danych, które mogą gromadzić te urządzenia jest ogromna. Należy podkreślić, że często są to właśnie dane wrażliwe, które zgodnie z RODO podlegają szczególnej ochronie. Co to oznacza dla użytkowników? Na pewno potrzebę świadomego korzystania z tych urządzeń. Użytkownicy urządzeń wearables powinni zdawać sobie sprawę z tego jakie dane są zbierane przez ich urządzenia i jak są wykorzystywane oraz mieć kontrolę nad ich udostępnianiem. Z kolei dostawcy tego typu urządzeń powinni dostosować się do przepisów prawnych, przestrzegając przepisów RODO. Na temat tych urządzeń pisaliśmy w październikowym wydaniu **Biuletynu UODO**.

1 ROZMOWA Z EKSPERTEM

Jak powinniśmy dbać o swoje dane i powiązane z nimi informacje w erze cyfrowej?

Tomasz Ochmiński: Dbanie o swoje dane osobowe w erze cyfrowej jest niezwykle ważne dla ochrony naszej prywatności, bezpieczeństwa i praw. Oto kilka wskazówek:

- Nie udostępniajmy swoich danych osobowych lub informacji z nimi powiązanych nieznajomym, podejrzanym lub niezaufanym źródłom.
- Nie klikajmy w podejrzane linki, nie otwierajmy nieznanych załączników, nie pobierajmy niezweryfikowanych plików.
- Nie podawajmy swoich danych osobowych lub haseł na stronach internetowych, które nie są zabezpieczone protokołem HTTPS lub nie mają odpowiedniego certyfikatu TLS.
- Nie używajmy tego samego hasła do różnych kont lub usług.
- Nie logujmy się na swoje konta lub usługi na publicznych lub współdzielonych komputerach lub urządzeniach.
- Nie udostępniajmy swoich danych osobowych lub informacji z nimi powiązanych w social mediach lub innych publicznych platformach, chyba że jest to konieczne lub świadomie tego chcemy.

Istnieje wiele narzędzi, które mogą pomóc w ochronie danych osobowych i informacji z nimi powiązanych. Niektóre z nich to: antywirusy, zapory sieciowe, programy do szyfrowania danych, menedżery haseł, klucze sprzętowe stanowiące drugi składnik uwierzytelniania, VPN, adblockery, programy do usuwania plików cookies, programy do anonimizacji danych, programy do usuwania danych z dysków lub urządzeń.

W erze cyfrowej nieustannie pojawiają się nowe technologie, zagrożenia i wyzwania związane z ochroną danych osobowych i informacji z nimi powiązanych. Dlatego ważne jest, aby być na bieżąco z tymi kwestiami i stale podnosić swoją świadomość i wiedzę na ten temat. Można korzystać z różnych źródeł informacji, takich jak strony internetowe np. strona UODO, blogi, podcasty, książki, artykuły, webinaria (również te organizowane przez UODO), szkolenia, konferencje, warsztaty i inne.

Czy monitoring wizyjny, w dobie coraz doskonalszych systemów rozpoznawania twarzy jest bezpieczny i legalny? Jak można chronić w tym kontekście swoje dane, swój wizerunek?

Tomasz Ochmiński: Monitoring wizyjny to system, który pozwala na rejestrowanie i przekazywanie obrazu z określonych miejsc w celu nadzoru nad obszarem. Monitoring wizyjny może być stosowany zarówno przez podmioty publiczne, jak i prywatne, w różnych celach, takich jak zwiększenie ochrony mienia, majątku lub bezpieczeństwa. Jednak monitoring wizyjny wiąże się także z przetwarzaniem danych osobowych, takich jak wizerunek twarzy, które podlegają ochronie prawnej. Musi zatem spełniać pewne warunki, aby być zgodny z RODO. Monitoring wizyjny, zwłaszcza gdy wykorzystuje technologię rozpoznawania twarzy, może stanowić zagrożenie dla prywatności, wolności i godności osób, których dane dotyczą. Rozpoznawanie twarzy to automatyczne przetwarzanie obrazów cyfrowych zawierających twarze osób w celu identyfikacji lub weryfikacji tych osób za pomocą szablonów twarzy. Rozpoznawanie twarzy może być używane do różnych celów, np. do kontroli

dostępu, personalizacji usług, profilowania, śledzenia, identyfikowania podejrzanych itp. Jednak rozpoznawanie twarzy może także prowadzić do naruszenia praw człowieka, takich jak prawo do nienaruszalności życia prywatnego, prawo do własnego wizerunku, prawo do niedyskryminacji, prawo do wolności wyrażania opinii, prawo do wolności zgromadzeń itp. W związku z tym, można stwierdzić, że monitoring wizyjny, w dobie coraz doskonalszych systemów rozpoznawania twarzy, nie jest ani całkowicie bezpieczny, ani całkowicie legalny. Bezpieczeństwo i legalność monitoringu wizyjnego zależą od tego, jak i w jakim celu jest on stosowany, przez kogo i w jakim zakresie, oraz czy są przestrzegane zasady ochrony danych osobowych i praw człowieka. Aby chronić swoje dane, swój wizerunek i swoją prywatność w tym kontekście, osoby, których dane dotyczą, powinny:

- być świadome tego, gdzie i kiedy są monitorowane, przez kogo i w jakim celu, oraz jakie mają, w związku z tym, prawa;
- żądać informacji od podmiotów stosujących monitoring wizyjny o przetwarzaniu ich danych, celach, podstawach prawnych, prawach, sposobach kontaktu, czasie przechowywania danych itp.;
- wyrażać lub cofać zgodę na przetwarzanie swoich danych, jeśli jest to podstawą prawną monitoringu wizyjnego;
- korzystać ze swoich praw do dostępu, sprostowania, usunięcia, przeniesienia, ograniczenia, sprzeciwu itp. w stosunku do swoich danych;
- zgłaszać naruszenia ochrony danych osobowych lub praw człowieka do organów nadzorczych lub sądów, jeśli uważają, że monitoring wizyjny jest niezgodny z prawem lub narusza ich prawa.

Jakie zagrożenia czekają na nas w najbliższym czasie w obszarze rozwoju technologii?

Natalia Misiuk: Na pewno w najbliższej przyszłości możemy spodziewać się kilku kluczowych zagrożeń związanych z rozwojem technologii. Po pierwsze wzrost złożoności sztucznej inteligencji i uczenia maszynowego może prowadzić do trudności w zrozumieniu i kontrolowaniu sposobu, w jaki te systemy podejmują decyzje, co rodzi ryzyko nadużyć i błędnych interpretacji. Po drugie, rosnące zastosowanie Internetu Rzeczy (IoT), które również może nieść ze sobą zagrożenia dla bezpieczeństwa danych, ze względu na ogromną liczbę urządzeń połączonych z siecią i często niewystarczające zabezpieczenia. Kolejnym wyzwaniem jest rozwój technologii kwantowych, które mogą zmienić obecną równowagę w kryptografii i bezpieczeństwie informacji. Dodatkowo, rozszerzona rzeczywistość (AR) i wirtualna rzeczywistość (VR) mogą stwarzać nowe obszary do nadużyć prywatności, na przykład poprzez zbieranie bardzo szczegółowych danych o zachowaniach i preferencjach użytkowników. Ważnym zagrożeniem jest również rosnące ryzyko cyberataków, które mogą być coraz bardziej zaawansowane i trudniejsze do wykrycia. Wszystkie te aspekty wymagają ciągłej uwagi zarówno ze strony twórców technologii, jak i regulatorów, aby zapewnić bezpieczeństwo i prywatność w szybko zmieniającym się świecie cyfrowym. Nie zapominajmy jednak, że rozwój nowych technologii to nie tylko zagrożenia, ale również ogromne możliwości. Ważne jest jednak aby regulacje nadążały za rozwojem nowych technologii.

ZA REALIZACJĘ PRAW OSÓB W ZAKRESIE DOSTĘPU DO DOTYCZĄCYCH ICH DANYCH ODPOWIADA ADMINISTRATOR

Za określoną w RODO realizację praw osób, w tym prawa dostępu do danych, odpowiada administrator. To on zatem jest właściwy do podpisania informacji przygotowanej na podstawie art. 15 RODO.

Na mocy art. 15 RODO każda osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarza on jej dane osobowe, a jeżeli tak, to ma prawo uzyskania dostępu do nich i określonych w powołanym przepisie informacji, w tym o: celu przetwarzania, kategoriach przetwarzanych danych, o odbiorcach tych danych czy o okresie przechowywania danych. Zarówno art. 15, jak i art. 12 RODO, który mówi o zasadach informowania i trybie wykonywania praw osób, których dane dotyczą, stanowią, że zobowiązany do realizacji prawa dostępu do danych jest administrator.
Z kolei art. 38 ust. 4 RODO dotyczący statusu inspektora ochrony danych stanowi, że osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących (w tym prawa do informacji na podstawie art. 15 RODO). Art. 38 ust. 6 RODO stanowi zaś, że inspektor ochrony danych może wykonywać inne zadania i obowiązki, pod warunkiem zapewnienia przez administratora braku występowania konfliktu interesów.

Powołując się na powyższe regulacje inspektor ochrony danych (IOD) jednego z miast zwrócił się do UODO z prośbą o wyjaśnienie następujących wątpliwości:

- Czy inspektor ochrony danych jest uprawniony do podpisania zbiorowej informacji uzyskanej od jednostek organizacyjnych administratora (np. od wszystkich wydziałów urzędu obsługującego organ administracji publicznej), która została przygotowana na wniosek osoby, której dane dotyczą w sprawie udzielenia informacji o fakcie i okolicznościach przetwarzania danych osobowych tej osoby przez administratora (organ administracji publicznej)?
- Czy w takim przypadku nie wystąpi konflikt interesów?
- Czy w przypadku braku możliwości podpisania informacji przygotowanej na podstawie art. 15 RODO przez inspektora ochrony danych może on podpisać taką informację jako pełnomocnik administratora?

Zadania administratora

W odpowiedzi organ nadzorczy wskazał, że zarówno art. 15, jak i art. 12 RODO wskazują na administratora jako podmiot, który w określony sposób i w określonym terminie ma realizować prawa osób, których dane dotyczą, a dodatkowo przewidzieć procedury mające na celu realizację tych praw i ułatwienie ich realizowania. W związku z tym należy wskazać, że udzielenie informacji o przetwarzaniu danych na podstawie art. 15 RODO należy do zadań administratora.

Rola IOD

Natomiast zadania inspektora ochrony danych to m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych przez administratora i doradzanie mu w tym zakresie (art. 39 ust. 1 RODO) oraz pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO). Rola IOD jako punktu kontaktowego dla osób, których dane dotyczą, jest mocno powiązana z obowiązkami administratora i ma przyczyniać się do skuteczniejszego ich wykonywania. Rolą IOD jest bowiem budowanie świadomości administratora w zakresie praw tych osób, a następnie monitorowanie skuteczności przyjętych w tym zakresie procedur i rozwiązań, a gdy to konieczne – proponowanie ich modyfikacji.
Zgodnie z powołanym powyżej art. 38 ust. 4 RODO osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Stosowanie tego przepisu nie powinno prowadzić do wyręczania administratora przez IOD w jego obowiązkach, ponieważ IOD nie mógłby przez to realizować własnych zadań, tj. w sposób niezależny monitorować i doradzać administratorowi w zakresie tych obowiązków. Nieprzestrzeganie rozróżnienia tych dwóch ról mogłoby doprowadzić do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do IOD art. 38 ust. 6 RODO. Dlatego rolę punktu kontaktowego należy rozumieć tu raczej jako wsparcie dla osób, których dane dotyczą w sytuacjach, w których osoby zgłosiłyby zastrzeżenia, trudności czy wątpliwości co do wykonywania praw przysługujących im na mocy RODO.

IOD nie powinien być pełnomocnikiem administratora

Jednocześnie organ nadzorczy zaznaczył, że IOD nie powinien być pełnomocnikiem administratora. Zadaniem pełnomocnika jest ochrona interesów mocodawcy, działanie według instrukcji i sugestii mocodawcy, co stoi w sprzeczności z niezależnością inspektora ochrony danych, zagwarantowaną w RODO, w tym w art. 38 ust. 3 RODO. Zgodnie z tym przepisem, administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań.
Pełnienie roli pełnomocnika przez IOD w sprawach z zakresu ochrony danych osobowych u administratora, u którego IOD pełni swoją funkcję, stoi ponadto w kolizji z nakazem nienakładania

na IOD zadań powodujących konflikt interesów. IOD działając jako pełnomocnik administratora (czyli zgodnie z wolą i interesem mocodawcy), mógłby być zmuszony do pomijania i własnych spostrzeżeń i rekomendacji, które wypracował jako IOD.

Podstawowym zadaniem IOD jest monitorowanie przestrzegania przepisów o ochronie danych osobowych przez administratora i doradzanie mu w tym zakresie. Występowanie w roli pełnomocnika administratora, w zakresie obowiązków nałożonych na administratora, może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są wykonywane i czy są wykonywane prawidłowo.

Z analogicznych powodów ocenić należy, że konflikt interesów powodowałoby dokonywanie przez IOD na podstawie pełnomocnictwa administratora również innych czynności, np. podpisywanie formularza zgłoszenia naruszenia czy pism, w których w imieniu administratora miałby zobowiązywać się do realizacji pewnych działań, w tym doskonalących, np. wdrożenie nowych rozwiązań informatycznych związanych z podniesieniem bezpieczeństwa danych.

Nadmienić również należy, że inspektor ochrony danych – ze względu na swoją rolę fachowego doradcy i podmiotu w sposób niezależny monitorującego przestrzeganie przepisów o ochronie danych osobowych – powinien ze swej strony odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia konfliktu interesów, by możliwe było odpowiednio wczesne zapobieganie mu. W przypadku wystąpienia takiego konfliktu inspektor ochrony danych powinien powstrzymać się od dokonywania czynności w imieniu administratora lub wypowiedzieć udzielone mu pełnomocnictwo.

Fot. Carlos Muza

GRUPA KAPITAŁOWA NIE MOŻE WNIOSKOWAĆ O ZATWIERDZENIE KODEKSU POSTĘPOWANIA

Zgodnie z przepisami RODO podmiotami, które mogą opracowywać kodeksy postępowania są zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Uprawnienia takiego nie mają podmioty działające w ramach jednej grupy kapitałowej, a tym samym pozostające wobec siebie w ścisłych relacjach organizacyjnych i gospodarczych.

W związku z podejmowanymi przez różne środowiska inicjatywami stworzenia kodeksów postępowania UODO wyjaśnia, że podmiotami, które mogą opracowywać kodeksy postępowania są zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Przesądza o tym art. 40 ust. 2 RODO.
Dodatkowe wyjaśnienie treści tego przepisu zawiera motyw 98 RODO, w którym jest mowa o zrzeszeniach lub innych organach reprezentujących kategorie administratorów lub podmiotów przetwarzających. Wskazano tam, że kodeksy postępowania mają ułatwiać skuteczne stosowanie RODO z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.
Można zatem przyjąć, że dla ustalenia, czy dany podmiot jest uprawniony do stworzenia kodeksu postępowania konieczne jest uznanie go za podmiot (jednolity lub składający się z wielu innych podmiotów działających w jakiejś branży – zrzeszenie) działający w imieniu grupy, którą reprezentuje. Intencją ustawodawcy nie było natomiast przyznanie inicjatywy do opracowania kodeksu postępowania wyłącznie podmiotom działającym w ramach jednej grupy kapitałowej, a zatem pozostających wobec siebie w ścisłych relacjach organizacyjnych i gospodarczych.
Grupę kapitałową można uznać za grupę przedsiębiorstw, o której mowa w art. 4 pkt 19 RODO. Gdyby ustawodawca uznał grupę przedsiębiorstw za zrzeszenie, to jasno wskazałby to w tekście rozporządzenia, jak ma to miejsce w przypadku grup przedsiębiorstw, o których mowa w art. 47 albo chociaż jako przykład wśród podmiotów wskazanych w art. 40.

Stanowisko EROD oraz opinie doktryny

Powyższe stanowisko znajduje potwierdzenie nie tylko w treści ww. przepisów, ale i w **Wytycznych Europejskiej Rady Ochrony Danych 1/2019** dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679 oraz w poglądach doktryny.
W powołanych Wytycznych jest mowa o reprezentacji branży (a nie o pozycji rynkowej). Element reprezentatywności jest powiązany z określeniem podmiotowym (zrzeszenia i inne organy).

Także w literaturze (m.in. w komentarzach do RODO pod redakcją P. Fajgielskiego czy P. Litwińskiego) powszechnie przyjmuje się, że kodeksy postępowania powinny sporządzać organizacje branżowe zrzeszające przedsiębiorców z danego sektora, a nie sami administratorzy czy podmioty przetwarzające. Stanowiska przyjęte w grupie kapitałowej, ze względu na podporządkowanie podmiotów w niej zebranych wobec spółki matki, trudno uznać za samoregulację branży. Zgodnie ze **stanowiskiem Grupy Roboczej Art. 29 z 14 stycznia 1998 r. o samoregulacji zarządzania branżą**, samoregulacja (lub inny instrument) należy rozumieć jako zbiór przepisów o ochronie danych mających zastosowanie dla wielu administratorów z tego samego zawodu lub sektora przemysłu, których treść została określona przede wszystkim przez członków danej branży lub danego zawodu. Zdecydowanie samoregulację można określić jako zbiór norm ujętych w ramach kodeksu postępowania (przyjętych w sformalizowany sposób i zatwierdzonych przez Prezesa UODO) pozwalających uszczegółowić przepisy RODO i w praktyczny sposób dostosować do specyfiki danej branży.
Reasumując, samoregulacja jest uzupełniającą metodą wdrażania i kontroli przestrzegania niektórych przepisów. Zgodne z treścią powołanych Wytycznych EROD 1/2019 kodeksy mogą stanowić mechanizm umożliwiający wykazywanie zgodności z RODO. Stanowią one również okazję dla konkretnych sektorów do refleksji nad wspólnymi czynnościami przetwarzania danych oraz do uzgodnienia specjalnych i praktycznych przepisów o ochronie danych, które będą odpowiadać potrzebom sektora, a także wymogom RODO.

Konkluzja

Podsumowując, grupa kapitałowa nie jest zrzeszeniem, o którym mowa w art. 40 ust. 2 RODO. Z faktu zajmowania przez określony podmiot pozycji dominującej w jakiejś branży nie wynika jego reprezentatywność dla branży czy sektora. Dlatego należy uznać, że grupa kapitałowa nie jest podmiotem uprawnionym do przedłożenia wniosku o zatwierdzenie kodeksu postępowania na podstawie art. 27 ustawy z 10 maja 2018 r. o ochronie danych osobowych.

UODO zachęca do współpracy

Biorąc jednak pod uwagę rolę kodeksów postępowania w zapewnianiu najwyższych standardów ochrony danych osobowych, organ nadzorczy zachęca grupy kapitałowe rozważające stworzenie takich dokumentów do nawiązania współpracy z innymi administratorami z danego sektora w celu utworzenia podmiotu, który mógłby być uznany za reprezentujący interesy branży, a nie wyłącznie jednej grupy kapitałowej. Podmiot taki nie musi być strukturą wysoce sformalizowaną.
Za wystarczające uznać można ciało powstałe w wyniku porozumienia zainteresowanych podmiotów z branży, które zdecydują się współpracować np. na podstawie pisemnego porozumienia.
Organ nadzorczy udzieli niezbędnego wsparcia, by taka inicjatywa zakończyła się stworzeniem kodeksu postępowania spełniającego wymogi RODO.

ZAMIESZCZENIE TREŚCI MARKETINGOWYCH NA KARCIE SIM WYMAGA ZGODY UŻYTKOWNIKA OKREŚLONEJ W PRZEPISACH PRAWA TELEKOMUNIKACYJNEGO

Kontakty SDN zamieszczone na karcie SIM mogą zostać uznane za prowadzenie marketingu bezpośredniego. Zdecydowana odmowa ponownego kontaktu telefonicznego stanowi sprzeciw na przetwarzanie danych osobowych w celach marketingowych. Takie rozstrzygnięcia przyjął Prezes UODO po rozpatrzeniu skargi na niezgodne z prawem przetwarzanie danych osobowych przez jednego z popularnych operatorów telefonii komórkowej.

Na nowej karcie SIM, którą skarżący otrzymał od operatora telefonii komórkowej, zapisano – w sposób trwały i niemożliwy do usunięcia – kontakty SDN. W większości są to skróty do usług dodatkowych, oferowanych przez operatora, z jednoczesnym wskazaniem ceny za ich aktywację typu: „Audiobooki", „Magia i Horoskopy", „Czytelnia". Zdaniem skarżącego jest to forma marketingu bezpośredniego, na którą nie wyraził zgody.

W skardze została podniesiona również kwestia wykonania przez spółkę niechcianych połączeń telefonicznych. Skarżący skontaktował się z infolinią operatora w sprawie przedstawienia ofert na przedłużenie usług telefonicznych. Propozycja złożona przez konsultantkę nie spełniła jednak jego oczekiwań, wobec czego zaoferowała ona kontakt w późniejszym terminie. Skarżący początkowo wyraził na to zgodę, ale ze względu na brak możliwości odebrania telefonu w zaproponowanych godzinach, zdecydowanie odmówił i poinformował, że samodzielnie skontaktuje się w dogodnym dla siebie czasie. Pomimo jasno wyrażonej odmowy, w dniu następnym spółka kilkukrotnie próbowała się z nim skontaktować telefonicznie.

Skarżący wskazał również, że zarzuty stawiane spółce dot. wniesienia sprzeciwu wobec niechcianego marketingu były już przedmiotem postępowania przed Głównym Inspektorem Ochrony Danych Osobowych (GIODO), w ramach którego wydano decyzję, zakazującej spółce przetwarzania danych osobowych w celach marketingowych oraz przed Urzędem Komunikacji Elektronicznej, w ramach którego spółka zobowiązała się do wymiany karty SIM na zawierającą mniej, pozbawionych treści marketingowych kontaktów SDN.

Marketing telefoniczny tylko za zgodą określoną w przepisach prawa telekomunikacyjnego

Badając sprawę organ nadzorczy przypomniał, że przepisem uprawniającym do przetwarzania danych jest art. 6 ust. 1 RODO, zgodnie z którym przetwarzanie danych jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z wskazanych w nim przesłanek. Odnosząc się do kwestii marketingu bezpośredniego

organ oparł swoje rozważania na zbadaniu przesłanki tzw. prawnie uzasadnionego interesu, określonej w art. 6 ust. 1 f RODO, której doprecyzowanie zamieszczono w motywie 47 rozporządzenia. Niezależnie od regulacji z zakresu ochrony danych osobowych, prowadzenie marketingu bezpośredniego przy wykorzystaniu połączeń i wiadomości telefonicznych oraz przy wykorzystaniu poczty elektronicznej określa również ustawa z dnia 16 lipca 2004 r. prawo telekomunikacyjne. Zgodnie z art. 172 ust. 1 wskazanej ustawy zakazane jest używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego lub przesyłania niezamówionej informacji handlowej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę. Powyższy przepis uzależnia zatem możliwość prowadzenia marketingu bezpośredniego za pośrednictwem telekomunikacyjnych urządzeń końcowych (za które w doktrynie uznaje się m.in. telefony komórkowe) od uzyskania odpowiedniej zgody.

Kontakt SDN na karcie SIM – marketing bezpośredni?

W badanej sprawie kluczowe było rozstrzygnięcie: czy kontakty SDN umieszczone na karcie SIM można w ogóle uznać za formę marketingu bezpośredniego? Operator, udzielając wyjaśnień organowi nadzorczemu odrzucił takie stanowisko i stwierdził, że nie można uznać tego rodzaju przetwarzania danych osobowych abonentów i użytkowników sieci za przetwarzanie w celach marketingowych.
Prezes UODO rozstrzygając tę kwestię wskazał, powołując się na wyrok NSA z dnia 5 grudnia 2018 r. o sygn. I OSK 53/17, że za marketing należy uznać informację o produktach, które stanowią podkreślenie ich atrakcyjności i nakłonienie do działania polegającego na skorzystaniu z prezentowanej oferty. Ponadto, zgodnie z ww. wyrokiem NSA, działania marketingowe mają nie tyle informować, co przekonywać do podjęcia określonych działań poprzez oddziaływanie na emocje odbiorcy. Organ nadzorczy przenosząc powyższe rozważania na grunt badanej sprawy stwierdził, że nazwy kontaktów SDN prezentowane na karcie SIM mają na celu zachęcenie do skorzystania z dodatkowych usług oferowanych przez spółkę. Wskazane kontakty zawierają bowiem, oprócz numeru kontaktowego, także informacje na temat danej usługi wraz z wyrazem „włącz", zachęcającym do ich aktywacji i wyświetlane są przy każdej próbie wykonania połączenia telefonicznego z użyciem kontaktów zapisanych obok nich w książce telefonicznej urządzenia. Zdaniem organu, zamieszczenie tego rodzaju treści w nazwach kontaktów SDN, które wraz z nazwą usługi zawierają informacje o cenie i umożliwiają jej natychmiastową aktywację, stanowi formę marketingu bezpośredniego i tym samym świadczy o przetwarzaniu danych osobowych w celach marketingowych.

Brak zgody na marketing bezpośredni

Odnosząc się do zgody, o której mowa w art. 172 ust. 1 prawa telekomunikacyjnego organ nadzorczy

wskazał, że nie jest to zgoda na podstawie art. 6 ust. 1 a RODO, niemniej jej wyrażenie jest niezbędne, aby uznać za legalny proces przetwarzania danych osobowych w celu prowadzenia marketingu bezpośredniego z użyciem telefonicznego kanału kontaktu. Natomiast samą kartę SIM należy uznać, zgodnie z poglądami doktryny, za urządzenie końcowe sensu stricto, a więc za część urządzenia, które jest przeznaczone do współpracy z siecią i stanowi znaczący element (podzespół urządzenia). Operator sieci komórkowej powinien zatem uzyskać zgodę skarżącego, która jak wskazuje wyrok Sądu Okręgowego - Sądu Ochrony Konkurencji i Konsumentów z dnia 22 października 2021 r., sygn. XVII AmT 24/20 , powinna mieć charakter wyraźny i nie wynikać z innych oświadczeń woli np. z umowy o świadczeniu usług komunikacyjnych. Prezes UODO uznał tym samym, że spółka przetwarzała dane skarżącego bez jego zgody wymaganej przepisami prawa telekomunikacyjnego. Przetwarzanie danych w celach marketingowych z wykorzystaniem telefonicznego kanału kontaktu poprzez zamieszczenie kontaktów SDN na karcie SIM, które wraz z nazwą usługi zawierają również informację o jej cenie i umożliwiają natychmiastową aktywację usługi poprzez wybranie kontaktu w telefonie, nie znajduje zatem uzasadnienia w przesłance wskazanej w art. 6 ust. 1 lit. f RODO i stanowi naruszenie ochrony danych osobowych. Korzystając z przysługujących mu uprawnień naprawczych organ nadzorczy nakazał spółce dostosowanie przetwarzania do przepisów RODO i zaprzestanie prezentowania skarżącemu treści marketingowych zawartych w nazwach kontaktów SDN zapisanych na karcie SIM jego telefonu.

Sprzeciw na przetwarzanie danych w celu marketingowym

Odnosząc się do drugiej podnoszonej przez skarżącego kwestii – niechcianego kontaktu telefonicznego w sprawie przedłużenia oferty na usługi telekomunikacyjne, Prezes UODO wskazał, iż zgodnie z art. 21 ust. 2 i 3 RODO, jeżeli dane osobowe przetwarzane są na potrzeby marketingu bezpośredniego osoba, której dane dotyczą może w dowolnym momencie wnieść sprzeciw wobec takiego przetwarzania. Taki sprzeciw jest natychmiast skuteczny i jakikolwiek kontakt po jego wyrażeniu stanowi naruszenie art. 21 ust 3 RODO. Zdaniem organu, za taki sprzeciw można uznać odmowę skarżącego na ponowny kontakt ze strony spółki i informację, że samodzielnie skontaktuje się z nią w innym, bardziej dogodnym dla siebie terminie.

Operator sieci komórkowej tłumaczył, że ponowne skontaktowanie się ze skarżącym, wbrew jego zdecydowanej odmowie, było spowodowane błędem po stronie jego partnera biznesowego, który nie zmodyfikował wprowadzonej do systemu informacji. Zdaniem organu, nie zdejmuje to jednak odpowiedzialności ze spółki, gdyż zgodnie z wyrażoną w art. 5 ust. 2 zasadą rozliczalności oraz wskazanym w art. 24 ust. 1 RODO ciążącym na administratorze obowiązku zapewnienia odpowiednich środków technicznych i organizacyjnych, to ona, jako administrator, powinna zorganizować proces przetwarzania danych osobowych w taki sposób, by był on zgodny z prawem, a w kontekście badanej sprawy, umożliwiał chociażby prawidłowe wprowadzanie danych do systemu. Tym samym Prezes UODO uznał, że również w tym wypadku doszło do naruszenia ochrony danych osobowych i udzielił spółce stosownego upomnienia.

ROLA PODMIOTU PRZETWARZAJĄCEGO W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH NA GRUNCIE RODO

Przepisy RODO nakładają na administratorów danych osobowych szereg obowiązków, takich jak konieczność zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu czy zawiadamiania o nich podmiotów danych. To na administratorach spoczywa główny ciężar odpowiedzialności za wykonanie ww. zadań, jednak istotną rolę w tym procesie odgrywają również podmioty przetwarzające. Jakie działania powinny one podejmować, aby we współpracy z administratorami prawidłowo realizować obowiązki wynikające z występujących naruszeń?

„Podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Stosownie do art. 28 ust. 3 RODO przetwarzanie to odbywa się na podstawie umowy lub innego instrumentu prawnego, określającego przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora. Art. 28 ust. 3 lit. f) RODO wskazuje zaś, że podmiot przetwarzający pomaga administratorowi wywiązać się z zadań określonych w art. 32-36 RODO (a zatem m.in. z obowiązku notyfikacji, o którym mowa w art. 33 RODO, oraz zawiadomienia osób, których dane dotyczą, w trybie art. 34 RODO), co należy uwzględnić w ramach ww. ustaleń.

Obowiązek zgłoszenia naruszenia administratorowi

W myśl art. 33 ust. 2 RODO po stwierdzeniu naruszenia ochrony danych osobowych podmiot przetwarzający ma obowiązek bezzwłocznego poinformowania o nim administratora.
Warto zauważyć, że podmiot przetwarzający nie jest zobowiązany do dokonania oceny ryzyka wynikającego z naruszenia – to administrator powinien przeprowadzić analizę ryzyka w związku z zaistniałym incydentem i podjąć decyzję o ewentualnym zgłoszeniu go organowi nadzorczemu (więcej na ten temat w „Biuletynie UODO" nr 7-8/07-08/23, s. 16) oraz zawiadomieniu osób, których dane dotyczą. W gestii podmiotu przetwarzającego pozostaje ustalenie, czy doszło do naruszenia, a jeśli tak – zgłoszenie tego faktu administratorowi.
Prawodawca unijny nie przedstawił w ramach przepisów RODO precyzyjnych wytycznych w zakresie treści i formy takiego zgłoszenia, a także konkretnego terminu na jego dokonanie (przepis wskazuje wyłącznie, że trzeba to zrobić „bez zbędnej zwłoki"). Mając jednak na uwadze przytoczony powyżej obowiązek wynikający z art. 28 ust. 3 lit. f) RODO, należy przyjąć, iż działanie to powinno mieć

na celu wsparcie administratora w wykonywaniu jego zadań, a więc dostarczać mu co najmniej tych informacji, o których mowa w art. 33 ust. 3 lit. a) RODO, jak również umożliwiać dochowanie przez niego terminu na zgłoszenie naruszenia Prezesowi Urzędu Ochrony Danych Osobowych, wynoszącego 72 godziny.

Pomoc w zawiadomieniu o naruszeniu osób, których dane dotyczą

Zgodnie z art. 34 ust. 1 RODO jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia o nim osoby, których dane dotyczą. Praktyka pokazuje jednak, że w niektórych sytuacjach to podmiot przetwarzający dysponuje informacjami niezbędnymi do prawidłowego dokonania zawiadomienia, takimi jak istotne szczegóły dotyczące incydentu czy dane kontaktowe osób objętych naruszeniem. W świetle powyższego sprawnie funkcjonująca komunikacja między administratorem a podmiotem przetwarzającym może okazać się niezbędna, aby we właściwy sposób wypełnić obowiązki związane z zawiadamianiem o naruszeniu objętych nim osób.

Współpraca administratora i podmiotu przetwarzającego

W celu zminimalizowania ryzyka wystąpienia ewentualnych nieprawidłowości, w ramach realizacji zadań wynikających z naruszeń ochrony danych osobowych, strony zawierające umowę powierzenia powinny precyzyjnie określić warunki współpracy w tym obszarze. Wypracowanie dobrych praktyk i spójnych procedur może poskutkować lepszą komunikacją, usprawniając reakcję na występujące incydenty. Warto jednak pamiętać, że ustalenia te nie wpływają na prawną odpowiedzialność administratora w przypadku naruszenia art. 33 lub 34 RODO, które skutkować może nałożeniem administracyjnej kary pieniężnej.

fot. rupixen.com

GENERATYWNA SZTUCZNA INTELIGENCJA: JAK WYKORZYSTAĆ JĄ W SPOSÓB ODPOWIEDZIALNY?

W dobie dynamicznego rozwoju nowych technologii, niewątpliwie jednym z najbardziej fascynujących obszarów, który wkracza do naszego codziennego życia jest generatywna sztuczna inteligencja (GSI). Budzi ona nie tylko zainteresowanie naukowców, ale także entuzjastów technologii, czy artystów, sprawiając, że granice między rzeczywistością a wirtualnym światem stają się coraz bardziej elastyczne. W niniejszym artykule skupimy się nie tylko na tym jak działa i jakie są jej możliwości, ale również na zagrożeniach, jakie może stwarzać dla ochrony danych i prywatności. Jak więc skutecznie korzystać z tych technologii, chroniąc jednocześnie swoją prywatność?

Zacznijmy od wyjaśnienia, co to jest generatywna sztuczna inteligencja (GSI)?

Generatywna sztuczna inteligencja (GSI) to dziedzina sztucznej inteligencji (SI), która zajmuje się tworzeniem nowych danych lub treści na podstawie już istniejących. GSI wykorzystuje generatywne modele sieci neuronowych, trenowane na dużych zbiorach danych z użyciem uczenia maszynowego, w celu naśladowania, modyfikowania lub ulepszania danych wejściowych, w postaci obrazów, tekstów, dźwięków, materiałów wideo itp.

Jednym z ciekawych przykładów opartym na GSI jest technologia, która wykorzystywana jest do przekształcania zwykłych fotografii niemalże w dzieła sztuki, naśladujące style znanych artystów. Po wybraniu dowolnego zdjęcia, użytkownik określa styl malarski, w jakim jego zdjęcie może zostać przekształcone, np. styl Vincenta van Gogha, Pabla Picassa czy Edvarda Muncha. Na podstawie tych danych, algorytm analizuje wybrany styl artystyczny i przekształca oryginalne zdjęcie nadając mu charakterystyczne cechy. To narzędzie jest jednym z wielu, które demonstruje potencjał generatywnej sztucznej inteligencji w dziedzinie sztuki czy tworzenia grafiki. Podobne podejścia są stosowane również w wielu innych obszarach, takich jak generowanie obrazów medycznych, projektowanie gier komputerowych czy nawet generowanie tekstu o zadanym stylu.

Niewątpliwie GSI ma wiele potencjalnych zastosowań i możliwości, ale może także stwarzać pewne zagrożenia, w tym również dla ochrony danych i prywatności użytkowników, jeśli nie będzie używana w sposób odpowiedzialny. To właśnie dane odgrywają kluczową rolę w szkoleniu i obsłudze tych systemów.

Modele generatywnej sztucznej inteligencji wytrenowane na danych osobowych mogą potencjalnie wyodrębnić poufne informacje, takie jak nazwiska, adresy, informacje zdrowotne, a nawet dane

finansowe, a następnie ponownie opublikować te dane w wynikach wyszukiwania dla innych użytkowników. Dane te mogą zostać następnie wykorzystane do działań niezgodnych z prawem, w tym do tworzenia i rozprzestrzeniania się „deepfakes", oszustw typu phishing, a w poważniejszych przypadkach nawet do kradzieży tożsamości. Niestety po udostępnieniu danych osobowych generatywnym modelom sztucznej inteligencji ich wycofanie może być procesem niezwykle skomplikowanym, a może nawet niemożliwym do zrealizowania.

Generatywne systemy SI zgodne z RODO

1. **Ocena skutków dla ochrony danych (DPIA)** – przed rozpoczęciem przetwarzania danych osobowych duże znaczenie ma identyfikacja związanego z nim ryzyka. Administrator danych ma obowiązek zidentyfikować potencjalne zagrożenia dla ochrony danych i zastosować odpowiednie środki techniczne i organizacyjne w celu zmniejszenia ryzyka do akceptowalnego poziomu. DPIA pozwala na budowanie i wykazywanie zgodności przetwarzania z przepisami RODO oraz minimalizowanie ryzyka naruszenia praw lub wolności osób fizycznych.
2. **Transparentność** – jest szczególnie istotna, ponieważ generatywne modele SI mogą być wykorzystywane do przetwarzania i generowania danych osobowych w sposób, który może być trudny do zrozumienia dla osób, których dane dotyczą. W związku z tym należy przedstawić użytkownikowi klarowną informację, sformułowaną jasnym i prostym językiem na temat przetwarzania jego danych, zawierającą m.in. cel i sposób przetwarzania, podstawę prawną czy okres przechowywania. Ponadto można zbierać wyłącznie te dane, które są adekwatne do osiągnięcia określonego celu. Dane powinny być istotne i ograniczone do tego, co niezbędne.
3. **Podstawa prawna** – jest jednym z kluczowych elementów RODO, ponieważ zapewnia, że przetwarzanie danych osobowych jest zgodne z prawem i nie narusza praw osób, których dane dotyczą. Zgodnie z art. 6 ust. 1 RODO, przetwarzanie danych jest zgodne z prawem, jeśli spełnia co najmniej jeden z sześciu przedstawionych warunków, w tym m.in. wyrażenie zgody przez osobę, której dane dotyczą. Dla modeli generatywnej sztucznej inteligencji, takich jak np. ChatGPT, przetwarzanie danych odbywa się zwykle w kontekście „uzasadnionego interesu" dostawcy usługi, gdzie celem jest poprawa jakości i skuteczności świadczonych usług.
4. **Prawa osób, których dane dotyczą** – osobie, której dane dotyczą przysługuje szereg praw, w tym m.in. prawo dostępu do danych czy ich sprostowania, gdy są nieprawidłowe lub niekompletne. Warto w tym miejscu przypomnieć, że do UODO została skierowana skarga na ChatGPT, ponieważ żądania związane z realizacją praw, jakie przysługują skarżącemu na gruncie RODO (w tym prawo do sprostowania danych po tym jak ChatGPT wygenerował nieprawdziwe informacje na temat osoby skarżącego), nie zostały zrealizowane przez OpenAI.
5. **Zautomatyzowane podejmowanie decyzji** – w przypadku operacji przetwarzania danych w przypadku operacji przetwarzania danych osobowych w kontekście generatywnej sztucznej

inteligencji, szczególne znaczenie będzie miało informowanie o aspektach przetwarzania w kontekście tzw. „zautomatyzowanego podejmowania decyzji". W takich sytuacjach osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Ma również prawo do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia przez niego własnego stanowiska i w stosownych sytuacjach zakwestionowania danej decyzji.

6. **Regularny audyt** – w celu monitorowania treści generowanych przez sztuczną inteligencję istotne jest przeprowadzanie regularnych audytów pod kątem zagrożeń dla prywatności. Ważne jest także wdrażanie mechanizmów umożliwiających identyfikację i reagowanie na wszelkie przypadki, w których mogą zostać ujawnione wrażliwe dane.

Warto w tym miejscu wspomnieć, że 26 października 2023 r. Konfederacja Europejskich Organizacji Ochrony Danych (CEDPO) opublikowała artykuł na temat Generatywnej Sztucznej inteligencji, w którym przedstawiono wytyczne dotyczące różnych skutków związanych ze stosowaniem modeli i metod generatywnej sztucznej inteligencji. W artykule omówiono również ryzyko związane z udostępnianiem danych, wdrażanie ochrony danych już w fazie projektowania, czy wybór zgodnej z prawem podstawy szkolenia generatywnych systemów SI. Wytyczne można znaleźć **tutaj**.

fot. Steve Johnson

Jak zatem korzystać z modeli GSI, żeby zadbać o swoją prywatność?

Podobnie jak w przypadku każdej nowej technologii, która zyskuje popularność i zainteresowanie, warto zachować ostrożność również podczas korzystania z rozwiązań opartych na generatywnej sztucznej inteligencji. Przed użyciem należy zapoznać się z treścią polityki prywatności.
Niestety informacje udostępniane narzędziom generatywnej SI przy użyciu ustawień domyślnych nie są prywatne i mogą ujawnić informacje zastrzeżone lub wrażliwe osobom nieupoważnionym.
W wielu przypadkach, informacje, które są wprowadzane np. podczas rozmowy z chatem działającym w oparciu o GSI, mogą zostać wykorzystane w celu dostarczania, ulepszania i rozwijania danego rozwiązania czy też do personalizacji wyświetlanych reklam. Mając to na uwadze, warto zachować dużą ostrożność przy wprowadzaniu danych. Nie wolno również zapominać o tym, że generatywna sztuczna inteligencja ułatwiła złośliwym podmiotom tworzenie wyrafinowanych e-maili phishingowych, czy „deepfake", dlatego należy podchodzić ostrożnie do treści generowanych przez sztuczną inteligencję, tym bardziej, że wygenerowane fałszywe treści są coraz trudniejsze do odróżnienia od autentycznych komunikatów.
Bez wątpienia generatywna sztuczna inteligencja pozostanie i będzie nadal ewoluować, oferując liczne możliwości poprawy jakości życia, czy rewolucjonizując przedsiębiorstwa w różnych sektorach.
Należy jednak wdrażać ją odpowiedzialnie, przestrzegając zasad ochrony danych, co pozwoli na wykorzystanie w pełni jej potencjału. Warto rozważyć wdrożenie mniejszych modeli SI (opensource), działających w oparciu o infrastrukturę danej organizacji – bez korzystania z modeli otwartych i upubliczniania danych przetwarzanych w organizacji. Ponadto edukowanie użytkowników na temat działania modeli sztucznej inteligencji, gromadzonych przez nie danych i potencjalnych zagrożeń z tym związanych może pomóc w podejmowaniu świadomych decyzji w zakresie ochrony prywatności podczas korzystania z takich technologii.

FRANCJA: ZAKAZ KORZYSTANIA Z SYSTEMU DO KONTAKTU Z URZĘDNIKAMI PAŃSTWOWYMI DO CELÓW KOMUNIKACJI POLITYCZNEJ

Francuski organ nadzorczy przeprowadził postępowanie, w wyniku którego stwierdził, że Minister Transformacji i Służby Publicznej dopuścił do naruszenia ochrony danych. Polityk wykorzystał przechowywane w systemie do komunikacji z urzędnikami dane do wysłania im komunikatu o tematyce politycznej.

26 stycznia 2023 r. do 2 346 303 czynnych zawodowo francuskich urzędników państwowych wysłano wiadomość e-mail pn. „Reforma emerytalna: Wiadomość od Stanislasa Gueriniego do urzędników służby cywilnej". E-mail zawierał link do materiału filmowego z orędzia Ministra Transformacji i Służby Publicznej uzasadniający, przyjmowaną w tym okresie reformę emerytalną oraz do dokumentu prezentacyjnego zatytułowanego „Dla naszych emerytur: projekt na rzecz sprawiedliwości, równowagi i postępu".

Po zdarzeniu Commission Nationale Informatique & Libertés (CNIL) otrzymał prawie 1600 powiązanych z incydentem skarg. W wyniku przeprowadzonego postępowania CNIL potwierdził, że Stanislas Guerini wykorzystał system ENSAP do wysłania wiadomości e-mail o tematyce politycznej, dopuścił się naruszenia ochrony danych zawartych w systemie i wykorzystał przechowywane w nim dane w nieprzeznaczonych do tego celach.

System ENSAP, zgodnie z prawem służy do służbowej wymiany i komunikacji między urzędnikami administracji publicznej. Znajdują się w nim też poufne dokumenty urzędników publicznych, takie jak miesięczne paski wynagrodzeń. Aby zarejestrować się do systemu, urzędnik podaje adres e-mail. Francuski organ nadzorczy ustalił, że minister wykorzystał zgromadzone w bazie systemu ENSAP adresy email urzędników administracji publicznej, by wysłać im komunikat polityczny.

Ostatecznie organ wezwał do usunięcia naruszenia nadawcę wysłanej wiadomości – Ministerstwo Transformacji i Finansów Publicznych oraz administratora systemu ENSAP – Ministerstwo Gospodarki, Finansów oraz Suwerenności Przemysłowej i Cyfrowej.

Źródło: Komunikat francuskiego organu nadzorczego

WŁOCHY: KARA ZA BRAK REAKCJI NA ŻĄDANIA PRACOWNIKÓW DOTYCZĄCE DOSTĘPU DO DANYCH

Włoski organ nadzorczy Garante Per La Protezione Dei Date Personali (GPDP) ukarał dwie powiązane z transportem firmy – Autostrade per l'Italia oraz Amazon Italia Transport za to, że nie udzielały swoim pracownikom odpowiedzi na prośby o dostęp do ich danych osobowych.

W reakcji na skargi obecnych oraz byłych pracowników obu firm, dotyczących braku odpowiedzi na wnioski o dostęp do ich danych osobowych, regulator nałożył administracyjne kary pieniężne: w wysokości 100 tysięcy euro dla Autostrade per l'Italia oraz 40 tysięcy euro dla Amazon Italia Transport.

fot. Steve Johnson

Źródło: Newsletter włoskiego organu nadzorczego

WŁOCHY: KARA ZA UDOSTĘPNIENIE DANYCH WRAŻLIWYCH OSOBY ZMARŁEJ

Włoski organ nadzorczy GPDP nałożył administracyjną karę pieniężną w wysokości 18 tys. euro na firmę świadczącą usługi szkoleniowe dla lekarzy za publikację informacji dotyczących wrażliwych danych zmarłego.

Do włoskiego organu nadzorczego wpłynęła skarga od mężczyzny na zamieszczenie danych osobowych jego zmarłego syna w internecie w materiałach szkoleniowych dla lekarzy psychiatrów. Opublikowane informacje obejmowały biografię syna, raporty psychiatryczne, historię medyczną, w tym przyjmowane przez niego leki, oraz informacje o popełnionych przestępstwach, w sprawie których toczyło się postępowanie. Dokumenty stanowiły część materiałów dydaktycznych wykorzystywanych do zilustrowania lekarzom konkretnej choroby, na którą cierpiał syn skarżącego. Materiały te – udostępnione uczestnikom za pośrednictwem linku przesłanego pocztą elektroniczną pod koniec kursu – były również dostępne online dla każdego, kto znał adres URL.
Włoski regulator nałożył na przedsiębiorstwo karę 18 000 euro, stwierdzając szereg naruszeń.
W swojej decyzji GPDP podkreślił, że ochrona prywatności nadal ma zastosowanie do danych osób zmarłych. Ponadto przedsiębiorstwo świadczące usługi szkoleniowe powinno było wdrożyć odpowiednie środki techniczne i organizacyjne, aby zagwarantować poufność przetwarzanych danych (np. zanonimizować dane oraz wdrożyć procedurę uwierzytelnienia, by umożliwić dostęp do dokumentacji wyłącznie lekarzom uczestniczącym w szkoleniu).

Źródło: Newsletter włoskiego organu nadzorczego

TSUE: WYROK W SPRAWIE C-340/21 | NATSIONALNA AGENTSIA ZA PRIHODITE

Po włamaniu hakerskim do systemu informatycznego bułgarskiej krajowej agencji przychodów skarbowych (NAP) i opublikowaniu danych osobowych milionów osób, poszkodowani pozwali agencję w celu uzyskania odszkodowania za szkodę niemajątkową. TSUE uznał, że obawa przed ewentualnym wykorzystaniem przez osoby trzecie danych osobowych może sama w sobie stanowić szkodę niemajątkową.

Bułgarska krajowa agencja przychodów skarbowych (NAP) jest organem działającym przy ministrze finansów. Jest ona w szczególności odpowiedzialna za identyfikację, zabezpieczanie i odzyskiwanie wierzytelności publicznoprawnych. W tym zakresie jest administratorem danych osobowych.
15 lipca 2019 r. media ujawniły, że miało miejsce włamanie do systemu informatycznego NAP.
W następstwie cyberataku w Internecie opublikowano zawarte w tym systemie dane osobowe dotyczące milionów osób. Wiele osób pozwało NAP w celu uzyskania odszkodowania za szkodę niemajątkową z uwagi na ich obawy dotyczące potencjalnego wykorzystania ich danych w sposób stanowiący nadużycie.
Bułgarski najwyższy sąd administracyjny zwrócił się do Trybunału Sprawiedliwości z kilkoma pytaniami prejudycjalnymi dotyczącymi wykładni ogólnego rozporządzenia o ochronie danych (RODO). Domagał się wyjaśnień dotyczących warunków odszkodowania za szkodę niemajątkową, na którą powołuje się osoba, której dane osobowe znajdujące się w posiadaniu organu publicznego zostały opublikowane w Internecie w następstwie ataku cyberprzestępców.
W swoim wyroku Trybunał uznał, że w przypadku nieuprawnionego ujawnienia danych osobowych lub nieuprawnionego dostępu do nich, z samej tej okoliczności sądy nie mogą wyprowadzać wniosku, że wdrożone przez administratora środki ochrony nie były odpowiednie. Okoliczność, czy takie środki mają właściwy charakter, sądy muszą oceniać w sposób konkretny.
Ciężar udowodnienia, że wdrożone środki ochrony były odpowiednie, spoczywa na administratorze. W przypadku gdy nieuprawnione ujawnienie danych osobowych lub nieuprawniony dostęp do nich zostały dokonane przez „osoby trzecie" np. cyberprzestępców, administrator może być zobowiązany do zapłaty odszkodowania osobom, które poniosły szkodę, chyba że uda mu się udowodnić, że w żaden sposób nie ponosi winy za tę szkodę. TSUE w swoim wyroku stwierdził, że obawa przed ewentualnym wykorzystaniem przez osoby trzecie danych osobowych w sposób stanowiący nadużycie w związku z naruszeniem RODO może sama w sobie stanowić „szkodę niemajątkową".

Źródło: Wyrok TSUE

TSUE: WYROKI W SPRAWACH C-683/21 | NACIONALINIS VISUOMENĖS SVEIKATOS CENTRAS I C-807/21 | DEUTSCHE WOHNEN

Zgodnie z wyrokami TSUE, jedynie zawinione naruszenie RODO może prowadzić do nałożenia administracyjnej kary pieniężnej. Jeżeli adresat kary pieniężnej należy do grupy spółek, kara ta powinna zostać obliczona na podstawie obrotu grupy.

Trybunał Sprawiedliwości wyjaśnił warunki, na jakich krajowe organy nadzorcze mogą nałożyć administracyjną karę pieniężną na jednego lub więcej administratorów danych za naruszenie ogólnego rozporządzenia o ochronie danych (RODO). W szczególności orzekł, że nałożenie takiej kary zakłada zawinione zachowanie, co znaczy, że naruszenie zostało popełnione umyślnie lub w wyniku zaniedbania. Ponadto jeżeli adresat kary pieniężnej należy do grupy spółek, obliczenie kary pieniężnej powinno opierać się na obrocie całej grupy.

Sądy litewski i niemiecki zwróciły się do Trybunału Sprawiedliwości o wykładnię ogólnego rozporządzenia o ochronie danych (RODO) co do możliwości nakładania przez krajowe organy nadzorcze sankcji za naruszenie RODO w drodze administracyjnej kary pieniężnej na administratora danych. W sprawie litewskiej krajowe centrum zdrowia publicznego przy ministerstwie zdrowia zakwestionowało karę pieniężną w wysokości 12 tys. euro, którą nałożono na nie w związku z utworzeniem, dzięki wsparciu prywatnego przedsiębiorstwa, aplikacji mobilnej w celu rejestracji i monitorowania danych osób narażonych na COVID-19. W sprawie niemieckiej spółka nieruchomościowa Deutsche Wohnen, która posiada pośrednio około 163 tys. lokali mieszkalnych i 3 tys. lokali użytkowych, zakwestionowała między innymi nałożoną na nią karę pieniężną w wysokości ponad 14 mln euro za przechowywanie danych osobowych najemców dłużej niż było to konieczne.

Trybunał orzekł, że wobec administratora danych można zastosować administracyjną karę pieniężną za naruszenie RODO tylko wtedy, gdy naruszenie to zostało popełnione w sposób zawiniony, to znaczy umyślnie lub w wyniku zaniedbania. Jest tak w przypadku, gdy administrator danych wiedział, że jego zachowanie stanowi naruszenie, niezależnie od tego, czy miał świadomość popełnienia naruszenia, czy też nie.

Jeżeli administratorem jest osoba prawna ponosi ona odpowiedzialność zarówno za naruszenia popełnione przez jej przedstawicieli, dyrektorów lub zarządców, jak i przez każdą inną osobę działającą w ramach jej działalności gospodarczej i na jej rachunek. Ponadto nałożenia administracyjnej kary pieniężnej na osobę prawną jako administratora danych nie można uzależnić od uprzedniego stwierdzenia, że naruszenie to zostało popełnione przez zidentyfikowaną osobę fizyczną. Co więcej, na administratora można nałożyć karę pieniężną również za operacje dokonywane przez podmiot przetwarzający, o ile operacje te można przypisać administratorowi.

W odniesieniu do współadministracji dwóch lub większej liczby podmiotów, Trybunał wyjaśnił, że wynika ona z samego faktu, iż podmioty te uczestniczyły w ustalaniu celów i sposobów przetwarzania danych. Zakwalifikowanie jako „współadministratorów” nie zakłada istnienia formalnych uzgodnień między danymi podmiotami. Wspólna decyzja lub nawet zbieżne decyzje są wystarczające. Jednakże, gdy rzeczywiście mamy do czynienia ze współadministratorami, powinni oni określić w drodze uzgodnień swoje obowiązki.

Trybunał również wskazał, że organ nadzorczy przy obliczaniu kary pieniężnej, gdy adresat jest przedsiębiorstwem lub jego częścią musi oprzeć się na pojęciu „przedsiębiorstwa” w prawie konkurencji. Maksymalną kwotę kary pieniężnej należy obliczyć na podstawie odsetka całkowitego rocznego światowego obrotu danego przedsiębiorstwa z poprzedniego roku obrotowego, postrzeganego jako całość.

fot. Tingey Injury

Źródła: Wyrok TSUE, Wyrok TSUE

PODSTAWA PRAWNA REALIZACJI AUDYTU INSPEKTORA OCHRONY DANYCH

Agnieszka Gębicka, Inspektor Ochrony Danych, Zakład Ubezpieczeń Społecznych
mec. Sławomir Wichrowski, Zastępca Inspektora Ochrony Danych, Zakład Ubezpieczeń Społecznych

Audyt jest jednym ze sposobów cyklicznej weryfikacji wdrożenia adekwatnych środków organizacyjnych i technicznych zapewniających odpowiedni poziom bezpieczeństwa danych osobowych. By zapewnić w procedurach wewnętrznych oraz w praktyce realizację audytów warto zwrócić uwagę na kilka kwestii.

Termin „audyt" występuje w RODO wielokrotnie. Sformułowania obejmujące ten zakres tematyczny znajdziemy odpowiednio w art. 28, art. 39, art. 47, a także art. 59 RODO. Jego zastosowanie odnosi się m.in. do działania organów kontrolnych, udostępniania danych osobowych czy procedury powierzania. Tak częste używanie tego terminu pozwala domniemywać, że kompleksowy i profesjonalnie zrealizowany audyt RODO stanowi o znaczącej wartości dodanej w przestrzeganiu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.
Zgodnie z art. 39 RODO jednym z podstawowych obowiązków inspektora jest monitorowanie zgodności przetwarzania danych z przepisami o ochronie danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Warto przyzwyczaić organizację w której odgrywamy rolę inspektora ochrony danych, do tego, że audyt realizujemy w celu poprawy procesu przetwarzania danych osobowych oraz doprowadzenia do sytuacji zgodności z przepisami RODO. Błędną praktyką jest przeprowadzanie audytu na zasadzie wykazywania nieprawidłowości i pełnienia funkcji tzw. „złego policjanta". Audyty, które były przez nas przeprowadzane przynoszą lepszy efekt, kiedy już w trakcie ich realizacji usuwane są nieprawidłowości. Oczywiście, jeśli zauważamy niezgodności, których komórka audytowana nie jest w stanie poprawić natychmiast, wówczas taka nieprawidłowość wykazywana jest w raporcie oraz określany jest czas na realizację i rekomendowane działania. Wyznacznikiem skutecznych działań IOD jako audytora powinno być doprowadzenie organizacji do zgodności procesów przetwarzania z przepisami o ochronie danych, a nie wykazywanie w raporcie jak największej liczby nieprawidłowości.
Aktywność inspektora ochrony danych w tym zakresie powinna mieć charakter ciągły i wielofazowy,

nie jednorazowy. Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektorów ochrony danych monitorowanie to:

- zbieranie informacji w celu identyfikacji procesów przetwarzania;
- analizowanie i sprawdzanie zgodności przetwarzania;
- informowanie, doradzanie i rekomendowanie określonych działań.

Wykonując ten obowiązek inspektor ochrony danych powinien dostosować sposób i rodzaj przekazywanych informacji do grupy docelowej, tak aby zadanie to było realizowane w sposób efektywny i skuteczny.

Kolejnym elementem, na który musimy zwrócić uwagę, by zapewnić sobie w procedurach wewnętrznych oraz w praktyce realizację audytów jest umiejscowienie IOD w strukturze organizacji bezpośrednio pod Prezesem oraz wyeliminowanie konfliktu interesów w kontekście realizowanych zadań. Przykładowo, IOD nie może projektować procesu, który w późniejszym okresie będzie audytował. Oczywiście wydanie rekomendacji czy zaleceń nie stanowi tu problemu, jest jednym z zadań Inspektora, musimy być jednak ostrożni, ponieważ granica pomiędzy zaleceniem a władczym planowaniem może okazać się płynna i niezrozumiała dla właściciela biznesowego.

W tym miejscu posłużymy się przykładem:

> W trakcie prac projektowych IOD (jako głos doradczy) zauważył, że zabezpieczenia są nieadekwatne dla ryzyk, ponieważ zostały zaplanowane wg znanego i stosowanego od lat w organizacji klucza, podczas gdy do IOD spływała informacja o zwiększającej się liczbie naruszeń w podobnym procesie przetwarzania. W takim przypadku Inspektor powinien zakomunikować o konieczności wdrożenia dodatkowych zabezpieczeń, uzasadniając to materializacją ryzyka, ale propozycja możliwych do implementacji mechanizmów kontrolnych to rola komórki odpowiedzialnej za tworzony proces oraz dział IT lub bezpieczeństwa.

Kolejnym ważnym elementem jest konieczność wypracowania zasad współpracy IOD z komórkami audytu wewnętrznego lub kontroli wewnętrznej. W naszej organizacji ukształtowaliśmy tę współpracę na zasadach ściśle rozdzielających kwestie związane z ochroną danych osobowych i pozostałymi aspektami. Jeśli w przypadku audytu realizowanego przez komórkę audytu zostaną ujawnione kwestie związane z obszarem ochrony danych, wtedy sprawa przekazywana jest do IOD celem zajęcia stanowiska. Podobnie działa to w przypadku współpracy z komórką kontroli wewnętrznej. Taka praktyka ma również potwierdzenie w dokumencie wydanym przez Ministerstwo Finansów i Urząd Ochrony Danych Osobowych o nazwie „Zasady współpracy audytora wewnętrznego i inspektora ochrony danych przy realizacji zadań w jednostce sektora finansów publicznych”. Działania audytorów wewnętrznych i inspektorów ochrony danych powinny być

komplementarne. Zarówno w przypadku audytora wewnętrznego, jak i inspektora ochrony danych kluczową rolę odgrywa niezależność w realizowaniu zadań. Stąd audytorzy i inspektorzy muszą w swojej pracy uwzględniać wzajemną niezależność i nie wpływać na jej ograniczanie.

Audyty – cel i zakres

Audyt jest jednym ze sposobów cyklicznej weryfikacji wdrożenia adekwatnych środków organizacyjnych i technicznych zapewniających odpowiedni poziom bezpieczeństwa danych osobowych.
Przedmiot audytów IOD powinien być szeroki i obejmować zarówno środki organizacyjne, jak i techniczne stosowane przez administratora w celu wykazania, iż przetwarzanie danych osobowych następuje z poszanowaniem zasad określonych w art. 5 RODO.
Jednym z kluczowych elementów jest wybór obszarów, które zostaną poddane audytowi.
W tym celu niezbędne jest przygotowanie, przez IOD, rocznego planu audytów co pozwala na kompleksowe przeprowadzenie tego procesu z uwzględnieniem specyfiki danej organizacji.
W razie konieczności IOD powinien również przeprowadzać audyty doraźne.
Wybierając procesy, które zostaną poddane audytowi, zgodnie z koncepcją risk-based approach należy wziąć pod uwagę zagrożenia wynikające z analizy ryzyka przeprowadzanej dla operacji przetwarzania danych osobowych, w szczególności:

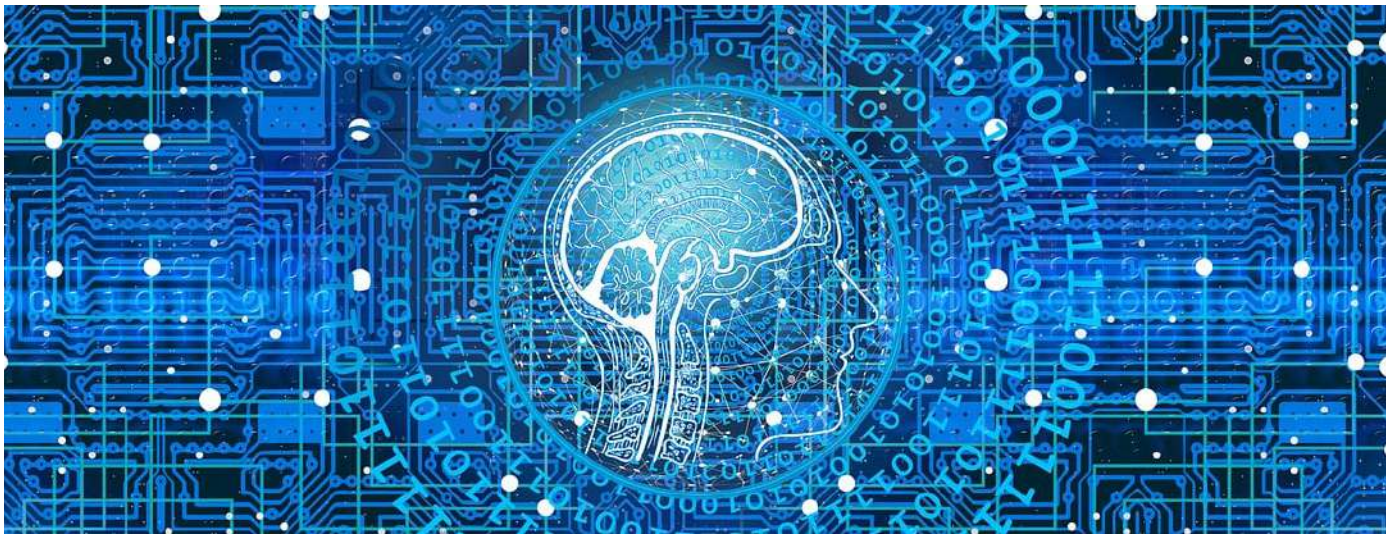
- wyniki analizy ryzyka w zakresie bezpieczeństwa informacji w organizacji;
- wyniki przeprowadzonej oceny skutków dla ochrony danych (DPIA);
- wyniki audytów IOD w organizacji;
- wyniki analizy naruszeń ochrony danych osobowych;
- monitorowanie rejestru czynności przetwarzania, np. pod kątem nowych procesów z wysokim ryzykiem związanym z przetwarzaniem danych lub zmianami w dotychczas prowadzonych czynnościach przetwarzania;
- roczny plan kontroli sektorowych UODO;
- wnioski płynące z uzasadnień decyzji Prezesa UODO nakładających kary oraz z orzecznictwa sądów administracyjnych.

W trakcie audytu należy całościowo podejść do badanego procesu i ocenić zgodność operacji przetwarzania prowadzonej przez administratora z przepisami o ochronie danych osobowych.
Zagadnienia wymagające szczególnego zainteresowania audytora to:

- zapewnienie przestrzegania zasad privacy by design oraz privacy by default w trakcie projektowania operacji przetwarzania danych osobowych;
- przeprowadzenie oceny skutków dla ochrony danych;
- zasady przetwarzania danych osobowych w systemach IT;

7 WSPÓŁPRACA Z UODO

- cykliczne testowanie skuteczności zabezpieczeń technicznych, w tym cykliczne tworzenie i odtwarzanie kopii zapasowych;
- zarządzanie uprawnieniami dostępu i rozliczalność w systemach IT;
- zapewnienie realizacji praw osób;
- cykl życia i retencja danych osobowych.



SZTUCZNA INTELIGENCJA I WYZWANIA ZWIĄZANE Z NOWOCZESNYMI TECHNOLOGIAMI

Gwałtowny rozwój nowoczesnych technologii, w tym modeli predykcyjnych wykorzystywanych do wspierania pracy, jak również pojawienie się procesów opierających się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołujących skutki prawne wobec osób (zautomatyzowane podejmowane decyzji) powoduje szczególne wyzwania dla administratorów. Szczególne zainteresowanie budzi obecnie zagadnienie sztucznej inteligencji, w tym generatywnej sztucznej inteligencji opartej na modelach językowych (LLM).

Badając możliwość wdrożenia sztucznej inteligencji należy zwrócić uwagę na kilka kwestii.

Istnieje wiele modeli sztucznej inteligencji, przykładowo można wskazać na techniki takie jak:

- uczenie maszynowe;
- uczenie nadzorowane;
- uczenie nienadzorowane;
- uczenie głębokie;
- zdecentralizowany model Federated Learning;
- sztuczna inteligencja.

Każdy z nich różni się sposobem działania i może być używany do wsparcia w innym zakresie. Nie każdy proces wymaga wsparcia przy użyciu tak zaawansowanych narzędzi jak generatywna sztuczna inteligencja. Przykładowo pomoc w przeprowadzaniu analiz może być oparta na drzewkach decyzyjnych i uczeniu maszynowym.

Powinniśmy również zwrócić uwagę, że w procesie rozwoju narzędzi opartych na sztucznej inteligencji wyróżnia się dwie kluczowe fazy:

- testowanie i walidacje (trening sztucznej inteligencji);
- produkcyjne wykorzystanie.

Ma to istotne znaczenie, przykładowo wskazać należy, że francuski organ ochrony danych (CNIL) w sposób wyraźny stwierdza, że faza treningowa i faza produkcyjna z perspektywy przepisów o ochronie danych osobowych mają inne cele i powinny być od siebie oddzielone. Oznacza to, iż w każdej z wymienionych faz administrator jest zobowiązany do zapewnienia zasad przetwarzania wymienionych w art. 5 RODO.

* AI: ensuring GDPR compliance, CNIL, 21.09.2022 r., https://www.cnil.fr/en/ai-ensuring-gdpr-compliance (dostęp w dniu 15.12.2023 r.); M. Nowakowski, Sztuczna inteligencja. Praktyczny przewodnik dla sektora innowacji finansowych, Wolters Kluwer 2023, str.

Szczególne wyzwania w tym zakresie są związane z wykazaniem legalności przetwarzania i realizacją obowiązków informacyjnych, powstają w fazie treningu sztucznej inteligencji. W konkretnych przypadkach mogą one powodować brak możliwości wykorzystania w tej fazie historycznych danych indywidualnych, które były zebrane i wykorzystywane przez administratora w innych celach. Alternatywą może być wykorzystanie danych statystycznych (zagregowanych) lub danych zanonimizowanych. Należy jednak pamiętać, że prawidłowo przeprowadzony proces anonimizacji zakłada nieodwracalność i musi być przeprowadzony przy łącznym zastosowaniu kilku technik takich jak: zaciemnianie danych czy dodawanie zakłóceń, permutacja, K-anonimizacja, L-dywersyfikacja lub L-różnorodność, T-bliskość, prywatność różnicowa. W praktyce dane zanonimizowane w taki sposób w wielu przypadkach mogą w znaczny sposób odbiegać od historycznych danych indywidualnych i wykazywać ograniczoną przydatność dla treningu sztucznej inteligencji. Rozwiązaniem wtedy może być użycie danych statystycznych mówiących o powtarzalnych zjawiskach, a nie konkretnych osobach.
W procesie rozwoju i wykorzystania sztucznej inteligencji musimy zadbać również o rozliczalność decyzji podejmowanych przez system (co jest utrudnione w przypadku generatywnej sztucznej inteligencji) oraz o zapewnienie braku dyskryminacji związanej ze stronniczym działaniem algorytmu (zjawisko takie może wystąpić, np. wskutek użycia niewłaściwych danych w fazie treningu). Dodatkowe wymagania powstają w razie wykorzystania sztucznej inteligencji do podejmowania zautomatyzowanych decyzji w rozumieniu art. 22 RODO.
Dlatego też planując wykorzystanie sztucznej inteligencji w organizacji powinniśmy:

- przeprowadzić analizę obszarów wykorzystania sztucznej inteligencji np. back office, front office, wsparcie IT (programowanie, cyberbezpieczeństwo);
- mieć świadomość ograniczeń w działaniu sztucznej inteligencji np. zjawiska halucynacji AI czy braku rozliczalności w działaniu (black box) w przypadku generatywnej sztucznej inteligencji opartej na modelach językowych;
- wprowadzić w organizacji polityki określające zasady wykorzystania AI i przypadki w których jest to zabronione (np. tajemnica przedsiębiorstwa, dane prawnie chronione);
- poddawać procesy wykorzystujące sztuczną inteligencję ciągłemu monitoringowi i doskonaleniu.

** Opinia Grupy Roboczej Art. 29 nr 05/2014 w sprawie technik anonimizacji, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pl.pdf (dostęp w dniu 15.12.2023 r.); Analiza rozwiązań w zakresie anonimizacji danych i generowania danych syntetycznych, NASK, Kancelaria Prezesa Rady Ministrów, Warszawa 2022, https://www.nask.pl/download/30/4575/AIDApublikacja-analiza-danych.pdf (dostęp w dniu 15.12.2023 r.).

TRENDY W OCHRONIE DANYCH OSOBOWYCH – 2024

r.pr. Ewa Kurowska-Tober

Współprowadząca Globalną Praktykę Ochrony Danych, Prywatności i Cyberbezpieczeństwa w Kancelarii DLA Piper

Nie jest zaskakujące, że w nowym roku jednym z największych wyzwań w zakresie prywatności i ochrony danych osobowych będzie dalej niezwykle szybko postępujący rozwój sztucznej inteligencji. Modele AI oparte na przetwarzaniu olbrzymiej ilości danych, w tym w dużej części stanowiących również dane osobowe to obszar, który wymaga szczególnej uwagi ze strony specjalistów od prywatności. Korzystanie ze sztucznej inteligencji budzi w pierwszej kolejności pytania o źródła przetwarzanych danych. Na jakich danych i na jakiej podstawie przetwarzania opierają się modele AI? Czy przetwarzanie danych wykorzystywanych przez sztuczną inteligencję spełnia zasady wyrażone w RODO, w tym na przykład, czy zapewnione jest pozyskanie i dalsze przetwarzanie wyłącznie danych niezbędnych do znalezienia rozwiązania, którego szuka AI, zgodnie z zasadą minimalizacji danych? Bardzo często nie jesteśmy pewni z jakich zasobów korzysta sztuczna inteligencja, co budzi poważne wątpliwości co do zgodnego z prawem jej zastosowania, w tym w szczególności odnośnie zasady transparentności, o czym jeszcze za chwilę. Wyzwaniem pozostaje realizowanie obowiązków informacyjnych względem podmiotów danych, których dane wykorzystują modele AI i realizacja ich praw podmiotowych zagwarantowanych w RODO. W końcu korzystający z modeli AI przetwarzających dane osobowe nie mogą zapominać o przeprowadzaniu oceny skutków dla ochrony danych, która w wielu przypadkach będzie obowiązkowa na gruncie RODO.

Wracając do zasady transparentności wyrażonej w RODO, przejrzystość procesów przetwarzania danych jest wyzwaniem nie tylko dla sztucznej inteligencji, ale dla wszelkich skomplikowanych nowoczesnych systemów informatycznych, których coraz więcej w naszym życiu. Pełna wiedza o procesach przetwarzania danych, metodach dochodzenia do oczekiwanego rozwiązania, źródłach danych to wciąż aktualne wyzwanie dla administratorów w 2024 roku.

Z tym wiąże się także kolejny silny trend skupiony wokół zapewnienia bezpieczeństwa przetwarzanych danych. W związku z ciągle rosnącym zagrożeniem cyberatakami, co obserwujemy w coraz częstszych naruszeniach danych dotyczących tego typu przestępstw, administratorzy danych nie mogą ustawać w zapewnieniu jak najlepszej ochrony danych osobowych, które przetwarzają w swoich organizacjach. Ten ciągły wyścig pomiędzy cyberprzestępcami i administratorami danych

chroniącymi swoje dane, będzie niewątpliwe ulegał intensyfikacji.
W końcu, specjaliści w zakresie ochrony danych osobowych z uwagą przyglądają się najnowszej legislacji Unii Europejskiej, która w wielu obszarach dotyka także ochrony danych osobowych.

fot. Romain Dancre

Będące na ukończeniu Rozporządzenie o sztucznej inteligencji, przyjęty już przez Parlament UE Akt w sprawie danych (Data Act) czy tworzona Europejska Przestrzeń Danych Medycznych (European Health Data Space) to jedynie wybrane przykłady obszarów, które wymagają uwzględnienia zasad ochrony danych osobowych. Współistnienie coraz bardziej skomplikowanych przepisów unijnych w tym zakresie, nie rzadko na siebie nachodzących, będzie niewątpliwym wyzwaniem dla rynku i praktyków ochrony danych osobowych.

WYZWANIA DLA ADMINISTRATORÓW DANYCH OSOBOWYCH DOTYCZĄCE PRZETWARZANIA DANYCH W OBSZARZE ZATRUDNIENIA

r. pr. dr Dominika Dörre-Kolasa

Partner w Kancelarii RACZKOWSKI

IUS LABORIS, Global HR Lawyers

Zbliżająca się wielkimi krokami implementacja dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii, potocznie zwana dyrektywą o ochronie sygnalistów spowoduje, iż największym wyzwaniem roku 2024 dla administratorów danych będzie z jednej strony zorganizowanie procesu przyjmowania zgłoszeń wewnętrznych i podejmowanie tzw. działań następczych, z drugiej zapewnienie ochrony osoby zgłaszającej przed możliwymi działaniami odwetowymi.

Zgodnie z projektowaną implementacją firmy będą musiały ustalić wewnętrzne procedury zgłaszania naruszeń. Obowiązek ten będzie odnosił się do przedsiębiorstw z sektora prywatnego, zatrudniających powyżej 50 osób oraz, bez względu na liczbę zatrudnionych pracowników, podmiotów wykonujących działalność w zakresie usług, produktów i rynków finansowych oraz przeciwdziałania praniu pieniędzy i finansowania terroryzmu, bezpieczeństwa transportu i ochrony środowiska. W dużym uproszczeniu obowiązek ten będzie odnosił się również do podmiotów publicznych. Każdy inny podmiot będzie mógł przyjąć wewnętrzną procedurę przyjmowania zgłoszeń na zasadzie dobrowolności. Ustawodawca krajowy, w ślad za dyrektywą, ustanowił również, że informacje podlegające zgłoszeniu będą miały być pozyskiwane w kontekście związanym z pracą. Ogólne rozporządzenie o ochronie danych będzie znajdować zastosowanie zarówno do przetwarzania danych osobowych w ramach wewnętrznych kanałów dokonywania zgłoszeń, jak również podejmowania działań następczych, o ile oczywiście ustawodawca krajowy nie dokona w tym zakresie określonych wyłączeń.

W dyrektywie o ochronie sygnalistów szczególną uwagę zwrócono na zasady dotyczące przetwarzania danych osobowych określone w art. 5 RODO. Mając na uwadze kontekst i okoliczności, w jakich będzie dochodzić do przetwarzania danych osobowych w ramach zgłoszeń wewnętrznych i postępowań wyjaśniających, w praktyce szczególnie problematycznie zapowiada się realizacja zasady przejrzystości przetwarzania. Poufność w ramach systemu zgłoszeń wewnętrznych i postępowań wyjaśniających, w tym przede wszystkim nieinformowanie osób których dane dotyczą, może bowiem pozostawać w oczywistej kolizji z realizacją tej zasady.

Ustawodawca krajowy powinien zatem w sposób właściwy i jednoznaczny skorzystać ze wskazówek zawartych w dyrektywie oraz uregulować zakres ingerencji regulacji o ochronie osób zgłaszających naruszenia zgodnie z zasadą przejrzystości ze szczególnym uwzględnieniem możliwości wyłączenia obowiązków informacyjnych. Polski ustawodawca skorzystał z tej możliwości i w projektowanej ustawie wyłączył zastosowanie art. 14 ust 2 lit. f oraz art. 15 ust. 1 lit g. RODO, które odnoszą się do zbierania danych z innych źródeł niż od podmiotu danych.

W mojej ocenie, uznanie ustanowienia przez podmiot prawny kanałów zgłoszeń oraz wdrożenie procedury ich wnoszenia jako realizacji zadania publicznego o doniosłym społecznie znaczeniu, pozwala na skorzystanie z możliwości jakie przewiduje art. 4 i 5 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych i pozwala na znacznie dalej idące wyłączenia. Na poparcie tej tezy można przywołać motyw (84) dyrektywy, w którym stwierdzono, iż procedury dotyczące działań następczych związanych ze zgłoszeniami naruszeń prawa Unii w dziedzinach objętych zakresem jej stosowania służą osiągnięciu ważnego celu leżącego w ogólnym interesie Unii i państw członkowskich w rozumieniu art. 23 ust. 1 lit. e) RODO, gdyż ich celem jest poprawa egzekwowania prawa i polityk Unii w określonych dziedzinach, w których naruszenia mogą wyrządzić poważną szkodę dla interesu publicznego. Uzupełniająco wskazuję, że artykuł 23 RODO reguluje zagadnienia dotyczące możliwości ograniczenia uprawnień podmiotu danych składających się na szeroko rozumiane prawo do ochrony danych osobowych oraz obowiązków administratorów względem tych podmiotów.

Należy przypuszczać, iż w tym zakresie będą występowały również inne interpretacje, a kontrowersyjnych sytuacji, w których zachodzi kolizja praw podmiotów danych będzie najprawdopodobniej wiele.

Podmiot prawny, decydując się na wybór określonych narzędzi informatycznych do przyjmowania zgłoszeń wewnętrznych, czy też rozważając skorzystanie z usług podmiotów zewnętrznych, będzie musiał zatem wziąć pod uwagę, czy zapewnią on należyte gwarancje poszanowania niezależności, poufności, ochrony danych i zachowania tajemnicy.

Na zakończenie należy również zwrócić również uwagę na właściwe zorganizowanie procesu przechowywania, a następnie niszczenia danych przetwarzanych w związku z przyjęciem zgłoszenia i podjęciem działań następczych oraz niszczenia dokumentów związanych ze zgłoszeniem. Dokumenty mają być przechowywane przez okres 3 lat po zakończeniu roku, w którym zgłoszenie zostało przekazane do organu publicznego właściwego do podjęcia działań następczych, lub też działania te zostały zakończone lub też po zakończeniu postępowań zainicjowanych tymi działaniami.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl