SK&S PRIVACY INSIGHT

Kwartalnik o prawie ochrony danych osobowych

30 LAT | SK&S SOŁTYSIŃSKI KAWECKI SZLĘZAK

W tym numerze

CZERWIEC 2022 | NUMER 1

Sygnaliści a RODO – projekt ustawy o ochronie osób zgłaszających naruszenia prawa

Sylwia Macura-Targosz
Starszy Prawnik, radca prawny
sylwia.macura-targosz@skslegal.pl
+48 694 415 447

Analizując nowe obowiązki pracodawców wynikające z dyrektywy o ochronie sygnalistów oraz projektu ustawy o ochronie osób zgłaszających naruszenia prawa, nie można zapomnieć o przepisach RODO oraz przetwarzaniu danych osobowych w związku ze zgłoszeniem naruszenia. W procesie tym bowiem pracodawca jest administratorem danych zgromadzonych w trakcie całego procesu, a sygnalista oraz inne osoby wymienione w zgłoszeniu – podmiotem danych.

Opublikowany 12 kwietnia br. (drugi) projekt ustawy o ochronie osób zgłaszających naruszenia prawa ma na celu wdrożeniu unijnej dyrektywy o ochronie sygnalistów. Warto przypomnieć, że Polska zobowiązana była do przyjęcia ww. ustawy do 17 grudnia 2021 r. Obecnie projekt ustawy jest na etapie ponownych uzgodnień międzyresortowych.

Jakie regulacje zawiera obecny projekt ustawy? Na co należy zwrócić uwagę? Co warto byłoby jeszcze uregulować?

- **dane osobowe sygnalisty to nie tylko imię i nazwisko**, ale również *„inne informacje, na podstawie których można bezpośrednio lub pośrednio zidentyfikować tożsamość”* sygnalisty (np. informacje o szczególnym czasie lub miejscu, w którym nastąpiło naruszenie, stanowisko, specyficzne kwalifikacje);

- **podstawą prawną przetwarzania danych osobowych sygnalisty oraz osób wymienionych w zgłoszeniu będzie art. 6 ust. 1 lit. c) RODO,** tj. wypełnienie obowiązków prawnych ciążących na administratorze i taki obowiązek znajdujemy w art. 8 projektu ustawy, zgodnie z którym podmiot zbiera i przetwarza dane w zakresie niezbędnym do realizacji celów ustawy. Niestety projektodawca pomija kwestie przetwarzania danych szczególnych kategorii czy danych dotyczących skazań, które mogą przecież zostać wskazane w zgłoszeniu przez sygnalistę;

- **brak obowiązku administratora przekazania informacji o źródle danych (czyli o tożsamości sygnalisty) – wyłączenie stosowania art. 14 ust. 2 lit. f) RODO;** Projektodawca nie zdecydował się jednak ani na wyłączenie w ogóle obowiązku informacyjnego z art. 14 RODO ani na odsunięcie jego realizacji czasie – należy mieć świadomość, że czasami sama informacja o toczącym się postępowaniu może spowodować, że dalsze działania następcze mogą okazać się bezcelowe;

- **przekazanie informacji o źródle danych na mocy art. 15 RODO** (prawo dostępu do treści danych) w terminie późniejszym niż wynika to z przepisów RODO, nie później jednak niż w terminie 3 miesięcy od dnia zakończenia działań następczych; Projektodawca zdecydował się na odsunięcie w czasie tylko realizacji obowiązku podania informacji o źródle danych (art. 15 ust. 1 lit. g) RODO); pozostałe informacje administrator zobowiązany jest przekazać w terminie wynikającym z RODO;

- **dostęp do danych osobowych tylko dla osób posiadających pisemne upoważnienie do przetwarzania danych osobowych lub podmiotów, z którymi administrator zawarł umowę powierzenia przetwarzania danych osobowych;** zgodnie z przepisami RODO administrator może powierzać przetwarzanie danych wyłącznie podmiotom, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych;

- **dane osobowe przetwarzane w związku ze zgłoszeniem są przechowywane nie dłużej niż przez okres 15 miesięcy od dnia zakończenia działań następczych** (w pierwszym projekcie ustawy okres ten wynosił 5 lat od dnia przyjęcia zgłoszenia).

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii

Pamiętajmy o ogólnych przepisach RODO!

Projektowana ustawa nie zawiera kompleksowych i wyczerpujących regulacji w obszarze ochrony danych osobowych sygnalistów czy osób wskazanych w zgłoszeniu. Tym samym, administratorzy projektując procedury / systemy dotyczące zgłoszeń sygnalistów w obszarze danych osobowych powinni opierać się w dużej mierze na ogólnych przepisach RODO. A zatem, administratorzy nie powinni zapomnieć m.in. o zaktualizowaniu rejestru czynności przetwarzania danych poprzez dodanie nowego procesu czy przeprowadzenie oceny skutków dla ochrony danych osobowych – systemy do zgłaszania nieprawidłowości zostały wprost wskazane przez Prezesa UODO jako te, które wymagają wykonania oceny skutków dla ochrony danych osobowych.

Projekt ustawy można znaleźć tutaj

Kilka słów komentarza do projektu ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji

Jakub Derulski
Prawnik, adwokat
jakub.derulski@skslegal.pl
+48 880 780 275

Projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji został opublikowany 21 kwietnia bieżącego roku i aktualnie jest na wczesnym etapie konsultacji publicznych przed skierowaniem go do Sejmu (szczegóły dotyczące projektu oraz prac legislacyjnych znajdziecie ***tutaj***). Głównym celem projektu jest usunięcie ograniczeń systemowych w rozwoju e-administracji m.in.: poprzez stworzenie ram dostępnego dla wszystkich organów publicznych repozytorium dokumentów, czy usunięcie ograniczeń związanych z rozwojem usług cyfrowych.

Zmiany w sposobie funkcjonowania portalu GOV.PL i systemu EZD

Projekt wprowadza postanowienia regulujące administrowanie portalem GOV.PL oraz Elektroniczne Zarządzanie Dokumentacją (EZD RP). Zgodnie z założeniami twórców projektu Portal GOV.Pl ma dać obywatelom pełny dostęp do zbioru informacji i usług online świadczonych przez administrację publiczną. Natomiast EZD ma umożliwić wykonywanie czynności kancelaryjnych, dokumentowanie przebiegu załatwiania i rozstrzygania spraw oraz gromadzenie i tworzenie dokumentacji w postaci elektronicznej. Efektem zmian będzie stworzenie potężnej i zintegrowanej ze sobą bazy danych, pozwalającej na efektywne wykorzystanie potencjału danych. Tak jak same zmiany należy ocenić bardzo pozytywnie, to już przygotowaną Ocenę wpływu na ochronę danych już nie (więcej o zagrożeniach w części poświęconej ocenie).

Z drugiej strony, precyzyjne wskazanie ministra ds. administracji jako administratora danych zawartych w portalu GOV.Pl jest bardzo dobrym rozwiązaniem, które pozwoli zaoszczędzić czas obywatelom, których dane są przetwarzane np.: poprzez kierowanie wniosku dot. zmiany danych do jednego adresata, a nie do kilku właściwych urzędów.

Zmiany w Ustawie o dowodach osobistych

Szereg daleko idących zmian dotyczy również ustawy o dowodach osobistych. Celem zmian jest zwiększenie skuteczności oraz bezpieczeństwa procesów związanych z ustalaniem tożsamości osób fizycznych. Narzędziem do realizacji celów ma być m.in.: dodanie 2-stopniowej procedury polegającej na weryfikacji danych zawartych w dowodzie osobistym, a następnie weryfikacji opartej na wizerunku twarzy, który będzie przechowywany w Rejestrze Dowodów Osobistych. Przy pozytywnej weryfikacji przewidywane jest generowanie raportu o zgodności danych. Samo rozwiązanie ułatwi działalność podmiotom, szczególnie w sektorze finansowym.

Katalog podmiotów uprawnionych do weryfikacji baz danych

Katalog podmiotów mogących korzystać z rejestru został ograniczony do podmiotów dla których przy wykonywaniu zakresu swoich obowiązków niezbędna jest weryfikacja klienta. W naszej ocenie do przeprowadzenia w sposób precyzyjny tego procesu niezbędne będzie rozszerzenie katalogu, który dodatkowo powinien zawierać: banki krajowe, oddziały banków zagranicznych, instytucje kredytowe i oddziały instytucji kredytowych oraz spółdzielcze kasy oszczędnościowo-kredytowe, które nie prowadzą działalności jako dostawcy usług płatniczych.

Dalsze zmiany przewidziane zostały w ustawie o ewidencji ludności polegające m.in.: na udostępnianiu określonych danych z rejestru PESEL podmiotom wymienionym w art. 2 Prawa bankowego oraz spółdzielczym kasom oszczędnościowo-kredytowym. W naszej ocenie odsyłanie do art.2 wspomnianej ustawy jest wadliwe, bo odnosi nas do katalogu czynności bankowych, a nie katalogu podmiotów, co może rodzić wątpliwości interpretacyjne.

Czy wszyscy są gotowi na zmiany?

Umożliwienie przedsiębiorcom prowadzącym działalność regulowaną swobodnej weryfikacji danych należy ocenić bardzo pozytywnie. Jednak brak ograniczenia celów i zakresów przetwarzania danych może długoterminowo budzić wątpliwości interpretacyjne zarówno po stronie obywateli, innych uczestników rynku oraz organów nadzoru.

Niniejszy wniosek zdaje się potwierdzać stanowisko Prezesa Urzędu Ochrony Danych Osobowych zaprezentowane, odpowiednio, w komunikacie z dnia 24 lipca2019 r. pt. *„Zakaz wykonywania replik dokumentów publicznych ograniczy kradzieże tożsamości”* oraz w piśmie do Prezesa Związku Banków Polskich z sierpnia 2019 r. W związku z powyższym dobrym rozwiązaniem wydaje się ustawowe ograniczenie zakresu wykorzystania danych dostępnych w ww. rejestrach.

Warto również zwrócić uwagę na zmianę w ustawie o narodowym zasobie archiwalnym i archiwach, która ma polegać na zmianie wyrazu „mogą być” na wyraz „są”. Z pozoru drobna i kosmetyczna zmiana ma na celu nałożenie na podmioty publiczne obowiązku realizacji zadań w zakresie elektronicznego zarządzania dokumentacją. Wydawać by się mogło, że taką inicjatywie należy oceniać tylko pozytywnie, biorąc pod uwagę uciążliwość dokumentów w postaci papierowej. Realia mogą być inne. W obecnym kształcie zmiany te mogą uniemożliwić organom państwowym, państwowym jednostkom organizacyjnym oraz innym zobowiązanym podmiotom, odpowiednią ewidencję, przechowanie oraz ochronę przed uszkodzeniem dokumentów sporządzonych lub otrzymanych w postaci papierowej. Jeżeli zadania zawsze mają być realizowane w ramach EZD, to może oznaczać to wyłączenie możliwości prowadzenia dokumentacji w innej postaci niż elektroniczna. Takie rozwiązanie może okazać się rewolucją do której na chwilę obecną nie wszyscy są przygotowani.

Podsumowanie przygotowanej Oceny wpływu na ochronę danych i nie tylko oraz obawy praktyczne

Mimo, że inicjatywę należy ocenić bardzo pozytywnie jako wpisującą się w obserwowany na całym świecie trend informatyzacji administracji, to w projekcie znalazło się kilka postanowień problematycznych z perspektywy ochrony danych osobowych. Poniżej krótkie podsumowanie zmian na lepsze oraz ryzyk związanych z projektem w kontekście danych osobowych.

Zmiany na lepsze:

- Pozytywnie należy ocenić przeprowadzenie oceny wpływu na ochronę danych w przypadku samego projektu. Mimo sposobu jej przeprowadzenia, nagminna praktyką dot. wielu ustaw mających wpływ na ochronę danych osobowych jest pomijanie wymaganego prawem oceny Data Protection Impact Asessment. Tutaj został on przeprowadzony. Niestety do sposobu przeprowadzenia oceny należy mieć zastrzeżenia, co wskazano poniżej.

- Zmiany w kierunku integracji wewnętrznych systemów wykorzystywanych przez administrację (portal.gov i EZD) stanowią milowy krok w rozwoju nowoczesnej administracji i nowoczesnego państwa. Efektywna weryfikacja tożsamości oraz innych informacji przez urzędy i uczestników rynku w centralnych bazach danych stanowi fundament w rozwoju nowoczesnego państwa.

- Ustawa wprowadziła drobne zmiany skutkujące likwidacją drobnych przeszkód prawnych, utrudniających życie zwykłym obywatelom. Przykładowo zmienione zostały przepisy Kodeksu Rodzinnego i Opiekuńczego oraz ustawy o dowodach osobistych co umożliwi obywatelom zmianę nazwiska przez Internet.

Ryzyka związane z projektem:

- Prędkość i sposób wprowadzania zmian generuje ryzyko niezgodności zmian z obowiązującymi przepisami i nieskutecznego wdrożenia zmian. Wprowadzenie szczegółowych warunków technicznych, mających podstawowe znaczenie dla funkcjonowania projektu w formie Komunikatu właściwego ministra, a nie w formie rozporządzenia jest niezrozumiałe z perspektywy wymogów Rozporządzenia Prezesa Rady Ministrów w sprawie Zasad Techniki Prawodawczej. Zaś wprowadzenie krótkiego, 14 sto dniowego terminu na wdrożenie niniejszych warunków od momentu ich publikacji, może być poważnym wyzwaniem utrudniającym efektywne wdrożenie tychże zmian.

- W naszej ocenie sposób przeprowadzenia oceny ryzyka przetwarzania w zakresie danych osobowych (Ocena) nie spełnia wymogów opisywanych w RODO oraz wymogów stawianych przez PUODO w tym zakresie. Przykładowo w załączonej do projektu Ocenie nie ujęto wszystkich operacji przetwarzania będących efektem zmian ustawowych, a sama ocena opisanych procesów, np.: w zakresie ryzyk, które generuje tworzenie bazy danych wykorzystujących wizerunek, jest wątpliwa.

Podsumowując, projekt wydaje się dobrym krokiem w przód, ale wydaje się, że osiągnięcie zamierzonych przez ustawodawcę celów wymaga dalszej pracy nad szczegółami projektu.

CIEKAWOSTKI

Pierwsza kara za nienależytą ochronę danych osobowych sygnalistów

W związku z coraz większym zainteresowanie tematyką dotycząca tzw. sygnalistów oraz pracami nad polską ustawą regulującą instytucję sygnalisty warto zwrócić uwagę, że kwestia zapewnienia poufności oraz ochrony danych osobowych sygnalistów jest niezmiernie ważna, jeśli faktycznie chcemy aby przekazywali oni znaczące informacje. Na fakt ten zwrócił uwagę również włoski organ nadzorczy GPDP (Garante Per La Protezione Dei Date Personali), który 10 czerwca 2021 r. nałożył na spółkę Aeroporto Guglielmo Marconi di Bologna S.p.a., zarządzającą portem lotniczym w Bolonii, karę pieniężną w wysokości 40.000,00 EUR. Przyczyną nałożenia kary była nienależyta ochrona danych osobowych sygnalistów. Włoski administrator wdrażając system ochrony sygnalistów zdecydował się na wykorzystanie aplikacji „WB Confidential" dostarczanej przez spółkę aiComply S.r.l. W ocenie organu nadzoru przetwarzane w aplikacji dane osobowe były nieprawidłowo zabezpieczone z tego względu, że dostęp do aplikacji odbywał się poprzez niezabezpieczony protokół http, który nie gwarantuje integralności oraz poufności danych. W konsekwencji, w opinii organu administrator nie podjął odpowiednich środków technicznych oraz organizacyjnych celem zabezpieczenia danych. W trakcie kontroli okazało się również, że administrator nie przeprowadził procedury „Privacy by design" oraz „Privacy by default" dla oceny wdrażanego procesu, które zdaniem organu powinny zostać przeprowadzone. Włoski organ nadzoru odniósł się do podstaw przetwarzania danych osobowych sygnalistów, wskazując, że takich podstaw należy upatrywać w art. 6 ust. 1 lit. c), art. 9 ust. 2 lit. b) oraz art. 10 RODO. W Polsce kwestia ta nadal nie jest przesądzona.

Decyzja GPDP dostępna jest tutaj

Decyzje organów europejskich - Odpowiedzialność podmiotu przetwarzającego za przetwarzanie danych osobowych

Francuski organ nadzorczy (CNIL) wydał decyzję nakładającą administracyjną karę finansową na podmiot przetwarzający (spółkę Dedalus Biologie) w wysokości 1,5 miliona euro. Kara finansowa została nałożona na podmiot przetwarzający za naruszenie obowiązku (1) zapewnienia odpowiednich środków bezpieczeństwa ochrony danych osobowych (art. 32 RODO), (2) stosowania się do poleceń administratora (art. 29 RODO) oraz (3) formalizowania relacji powierzenia z administratorami (klientami podmiotu przetwarzającego).

Naruszenia podmiotu przetwarzającego doprowadziły do ujawnienia danych osobowych ponad 500 tysięcy osób, a zakres ujawnionych danych osobowych obejmował m.in. dane dotyczące zdrowia (informacje o chorobach: HIV, nowotwory, choroby genetyczne, czy ciąży, terapiach lekowych, danych genetycznych).

W sprawie CNIL wskazał m.in., że obowiązek zawarcia umowy powierzenia danych osobowych spoczywa zarówno na administratorze oraz podmiocie przetwarzającym. Jednak, w niniejszej sprawie to podmiot przetwarzający będący dostawcą usług dostarczał wszelką dokumentację handlową, która nie uwzględniała postanowień dotyczących powierzenia przetwarzania danych osobowych lub zawierała nieprawidłowe postanowienia. W konsekwencji, CNIL uznał, że podmiot przetwarzający naruszył art. 28 ust. 3 RODO. Innym istotnym rozstrzygnięciem CNIL jest stwierdzenie przekroczenia polecenia administratora przez podmiot przetwarzający, co nastąpiło przez pozyskanie większej ilości danych niż było to wymagane w ramach migracji z oprogramowania do innego narzędzia wykonanej (wykonanej na żądanie administratorów).

Niniejsza sprawa jest o tyle ciekawa, że w przeciwieństwie do większości spraw, które przypisują odpowiedzialność w ramach powierzenia przetwarzania administratorowi, w tej sprawie CNIL przypisał taką odpowiedzialność tylko przetwarzającemu Co więcej, CNIL nie odniósł się do oceny czy administrator ponosi odpowiedzialność za naruszenie ochrony danych osobowych w niniejszej sprawie.

Decyzja CNIL dostępna jest tutaj

Polska - Kodeks branżowy dot. przetwarzania danych osobowych dla sektora ochrony zdrowia dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających

Adrianna Gnatowska
Prawnik, adwokat
adrianna.gnatowska@skslegal.pl
+48 538 628 072

Kodeks postępowania dla sektora ochrony zdrowia znajduje się na końcowym etapie procedowania. Kodeks ten wskazuje rozwiązania dotyczące ochrony danych osobowych w ramach działań sektora zdrowia, w tym wskazuje obowiązki wynikające z RODO dla podmiotów leczniczych oraz proponowane podstawy prawne przetwarzania. Przedstawione w dokumencie rozwiązania pomogą administratorom wybrać prawidłowe rozwiązania w toku przetwarzania danych osobowych i przyczynią się do ujednolicenia podejścia do tej problematyki na rynku. Mimo, że kodeks nie będzie stanowił wiążących przepisów prawa, działanie zgodnie z nim zwiększy poziom bezpieczeństwa prawnego administratora. Po jego zatwierdzeniu przez UODO, kodeks będzie mógł stanowić narzędzie do potwierdzenia działania podmiotu zgodnie z RODO, a w konsekwencji – wpływać na łagodzenie kar związanych z naruszeniem przepisów ochrony danych osobowych. Ponadto wprowadzenie i stosowanie kodeksu zapewni zwiększony poziom ochrony danych osobom, których dane dotyczą - zgodnie z ustawą z dnia 23 sierpnia 2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, za działanie wprowadzające w błąd uznaje się nieprzestrzeganie kodeksu dobrych praktyk, do którego przedsiębiorca dobrowolnie przystąpił, jeżeli przedsiębiorca ten informuje w ramach praktyki rynkowej, że jest związany kodeksem dobrych praktyk.

Dokument jest dostępny na stronie

Zatwierdzone przez UODO kodeksy znajdować się będą tutaj.

ORZECZNICTWO & DECYZJE

Agata Szeliga
Partner, radca prawny
agata.szeliga@skslegal.pl
+48 698 660 648

Katarzyna Klonecka
Prawnik
katarzyna.klonecka@skslegal.pl
+48 602 151 178

Ostatnie orzecznictwo – najważniejsze wyroki i decyzje z zakresu ochrony danych osobowych

Rok 2022 rozpoczął się od wydania kilku znaczących decyzji przez Prezesa Urzędu Ochrony Danych Osobowych („PUODO"). Ponadto w ostatnim czasie wydane zostały interesujące wyroki sądowe w tym zakresie. Poniżej znajduje się podsumowanie najważniejszych wniosków, które należy wyciągnąć z tych wyroków i decyzji:

WNIOSKI

1. **Wskazówki do oceny ryzyka związanego z naruszeniem ochrony danych – Santander Bank Polska S.A. (nałożona kara - ponad 545 tys. zł. wraz z obowiązkiem powiadomienia osób o naruszeniu; decyzja dostępna *tutaj*).** Brak zawiadomienia osób o naruszeniu poufności ich danych w związku z dalszym dostępem byłych pracowników do danych pracowników administratora na platformie usług elektronicznych ZUS.

- **Podczas oceny ryzyka związanego z naruszeniem administratorzy powinni brać pod uwagę zarówno ilość osób, jak i ilość danych dotkniętych naruszeniem oraz ich charakter – należy zawsze z większą ostrożnością oceniać naruszenia, które obejmują dane szczególnej kategorii lub większy zbiór danych osobowych.** Duża ilość osób objętych naruszeniem i zakres naruszonych danych (w tym informacje o zwolnieniach lekarskich zakwalifikowanych jako dane dotyczące zdrowia) doprowadziły PUODO do wniosku, że naruszenie wiąże się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, a więc zawiadomienie ich o naruszeniu było konieczne.

- Wystąpienie skutku w postaci faktycznego wykorzystania danych nie jest konieczne dla oceny, że zachodzi obowiązek zawiadomienia o naruszeniu. Wystarczy możliwość wystąpienia takiego ryzyka.

- **Były pracownik nie stanowi „zaufanego odbiorcy"** (tj. osoby wobec której udostępnienie danych może być uznane za mniej ryzykowne). Administratorzy powinni z większą ostrożnością podchodzić do naruszeń powiązanych z byłymi pracownikami, niezależnie od innych czynników (np. przeszkolenia pracownika jeszcze podczas zatrudnienia) i niezależnie od faktu, że pracownik zatrudniony u administratora posiada co do zasady status zaufanego odbiorcy (do momentu zakończenia zatrudnienia). Na brak zaufania powinny wpływać również podejrzane zachowania osoby, takie jak logowanie się do systemu mimo zakończenia współpracy lub braku upoważnienia.

- **Administratorzy powinni wdrożyć lub zweryfikować środki stosowane w przypadku ustania stosunku pracy z osobą mającą dostęp do danych osobowych.** Administrator powinien m.in. odbierać takim osobom dostęp do wszelkich baz danych.

- **W przypadku zawiadamiania o naruszeniach, administratorzy powinni podawać konkretne informacje o naruszeniu, spełniające wymogi określone w art. 34 ust. 1 RODO.** Administrator może spełnić ten obowiązek nie tylko za pomocą wysłania bezpośredniej informacji do pracowników, ale i poprzez ogólnodostępny komunikat (np. w Intranecie). Ważne jest by komunikat dotarł do wszystkich zagrożonych naruszeniem osób oraz żeby jasno wskazywał że dotyczy konkretnego naruszenia.

WNIOSKI

2 **To administrator (a nie pracownik) odpowiada za wdrażanie środków ochrony danych w organizacji – wyrok WSA w Warszawie z 15 lutego 2022 r. (sygn. akt II SA/Wa 3309/21) utrzymujący w mocy decyzję PUODO o nałożeniu administracyjnej kary pieniężnej (10 tys. zł.) na Prezesa Sądu Rejonowego w Zgierzu.** Zgubienie przez kuratora sądowego niezaszyfrowanego pendrive'a, na którym były zapisane dane osobowe.

- **To administrator danych jest odpowiedzialny za stosowanie odpowiednich zabezpieczeń danych i nie może przenosić ciężaru tej odpowiedzialności na pracowników.** W przedmiotowej sprawie kurator otrzymał niezabezpieczony pendrive oraz został zobowiązany do wdrożenia zabezpieczeń nośnika we własnym zakresie. Kurator nie wdrożył zabezpieczeń, przez co zgubienie nośnika skutkowało umożliwieniem osobom nieuprawnionym dostępu do danych osobowych zawartych na nośniku (tj. danych osób podlegających nadzorowi kuratorskiemu i objętych wywiadem środowiskowym).
- **Administrator powinien być świadomy zabezpieczeń funkcjonujących w organizacji i ich skuteczności.** Obciążenie pracowników obowiązkiem wdrażania środków ochrony pozbawia administratora takich informacji.
- **Administrator nie może ograniczyć się do szkolenia dla pracowników.** Powinien wdrażać dalsze środki techniczne i organizacyjne w celu spełnienia wymogów związanych z bezpieczeństwem danych.

WNIOSKI

3 **Prawo do bycia zapomnianym jednak znajduje zastosowanie do działalności prasowej – wyrok WSA w Warszawie z 21 stycznia 2022 r. (sygn. akt II SA/Wa 1055/21) uchylający decyzję PUODO w przedmiocie umorzenia postępowania w przedmiocie żądania usunięcia danych osobowych z artykułu prasowego.**

- Art. 2 ust. 1 ustawy z 10 maja 2018 r. o ochronie danych osobowych wyłącza stosowania części przepisów RODO w zakresie działalności dziennikarskiej. Wśród wyłączonych przepisów nie znajduje się jednak art. 17 ust. 1 RODO, tj. „prawo do bycia zapomnianym". Tym samym „prawo do bycia zapomnianym" może być stosowane w stosunku do artykułów prasowych
- Powyższe zmienia wcześniejsze orzecznictwo, które stwierdzało brak kompetencji PUODO do zbadania konieczności usunięcia danych ze względu na brak podstawy prawnej..

4 **(Zarówno administrator, jak i przetwarzający odpowiadają za brak wystarczających środków bezpieczeństwa – Fortum Marketing and Sales S.A. – administrator (kara w wysokości ponad 4,9 mln zł) oraz PIKA sp. z o.o. – przetwarzający (kara w wysokości 250 tys. zł); decyzja dostępna jest *tutaj*).**

Administrator oraz podmiot przetwarzający nie wdrożyli odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych. Administrator nie weryfikował też środków technicznych i organizacyjnych stosowanych przez podmiot przetwarzający przed zawarciem umowy powierzenia oraz w trakcie powierzenia.

WNIOSKI

- Długotrwała współpraca między administratorem a przetwarzającym, niepoparta audytami lub inspekcjami, nie gwarantuje, że przetwarzający prawidłowo wykonuje zadania wymagane przez prawo i umowę o przetwarzaniu danych i nie zwalnia administratora z wykonywania swoich obowiązków zgodnie z RODO.

- W konsekwencji:
  - Administrator jest zobowiązany przed umową powierzenia sprawdzić czy przetwarzający daje wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (realizacja art. 28 ust. 1 RODO).

  - Administrator jest zobowiązany przeprowadzać regularne audyty lub inspekcje podmiotu przetwarzającego w celu sprawdzenia, czy podmiot przetwarzający wywiązuje się ze swoich obowiązków (realizacja art. 28 ust. 3 lit. h) RODO). Poleganie na listach sprawdzających dołączonych do umowy lub wysłanych przed jej zawarciem nie jest wystarczające.

- Odpowiedzialność administratora za naruszenie bezpieczeństwa ochrony danych osobowych, nie wyklucza odpowiedzialności podmiotu przetwarzającego, jeśli to on swoim działaniem/zaniechaniem doprowadza bezpośrednio do powstania naruszenia.

CO NAJWAŻNIEJSZE

5

Można sięgnąć po informacje wynikające z monitoringu budynku aby sprawdzić, czy listonosz wrzucił awizo do skrzynki – wyrok NSA z 15 marca 2022 r. (sygn. akt II GZ 50/22)

W swoim wyroku, NSA stwierdził że w celu wyjaśnienia rozbieżności co do kwestii prawidłowości dostarczenia przesyłki poleconej, konieczne będzie zwrócenie się do zarządcy budynku o udzielenie informacji czy z nagrań monitoringu wizyjnego wynika, że listonosz podjął próbę doręczenia jakiejkolwiek korespondencji do lokalu. W przedmiotowej sprawie inne przedstawione dowody nie pozwoliły na ocenę tej sytuacji bowiem operator pocztowy stwierdził niemożliwość ustalenia okoliczności dot. awizacji przesyłki. Dopiero po uzyskaniu informacji o tym, co wynika z monitoringu, możliwa będzie ocena czy skuteczne doręczono korespondencję.

6

Jakie osoby można poinformować o odejściu pracownika? – wyrok WSA w Warszawie 29 września 2021 r. (sygn. II SA/Wa 1724/21)

Pracodawca wysłał informacje o odejściu z pracy jednego z pracowników do innych pracowników oraz do jednej osoby spoza organizacji. Zgodnie z potwierdzonym przez sąd stanowiskiem PUODO, pracodawca mógł wysłać tę informację do pracowników, niemniej jednak nie powinien był wysyłać danych do osoby niebędącej pracownikiem – za ostatnie z działań pracodawca otrzymał upomnienie.

- zgodnie ze stanowiskiem sądu, udostępnienie danych osobowych pracownika w informacji o jego odejściu osobie, która nie jest pracownikiem firmy nie znajduje podstawy prawnej w RODO i jest naruszeniem zasady minimalizacji danych;

- niemniej jednak, udostępnienie danych osobowych zawartych w wiadomości o odejściu pracownika jego ówczesnym współpracownikom jest zgodne z RODO – udostępnienie to można oprzeć na prawnie uzasadnionym interesie administratora w postaci konieczności przeorganizowania pracy;

- niezależnie od kwestii ochrony danych osobowych, wiadomość o odejściu pracownika powinna również zawierać treść nienaruszającą dóbr osobistych pracownika (tj. przede wszystkim powinno unikać się ocen lub opinii naruszającej dobra osobiste).

www.skslegal.pl