Urząd Ochrony Danych Osobowych

NEWSLETTER
UODO DLA INSPEKTORÓW OCHRONY DANYCH

Obserwuj nas także na:

Numer 6/2019 (6)
Wrzesień 2019

Podstawy przetwarzania i okresy przechowywania danych uczestników pracowniczych planów kapitałowych (PPK)

Dane identyfikujące uczestników PPK w postaci adresu e-mail i numeru telefonu osoby zatrudnionej, pracodawcy powinni przekazywać na podstawie zgody tej osoby. Co więcej przekazywanie danych osobowych pracowników w związku z tworzeniem, wdrażaniem i prowadzeniem pracowniczych planów kapitałowych musi odbywać się z poszanowaniem zasady ograniczenia przechowywania danych osobowych bez względu na podstawę zatrudnienia. W przypadku dokumentacji dotyczącej uczestnika PPK okres jej przechowywania, zgodnie z przepisami prawa, wynosi 10 lat.

W dniu 1 stycznia 2019 r. zaczęła obowiązywać ustawa o pracowniczych planach kapitałowych zobowiązująca pracodawców do terminowego wdrożenia PPK. Do 26 września pracodawcy zatrudniający co najmniej 250 osób powinni zawrzeć umowy o zarządzenie PPK. Ponieważ okazało się, że nowe przepisy mogą rodzić wątpliwości pracodawców co do podstaw prawnych przetwarzanych danych oraz okresów ich przechowywania, Prezes UODO - w odpowiedzi na kierowane do niego pytania - przedstawił swoje stanowisko w tym zakresie.

Wskazał, że przepisy regulujące funkcjonowanie PPK wskazują otwarty katalog informacji, które należy przekazać w związku z umową o prowadzenie PPK. Wśród tych informacji wymieniono „dane identyfikujące uczestnika PPK". Na gruncie tej ustawy „danymi identyfikującymi uczestnika PPK" mogą być: imię (imiona), nazwisko, adres zamieszkania, adres do korespondencji, numer telefonu, adres poczty elektronicznej, numer PESEL lub data urodzenia w przypadku osób nieposiadających numeru PESEL, seria i numer dowodu osobistego lub numer paszportu albo innego dokumentu potwierdzającego tożsamość w przypadku osób, które nie posiadają obywatelstwa polskiego. W oparciu o umowę o prowadzenie PPK pracodawca przekazuje dane identyfikujące uczestnika PPK, czyli osoby przez siebie zatrudnionej (w tym również dane o numerze telefonu i adresie poczty elektronicznej). Pozyskiwanie danych przez pracodawcę danych pracowników w postaci numeru telefonu i adresu poczty elektronicznej nie wynika z przepisów ustawy o PPK, ani z przepisów Kodeksu pracy. Co więcej, pracodawca może nie posiadać takich danych. Poza tym brak jest w polskim porządku prawnym przepisów zobowiązujących osoby fizyczne do posiadania numeru telefonu i poczty elektronicznej i w związku z tym należy zachować prawo do dobrowolności posiadania takich środków komunikacji i ich ujawniania.

Prezes UODO podkreślił, że dane pracownika, który będzie uczestnikiem PPK, przekazywane w umowie o prowadzenie PPK mają go identyfikować. Natomiast dane takie jak numer telefonu i adres poczty elektronicznej są to dane

W numerze m.in.:

Szkolenia UODO dla inspektorów ochrony danych

Transmisje z wydarzeń organizowanych przez UODO

Wydania archiwalne

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
kancelaria@uodo.gov.pl
godziny pracy urzędu 8:00-16:00

służące do szybszego – niż za pośrednictwem poczty tradycyjnej – kontaktu z osobą fizyczną. Zatem to nie przepis prawa powinien być podstawą do zbierania takich danych tylko udzielona przez pracownika zgoda, której warunki udzielenia muszą odpowiadać art. 22^{1a} Kodeksu pracy oraz art. 6 ust. 1 lit. a RODO. Nie jest przy tym istotne czy dane zostaną zebrane przed, czy po zawarciu umowy o zarządzanie PPK. Ważny jest cel ich pozyskiwania, którym nie powinna być identyfikacja uczestnika PPK w sytuacji kiedy będzie on już identyfikowany numerem PESEL lub serią i numerem dowodu osobistego lub numerem paszportu albo innego dokumentu potwierdzającego tożsamość oraz spełnienie wobec pracownika obowiązku informacyjnego z art. 13 RODO. Dodatkowo trzeba pamiętać, że w sytuacji, w której przedmiotowe dane nie będą już niezbędne do celu w jakim zostały zebrane powinny zostać usunięte (cofnięcie zgody na przetwarzanie danych, rezygnacja z dokonywania wpłat do PPK).

Co do okresu przechowywania dokumentacji dotyczącej uczestnika PPK Prezes UODO wyjaśnił, że w przepisach ustawy o PPK brak jest regulacji w tym zakresie. Kwestia ta nie została też szczegółowo uregulowana również w przepisach wykonawczych odnośnie dokumentacji pracowniczej. Należy jednak mieć na uwadze, że instytucja PPK jest ściśle powiązana z dokumentacją dotyczącą ustalania wymiaru wynagrodzenia, zatem okres przechowywania takiej dokumentacji wynosił będzie 10 lat, zgodnie z przepisami ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (art. 125a ust. 4a). Obowiązek prowadzenia przez pracodawcę dokumentacji pracowniczej dotyczącej wypłaconego wynagrodzenia reguluje też § 6 pkt 3 rozporządzenia w sprawie dokumentacji pracowniczej. Ponadto art. 94 ust. 9b Kodeksu pracy nakłada na pracodawcę obowiązek przechowywania dokumentacji pracowniczej przez okres zatrudnienia, a także przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł, chyba że odrębne przepisy przewidują dłuższy okres przechowywania dokumentacji pracowniczej.

W związku z powyższym słuszne będzie stosowanie takich samych zasad przechowywania dokumentacji uczestnika PPK niezależnie od formy jego zatrudnienia.

treść ustawy

Szkoły mają obowiązek udostępniać sprawdziany uczniowi i jego rodzicom

Do Prezesa UODO docierają sygnały, że nie zawsze obowiązek ten jest realizowany, a uczniowie i ich rodzice mają trudności w otrzymaniu sprawdzonych prac w celu ich przeanalizowania.

Sprawdzone i ocenione pisemne prace ucznia muszą być obligatoryjnie udostępniane uczniowi i jego rodzicom. Obowiązek udostępniania prac wynika nie tylko wprost z art. 44e ust. 4 ustawy o systemie oświaty, ale również stanowi realizację jednej z głównych funkcji, jaką pełni ocena pracy ucznia dokonywana przez nauczyciela. Realizowanie tego obowiązku ma bardzo duże znaczenie w procesie edukacyjnym. Możliwość zapoznania się i przeanalizowania sprawdzonej pracy pozwala uczniowi dowiedzieć się nie tylko jaką ocenę otrzymał, ale też w jakim stopniu opanował wymaganą wiedzę lub umiejętności, co zrobił źle i dlaczego. W ten sposób dowiaduje się, co jeszcze wymaga jego pracy i poprawy. Dzięki temu uczeń i jego rodzice uzyskują niezbędne wskazówki i informacje na temat trudności ucznia oraz jego osiągnięć i postępów.

Sposób udostępnienia dokumentacji powinien określać statut szkoły, co jednak nie oznacza, że szkoła może dowolnie uregulować te kwestie. Skoro art. 44e ust. 4 ustawy o systemie oświaty stanowi, że sprawdzone i ocenione prace pisemne ucznia są udostępniane uczniowi i jego rodzicom - oznacza to, że uczeń i jego rodzice nie muszą zwracać się do nauczyciela z wnioskiem o udostępnienie pracy (tak stanowiły poprzednio obowiązujące przepisy). Nauczyciel ma obowiązek udostępnić sprawdzone i ocenione bieżące prace pisemne. Zgodnie z oficjalnym stanowiskiem Ministerstwa Edukacji Narodowej sposób udostępniania pisemnych prac uczniów określony w statucie powinien umożliwiać szybkie zapoznanie się przez ucznia bądź jego rodziców z treścią pisemnej pracy ucznia np.: przez przekazanie zainteresowanym oryginału pracy lub jego kopii, udostępnienie

Dyrektywa PSD2 zwiększa bezpieczeństwo elektronicznych transakcji bankowych

W Polsce 20 czerwca 2018 r. weszły w życie zmiany wprowadzone m.in. do ustawy o usługach płatniczych, które w zakresie swojej regulacji wdrażają dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, tzw. dyrektywa PSD2. Jedna ze zmian zobowiązuje dostawców usług płatniczych do stosowania od 14 września 2019 r. tzw. silnego uwierzytelnienia (SCA, z ang. Strong Customer Authentication), m.in. w przypadku, gdy uzyskujemy dostęp do swojego rachunku w trybie on-line oraz inicjujemy transakcję płatniczą. Główną przesłanką wprowadzonych zmian jest podniesieniu poziomu bezpieczeństwa korzystania z usług płatniczych oferowanych drogą elektroniczną i tym samym ograniczenie możliwości wystąpienia oszustw związanych z tymi usługami.

Silne uwierzytelnianie opiera się na zastosowaniu co najmniej dwóch z niżej wymienionych elementów:

- wiedza (np. kod PIN, hasło),
- posiadanie (np. karta płatnicza, telefon z kartą SIM),
- cecha klienta (specyficzna dla klienta, np. biometryczna w postaci odcisku palca czy układ żył).

Istotne jest, by wybrane elementy były niezależne od siebie, tj. naruszenie jednego elementu nie osłabiało wiarygodności drugiego (np. na karcie płatniczej nie należy umieszczać nr PIN).

treść dyrektywy

treść ustawy

pracy do domu z prośbą o zwrot pracy podpisanej przez rodziców. Udostępnianie prac do wglądu tylko na terenie szkoły (np. w czasie organizowanych przez szkołę spotkań z rodzicami) nie spełnia warunku swobodnego dostępu rodziców ucznia do informacji o postępach i trudnościach w nauce ich dziecka. Określony przez szkołę sposób udostępniania sprawdzonych prac musi być w pełni akceptowany przez uczniów i ich rodziców, jako pełnoprawnych uczestników procesu kształcenia (na co m.in. wskazuje MEN).

Prawo dostępu do danych osobowych zawartych w sprawdzonych pisemnych pracach wynika również z przepisów RODO. Zgodnie z jego art. 15 administrator jest obowiązany udzielić dostępu do przetwarzanych danych osobie, której one dotyczą, jeśli zgłosi ona takie żądanie. Osoby, których dane dotyczą (w tym przypadku uczniowie i ich rodzice) mają zatem prawo uzyskania od administratora potwierdzenia, czy przetwarza on jego dane osobowe, a jeśli tak jest, to może żądać dostępu do tych danych oraz ich kopii. Warto pamiętać, że - jak rozstrzygnął Europejski Trybunał Sprawiedliwości w wyroku z dnia 20 grudnia 2017 r. C-434/16 Peter Nowak przeciwko Data Protection Commissioner - pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe. ETS przypomina, że dane osobowe stanowią wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej zaś o osobie możliwej do zidentyfikowania możemy mówić wówczas gdy jej tożsamość można ustalić bezpośrednio lub pośrednio. Według ETS pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu stanowią informacje dotyczące tej osoby ze względu na ich treść, cel czy skutek. Trybunał w swoim orzeczeniu odniósł się również do komentarzy, które w treści egzaminu pozostawia osoba go oceniająca, wskazując że stanowią one, tak jak udzielone na egzaminie przez przystępującą do niego osobę odpowiedzi, informacje dotyczące tej właśnie osoby.

treść wyroku

Jednakże wobec istnienia w ustawie o systemie oświaty obowiązku udostępniania sprawdzonych prac w niemalże każdym przypadku i z inicjatywy szkoły, uczniowie nie powinni być zmuszeni korzystać z uprawnienia określonego w art. 15 RODO. Przy czym wyjątkiem od tej zasady są egzaminy pisemne, w przypadku których tryb udostępniania prac został uregulowany odrębnie, np. wgląd do arkuszy egzaminu maturalnego określa art. 44zzz ustawy o systemie oświaty.

Obwieszczenie o licytacji komorniczej nie na klatce schodowej

Spółdzielnia nie ma prawa upubliczniać na drzwiach wejściowych do klatek schodowych obwieszczenia o licytacji komorniczej nieruchomości, które zawiera dane osobowe dłużnika.

Do spółdzielni, która postąpiła w ten sposób, Prezes UODO skierował wystąpienie, wskazując, że taka sytuacja nie powinna mieć miejsca. Jednocześnie zwrócił się o podjęcie działań mających na celu, m.in. niedopuszczenie do podobnych sytuacji w przyszłości.

W wystąpieniu Prezes UODO przypomniał, że kwestia doręczania i upubliczniania obwieszczenia o licytacji została uregulowana w art. 954 i 955 Kodeksu postępowania cywilnego. Podkreślił, że z powołanych przepisów nie wynika, by spółdzielnia miała obowiązek bądź uprawnienie do upublicznienia obwieszczenia o licytacji lokalu, wchodzącego w skład jej zasobów. Przepisy te jednoznacznie określają miejsca, w jakich obwieszczenie jest ogłaszane – nie wymieniono wśród nich budynków należących do stron czy uczestników postępowania egzekucyjnego. Żaden z przepisów prawa powszechnie obowiązującego nie zezwala spółdzielni na upublicznianie obwieszczenia o licytacji poprzez ich wywieszanie na klatkach schodowych budynków spółdzielni. Dodać należy, że są to miejsca ogólnodostępne, więc wywieszanie tam obwieszczeń o licytacji, które zawierają dane osobowe dłużników, stwarza możliwość zapoznania się z tymi danymi przez wiele przypadkowych, nieupoważnionych do tego osób. Narusza więc postanowienia RODO.

Takie działanie naraża dłużnika i jego rodzinę na szykany i agresywne zachowania ze strony mieszkańców osiedla. Może też stanowić naruszenie dóbr osobistych.

Odpowiadając na wystąpienie Prezesa UODO spółdzielnia poinformowała o zaprzestaniu kwestionowanych działań. Wskazała również, że przeprowadziła audyt w zakresie ochrony danych osobowych, a wszystkich swoich pracowników przeszkoliła z obowiązujących w tym zakresie przepisów. Powołała też inspektora ochrony danych, z którym konsultuje wszystkie kwestie związane z przetwarzaniem danych osobowych.

Transmitując sesje rady gminy i udostępniając informacje publiczne, trzeba chronić dane osobowe

Przeprowadzenie wewnętrznego audytu, opracowanie szczegółowej instrukcji anonimizacji dokumentów oraz przeszkolenie przez inspektora ochrony danych (IOD) pracownika zajmującego się obsługą biura rady miasta to tylko niektóre z działań podjętych przez jedną z gmin na skutek wystąpienia Prezesa UODO.

Zostało ono skierowane w związku z udostępnieniem w Biuletynie Informacji Publicznej (BIP) niezanonimizowanych bądź nieprawidłowo zanonimizowanych danych osobowych osób, które skierowały do rady miasta skargę na działalność sołtysa. Na stronie BIP umieszczona została niezanonimizowana retransmisja sesji rady, a także niewłaściwie zanonimizowana uchwała rady miasta podjęta w związku ze skargą na sołtysa. Reagując na te nieprawidłowości, Prezes UODO w wystąpieniu wskazał, że transmitując sesje rady gminy oraz umieszczając w BIP ich retransmisje, a także związane z nimi dokumenty, pamiętać należy o zasadach określonych w RODO, a także w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej.

Po tym zdarzeniu, w gminie szczegółowo przeanalizowano jego przyczyny i podjęto takie mające im zapobiegać w przyszłości działania, jak m.in.:

- przeprowadzenie wewnętrznego audytu jakości, w czasie którego sprawdzono m.in. poziom wiedzy pracowników w zakresie przyjętych w urzędzie polityk i instrukcji przetwarzania danych osobowych, z uwzględnieniem anonimizacji dokumentów udostępnianych w BIP,
- przeszkolenie przez inspektora ochrony danych (IOD), pracownika zajmującego się obsługą biura rady miasta, ze szczególnym uwzględnieniem zagadnień dotyczących ochrony danych osobowych w czasie posiedzeń sesji i komisji rady, ograniczeń w udostępnianiu informacji publicznej wynikających z art. 5 ust. 1-2a ustawy o dostępie do informacji publicznej, zasad i sposobów anonimizacji dokumentów udostępnianych w BIP,
- opracowanie instrukcji, opisującej, jak w praktyce krok po kroku zastosować metodę anonimizacji danych osobowych w dokumentach w formie tradycyjnej oraz elektronicznej, i udostępnienie jej pracownikom w bazie wiedzy Help Desk,
- wprowadzenie zasady dwupoziomowej weryfikacji anonimizacji.

Udostępnianie danych osobowych przez OPS

Czy ośrodek pomocy społecznej (OPS) może udostępnić posiadane dane osobowe – to częste pytanie, z jakim przedstawiciele tych jednostek zwracają się do UODO, wymieniając przy tym nazwy konkretnych instytucji, które o przekazanie takich danych wnioskują. Reprezentanci OPS wskazują, że ze względu na ustanowioną w art. 100 ust. 1 ustawy z dnia 12 marca 2004 r. o pomocy społecznej i wiążącą ich tajemnicę zawodową, mają wątpliwości, czy takie udostępnienie jest uprawnione.

Należy pamiętać, że kady wniosek o udostepnienie danych wymaga indywidualnej analizy. Rozpatrujący go administrator, który podejmuje ostateczną decyzję w tej sprawie, musi wziąć przy tym pod uwagę: obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie, w tym wskazanie przez niego podstawy prawnej żądania.

Podkreślić należy, że w przypadku, gdy o udostępnienie danych osobowych występuje podmiot publiczny, powinien w pierwszej kolejności wyraźnie wskazać podstawę prawną takiego żądania w postaci przepisów sektorowych. Podmioty publiczne są bowiem zobowiązane działać wyłącznie na podstawie i w granicach prawa, co zostało unormowane w art. 7 Konstytucji RP. W opinii UODO, występowanie z wnioskiem o udostępnienie danych osobowych wyłącznie na podstawie przepisów RODO nie znajduje uzasadnienia prawnego, ponieważ podstawą kompetencji i zadań realizowanych przez organy publiczne nie są unormowania RODO, lecz przepisy krajowe stanowiące o kompetencjach tych organów i sposobie ich realizacji. Zatem takie podmioty w pierwszej kolejności powinny wskazywać przepisy szczególne, na podstawie których działają, a następnie w ich świetle przesłanki z RODO.

Zatem przedstawiciele OPS słusznie powołują się na art. 100 ustawy o pomocy społecznej. Wynika bowiem z niego niedopuszczalność ujawniania informacji z postępowań administracyjnych prowadzonych przez ośrodki pomocy społecznej na rzecz wszelkich podmiotów, w tym innych organów administracji publicznej – o ile nie ma wyraźnej podstawy ustawowej. Dlatego w ocenie UODO, podmioty publiczne wnioskujące o udostępnienie danych

osobowych nie mogą powoływać się jedynie na niezbędność przetwarzania danych do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (tj. przesłankę z art. 6 ust. 1 lit. e RODO), bez jednoczesnego wskazania krajowych, sektorowych przepisów rangi ustawy, stanowiących podstawę realizacji ich zadań i określających cel przetwarzania. Natomiast gdy udzielenia informacji żąda od OPS sąd prowadzący postępowanie cywilne, pod uwagę należy wziąć art. 248 § 1 Kodeksu postępowania cywilnego, który stanowi, że każdy obowiązany jest przedstawić na zarządzenie sądu w oznaczonym terminie i miejscu dokument znajdujący się w jego posiadaniu i stanowiący dowód faktu istotnego dla rozstrzygnięcia sprawy, chyba że dokument zawiera informacje niejawne. Zatem w tym przypadku zastosowanie znajdzie przesłanka z art. 6 ust. 1 lit. c RODO, zgodnie z którą przetwarzanie danych osobowych jest zgodne z prawem, jeśli jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Problemy z zakresu ochrony danych osobowych administrator najpierw powinien konsultować z IOD

Wiele podmiotów, mających wątpliwości co do zastosowania w konkretnych przypadkach przepisów RODO, z pytaniami w takich sprawach zwraca się wprost do UODO. Niesłusznie pomija przy tym swojego inspektora ochrony danych (IOD). Tymczasem IOD, zgodnie z przyjętymi w RODO rozwiązaniami, ma być nie tylko doradcą dla administratora, ale także pełnić rolę punktu kontaktowego, a więc m.in. być pośrednikiem między nim a organem nadzorczym.

Inspektorzy ochrony danych, dysponujący odpowiednią wiedzą i umiejętnościami, mają stanowić fundament nowego, skutecznego systemu ochrony danych osobowych. Wiele podmiotów jest wręcz zobowiązanych do ich powołania. Grupa Robocza Art. 29 w swoich Wytycznych dotyczących inspektorów ochrony danych, rekomenduje wyznaczenie inspektora nawet przez podmioty do tego niezobowiązane, gdyż – jak zaznacza – „może on znacznie ułatwić przestrzeganie nowych przepisów oraz odegrać istotną rolę w pośredniczeniu pomiędzy zainteresowanymi stronami (organem ochrony danych osobowych, podmiotami danych oraz poszczególnymi jednostkami w ramach jednej organizacji)". Nikt bowiem lepiej niż IOD nie zna struktury i praktyk stosowanych w danej organizacji oraz branżowych przepisów prawa, które jest ona zobowiązana stosować.

Dlatego w budzących wątpliwości sytuacjach związanych z przetwarzaniem danych osobowych, administrator w pierwszej kolejności powinien zwrócić się do IOD. To jego zadaniem jest poddanie danego przypadku szczegółowej analizie i przedstawienie opinii na ten temat.

W uzasadnionych przypadkach to IOD może zwrócić się do UODO z prośbą o konsultacje. Zgodnie bowiem z art. 57 ust. 3 RODO, zadaniem organu nadzorczego jest bezpłatne wypełnianie zadań na rzecz osoby, której dane dotyczą, i – gdy ma to zastosowanie – inspektora ochrony danych. Co więcej - w Wytycznych Grupa Robocza Art. 29 odczytuje art. 39 ust. 1 lit. e RODO jako adresowany również do organów nadzorczych i zobowiązujący je do udzielania konsultacji i wskazówek inspektorom ochrony danych w stosownych przypadkach.

Trzeba jednak pamiętać, że często wiążące zaopiniowanie przez UODO konkretnych rozwiązań wyłącznie na podstawie przesłanej korespondencji, która dodatkowo w niepełny sposób opisuje ewentualne czynności wykonywane na danych osobowych, nie jest możliwe. Co do zasady Prezes UODO - stosownie do zadań określonych w art. 57 RODO - bada i kontroluje procesy przetwarzania danych osobowych w ramach prowadzonych postepowań administracyjnych. Jego wiążące stanowisko w konkretnej sprawie dotyczącej przetwarzania danych osobowych powinno być zawarte w treści decyzji administracyjnej, na podstawie zebranego materiału dowodowego.

Uwagi UODO do projektu ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw

Prezes UODO zakwestionował rozwiązania w projekcie ustawy o zmianie ustawy – Prawo energetyczne oraz niektórych innych ustaw (zwanym dalej projektem) dotyczące m.in. inteligentnego opomiarowania (liczniki pomiaru energii instalowane u odbiorców).

Inteligentne liczniki są instalowane w mieszkaniach odbiorców energii i posiadają zdolność dwustronnej komunikacji. Informują konsumentów o ilości zużywanej energii przy czym informacja ta może być również przekazywana dostawcom energii i innym wyznaczonym podmiotom. Kluczową cechą inteligentnych liczników jest możliwość zdalnej komunikacji pomiędzy licznikiem i upoważnionymi podmiotami, takimi jak dostawcy, operatorzy sieci, upoważnione osoby trzecie lub przedsiębiorstwa usług energetycznych. Informacje zbierane

od odbiorców końcowych przy pomocy liczników pozwalają zbudować profil użytkownika w zakresie ilości zużywanej energii i tym samym uzyskiwać szczegółowe informacje o jego zachowaniach. Podmioty, którym przekazywane są informacje z liczników mają wiedzę o tym w jakich ilościach i kiedy użytkownik zużywa energię co pozwala na ustalenie np. w jakich godzinach użytkownik pracuje, jak dużo posiada sprzętów elektrycznych etc.

Obawy Prezesa UODO budzi ryzyko profilowania użytkowników takich liczników, które w odstępach piętnastominutowych będą informowały dostawców o ilości i sposobach wykorzystywanej energii. Takie informacje pozwalają na stworzenie profilu osoby, jej zachowań, przyzwyczajeń, tj. w jakich godzinach pracuje, kiedy, ile i na co zużywa energii elektrycznej.

Projektodawca przyjął, że celem stosowania liczników zdalnego odczytu nie jest profilowanie odbiorców końcowych jakimi są gospodarstwa domowe. Jednakże ryzyko profilowania osób w związku z instalacją inteligentnych liczników w ocenie Prezesa UODO zdecydowanie zachodzi. Profilowanie nie musi być bowiem głównym celem działania systemu, może zaś zachodzić przy okazji jego użytkowania.

Ponadto Prezes UODO nie zgodził się ze stwierdzeniem, że przy zastosowaniu inteligentnych liczników nie dochodzi do podejmowania zautomatyzowanych decyzji. Informacje gromadzone w ramach usługi inteligentnego pomiaru dotyczą profilu energetycznego konsumenta wynikającego z jego sposobu użytkowania energii i służą do podejmowania decyzji bezpośrednio go dotyczących. Taka decyzja w najbardziej oczywisty sposób dotyczy kształtowania poziomu opłat za dostawy energii, przy czym nie ogranicza się tylko do fakturowania.

Prezes UODO wskazał, że projekt ten wymaga ponownej analizy i rozważenia wprowadzenia zmian w proponowanym przez niego zakresie.

treść uwag

Wystąpienie Prezesa UODO do Ministra Finansów w sprawie tzw. „rachunków uśpionych”

Prezes UODO ponownie zwrócił się do Ministra Finansów o podjęcie działań mających na celu wprowadzenie zmian w ustawie z dnia 29 sierpnia 1997 r. Prawo bankowe i ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, zapewniających zgodność unormowań dotyczących tzw. „rachunków uśpionych” z przepisami o ochronie danych osobowych.

Prezes UODO zwrócił uwagę, że przepisy wyżej wymienionych ustaw nakładają na banki i spółdzielcze kasy oszczędnościowo-kredytowe obowiązek przekazywania gminom szeregu informacji objętych tajemnicą bankową albo tajemnicą zawodową, w tym również danych osobowych, których przetwarzanie przez gminy nie znajduje uzasadnienia. Stwarza to ryzyko nadmiarowego przetwarzania danych osobowych przez gminy.

Obowiązek przekazywania przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminom informacji o posiadaczu rachunku (art. 111c ustawy Prawo bankowe i art. 13c ustawy o spółdzielczych kasach oszczędnościowo-kredytowych) dotyczy zarówno przypadku rozwiązania umowy rachunku z powodu śmierci posiadacza rachunku bankowego (śmierci członka spółdzielczej kasy oszczędnościowo-kredytowej posiadającego imienny rachunek), jak i wygaśnięcia umowy rachunku ze względu na długotrwały brak aktywności posiadacza tego rachunku. W przypadku rozwiązania umowy rachunku z powodu śmierci posiadacza albo członka spółdzielczej kasy oszczędnościowo-kredytowej informowanie gminy i przekazywanie jej pewnych informacji przez banki i spółdzielcze kasy oszczędnościowo-kredytowe można uznać za uzasadnione, gdyż gmina może stać się spadkobiercą koniecznym takiego posiadacza na podstawie art. 935 zdanie pierwsze i art. 1023 § 1 Kodeks cywilny. W przypadku zaś wygaśnięcia umowy rachunku z powodu długotrwałego braku aktywności posiadacza rachunku albo członka spółdzielczej kasy oszczędnościowo-kredytowej przekazywanie przez banki i spółdzielcze kasy oszczędnościowo-kredytowe gminie jakichkolwiek informacji o posiadaczu takiego rachunku nie jest prawidłowe, gdyż nie ma podstaw do stwierdzenia, że posiadacz rachunku (członek spółdzielczej kasy oszczędnościowo-kredytowej) zmarł, a zatem gmina nie jest w takiej sytuacji nawet potencjalnym spadkobiercą.

Również zakres informacji udostępnianych gminie w naszej ocenie jest zbyt szeroki. O ile sama informacja o śmierci posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) może być gminie potrzebna do przeprowadzenia postępowania spadkowego, to brak jest podstaw, by informować gminę o dacie wydania przez posiadacza rachunku (członka spółdzielczej kasy oszczędnościowo-kredytowej) ostatniej dyspozycji dotyczącej tego rachunku, wysokości środków pieniężnych zgromadzonych na rachunku oraz kwotach i tytułach wypłat dokonanych z rachunku, a także źródle i podstawie dokonanych ustaleń. Poza tym ustawodawca nie dookreślił w przepisach, jaki okres wstecz powinna obejmować informacja o kwotach i tytułach wypłat dokonanych z rachunku.

treść pisma

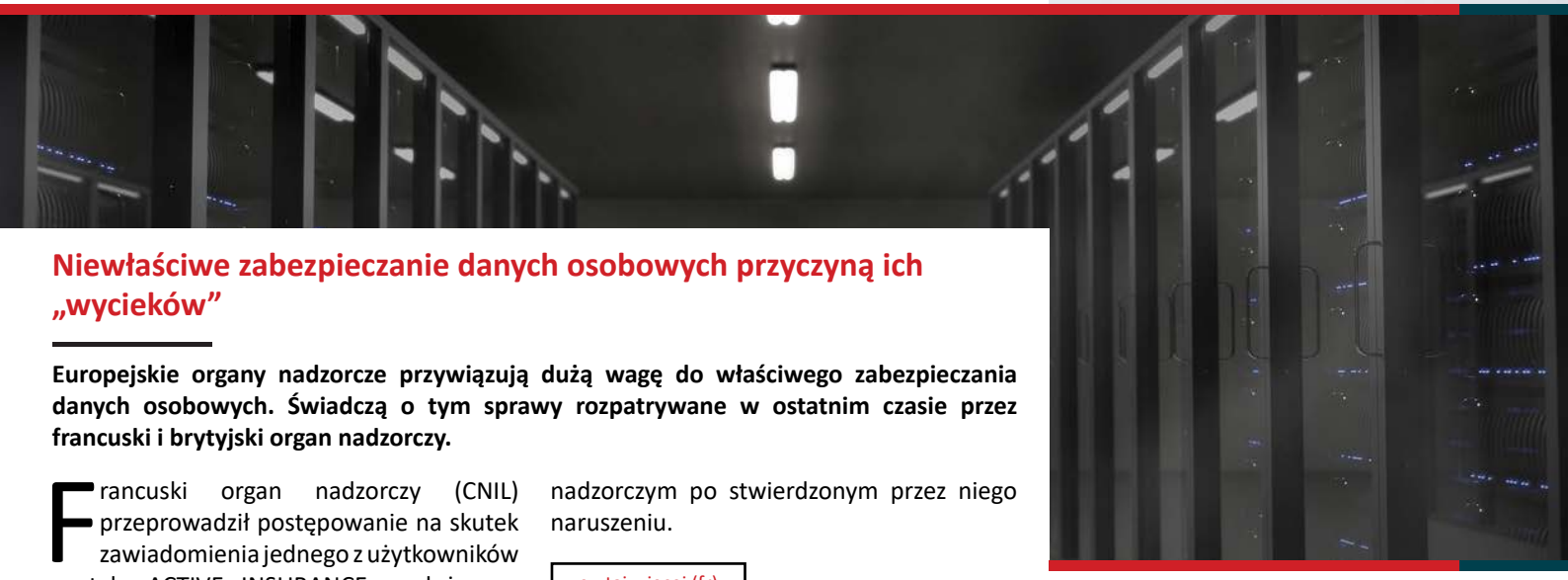
Nieprawidłowa podstawa przetwarzania danych pracowników przedmiotem postępowania greckiego organu nadzorczego

Grecki organ ds. ochrony danych w związku ze skargą przeprowadził z urzędu postępowanie w sprawie zgodności z prawem przetwarzania danych osobowych pracowników zatrudnionych w spółce „PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS SA" (PWC BS), którzy - jak wynikało ze skargi - byli zobowiązywani do wyrażania zgody na przetwarzanie ich danych osobowych.

Po przeprowadzeniu postępowania grecki organ nadzorczy uznał, że spółka niezgodnie z zasadami określonymi w art. 5 ust. 1 RODO przetwarzała dane osobowe swoich pracowników z powołaniem się na art. 6 ust. 1 lit. a RODO (przetwarzanie na podstawie zgody), w sytuacji gdy przetwarzanie miało na celu wykonywanie czynności bezpośrednio związanych z wykonywaniem umowy o pracę. Zobowiązywała swoich pracowników do podpisania oświadczeń, że ich dane osobowe są przetwarzane i przechowywane w związku ze stosunkiem pracy. Spowodowało to błędne przekonanie pracowników, że przetwarzanie ich danych osobowych odbywa się na podstawie ich zgody, podczas gdy w rzeczywistości przetwarzanie odbywało się na innej podstawie prawnej, o której pracownicy nigdy nie zostali poinformowani. Ponadto Spółka nie wywiązała się z obowiązku dostarczenia wewnętrznej dokumentacji dotyczącej wyboru zastosowanej podstawy prawnej przetwarzania danych osobowych, o które zwracał się do niej organ nadzorczy, co m.in. zostało ocenione jako naruszenie zasady rozliczalności.

Po stwierdzeniu ww. naruszeń grecki organ nakazał spółce, aby w ciągu trzech miesięcy doprowadziła do zgodnego z przepisami RODO przetwarzania danych osobowych swoich pracowników z uwzględnieniem zasad wynikających z art. 5 RODO. Nałożył również karę w wysokości 150000 EUR.

treść orzeczenia



Niewłaściwe zabezpieczanie danych osobowych przyczyną ich „wycieków"

Europejskie organy nadzorcze przywiązują dużą wagę do właściwego zabezpieczania danych osobowych. Świadczą o tym sprawy rozpatrywane w ostatnim czasie przez francuski i brytyjski organ nadzorczy.

Francuski organ nadzorczy (CNIL) przeprowadził postępowanie na skutek zawiadomienia jednego z użytkowników portalu ACTIVE INSURANCE – służącego do świadczenia usług ubezpieczeniowych. Okazało się, że portal umożliwia uzyskanie nieuprawnionego dostępu do danych osobowych innych klientów, w tym m.in. do kopii ich prawa jazdy.

CNIL uznał, że spółka naruszyła art. 32 RODO poprzez niewłaściwe zabezpieczenie danych osobowych. W swoim rozstrzygnięciu wskazał między innymi na konieczność używania przez użytkowników portalu silniejszych haseł i nieprzekazywania ich przez spółkę niezabezpieczonym odpowiednio e-mailem.

Organ decydując o wymierzeniu kary w wysokości 180 000 euro uwzględnił wagę naruszenia w tym charakter danych, liczbę poszkodowanych osób (kilku tysięcy klientów) oraz reakcję spółki na informację o naruszeniu i współpracę z organem nadzorczym po stwierdzonym przez niego naruszeniu.

czytaj więcej (fr)

Natomiast brytyjski organ nadzorczy przeprowadził postępowanie wobec agencji nieruchomości Life at Parliament View Ltd (LPVL) w sprawie naruszenia ochrony danych osobowych jej klientów. Naruszenie ochrony danych polegało na błędnej konfiguracji systemu – nie wyłączono funkcji „uwierzytelniania anonimowego" – przy przekazywaniu danych klientów między agencją a innym podmiotem. Na skutek niewdrożenia ograniczeń dostępu, każdy użytkownik Internetu mógł mieć wgląd do wszystkich przechowywanych danych. Z ustaleń ICO wynikało, że naruszenie miało miejsce w okresie między marcem 2015 r. a lutym 2017 r. i dotyczyło 18 610 osób. Na skutek naruszenia doszło do ujawnienia takich danych klientów jak: wyciągi bankowe, dane dotyczące wynagrodzeń, kopie paszportów, daty urodzenia, prawa jazdy oraz adresy.

W wyniku postępowania ICO wskazał na szereg błędów w zakresie bezpieczeństwa i stwierdził, że LPVL nie podjęła odpowiednich środków technicznych i organizacyjnych przeciwko nieuprawnionemu dostępowi do przetwarzanych danych osobowych. Ponadto LPVL powiadomiła ICO o naruszeniu wówczas, gdy skontaktował się z nią haker. Z uwagi na wagę naruszenia ochrony danych osobowych ICO zdecydował o nałożeniu na kary pieniężnej w wysokości 80 000 GBP.

komunikat ICO (en)

decyzja ICO (en)

Przetwarzanie danych biometrycznych dzieci może wiązać się z wysokim ryzykiem

Szkoła w Skellefteå w Szwecji wprowadziła system monitoringu wizyjnego rozpoznającego twarze do odnotowywania obecności uczniów na lekcjach. Celem wdrożenia przez szkołę nowej technologii było usprawnienie i uproszczenie ustalania frekwencji na lekcjach.

Rozwiązanie to spotkało się z reakcją szwedzkiego organu nadzorczego, który stwierdził, że o ile przetwarzanie danych w celu sprawdzenia obecności uczniów jest uzasadnione, to rozpoznawanie ich twarzy jest nieproporcjonalne w stosunku do tego celu. Wskazał dodatkowo, że doszło do przetwarzania danych biometrycznych, a zatem zastosowanie powinien mieć art. 9 RODO. Przy czym w tym konkretnym przypadku szkoła nie może powoływać się na którykolwiek z wymienionych w art. 9 ust. 2 RODO wyjątków od zakazu przetwarzania takich danych.

Ponadto organ ochrony danych stwierdził, że - z uwagi na zastosowaną nową technologię do przetwarzania szczególnie chronionych danych osobowych dzieci - miało miejsce przetwarzanie danych powodujące wysokie ryzyko naruszenia praw i wolności osób fizycznych, a szkoła nie była w stanie wykazać zgodności z art. 35 RODO (nie przeprowadziła oceny skutków dla ochrony danych) oraz nie skonsultowała swojego zamiaru z organem nadzorczym zgodnie z art. 36 ust. 1 RODO.

Z powyższych powodów szwedzki organ ochrony danych nałożył karę w wysokości 200.000 koron szwedzkich za naruszenie art. 5, 9, 35 i 36 RODO. Na stosunkowo niewielką wysokość kary miał wpływ, m.in. krótki okres wykorzystywania systemu (3 tygodnie) oraz niewielka liczba uczniów, których dane biometryczne znalazły się w bazie (22 osoby).

treść orzeczenia

Nowe odpowiedzi w zakładce „Inspektor Ochrony Danych”

Do funkcjonującej na naszej stronie zakładki „Inspektor Ochrony Danych”/„Zadania IOD” dodaliśmy nowe zagadnienia. Dotyczą one następujących kwestii:

- Kiedy administrator może pobrać opłatę za udzielenie informacji osobie, której dane dotyczą?
- Czy w przypadku dożywiania dzieci szkoła musi zawrzeć umowę powierzenia danych z OPS?

UODO w mediach

„Lubię to” czyli popularne w mediach porady UODO w sierpniu

Użycie wtyczki „Lubię to” prowadzi do współadministrowania danymi osobowymi – ta informacja była jedną z najczęściej powtarzanych przez media na podstawie komunikatu Urzędu Ochrony Danych Osobowych w sierpniu 2019 r. Na ten temat ukazało się ponad 300 informacji z ponad 1800, które odnosiły się do różnych działań realizowanych przez urząd w minionym miesiącu.

Przytoczone zdanie pochodzi z komunikatu UODO z 9 sierpnia 2019 r. nt. wyroku TSUE z 29 lipca br. Chętnie cytowały go nie tylko media branżowe, ale także ogólnopolskie. Komunikat zawierał informacje na temat wspomnianego wyroku. Ponadto UODO wskazało, jakie skutki dla podmiotów używających popularnej wtyczki niesie orzeczenie. Warto przypomnieć, że wg TSUE podmioty zamieszczające wtyczkę „Lubię to” na swoich witrynach internetowych są wspólnie z Facebookiem (dostawcą wtyczki społecznościowej) administratorami danych osobowych osób korzystających z witryn takich podmiotów. Jak wyjaśniło UODO, odpowiedzialność tych podmiotów ogranicza się do operacji zbierania danych oraz ich transmisji do Facebooka. Rozstrzygnięcie to ułatwia określenie ról podmiotów biorących udział w procesie przetwarzania danych osobowych.

Nie był to jedyny temat w sierpniu, który zwrócił uwagę dziennikarzy. W dalszym ciągu media informowały m.in. o stanowisku UODO, w którym stwierdzono, że nie ma podstawy prawnej, która umożliwiłaby pracodawcom samodzielną kontrolę pracowników alkomatem.

Ponadto pojawiały się już pierwsze wzmianki o jubileuszowej, X edycji programu edukacyjnego UODO dla szkół „Twoje dane – Twoja sprawa” w związku z rozpoczętym naborem uczestników.

Podsumowując, w sierpniu media poinformowały 1867 razy o działalności Prezesa i Urzędu Ochrony Danych Osobowych. Jak w poprzednich miesiącach informacje te były dostępne głównie w Internecie (1707 wzmianek), a także w prasie (160 wzmianek).

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
kancelaria@uodo.gov.pl
godziny pracy urzędu 8:00-16:00