



NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

- str. 2 **KOMORNIK MA PRAWO UDOSTĘPNIĆ DANE OSOBOWE DŁUŻNIKA DŁUŻNIKOM WIERZYTELNOŚCI**
- str. 3 **JAKIE DANE MOŻNA UDOSTĘPNIĆ RZECZNIKOWI DYSCYPLINARNEMU I KOMISJI DYSCYPLINARNEJ W POSTĘPOWANIU WOBEC NAUCZYCIELA**
- str. 4 **KIEDY PRACODAWCA MA PRAWO POZYSKAĆ ADRES ZAMELDOWANIA ORAZ ADRES DO KORESPONDENCJI OD ZATRUDNIANEGO PRACOWNIKA?**
- str. 5 **ZMIANA OSOBY LUB OSÓB UPRAWNIONYCH DO REPREZENTACJI PODMIOTU, KTÓRY WYZNACZYŁ IOD**
- str. 6 **PRAWIDŁOWA IDENTYFIKACJA ZAGROZEŃ POZWOLI NA WŁAŚCIWY DOBÓR ŚRODKÓW BEZPIECZEŃSTWA**
- str. 8 **KARY**
- Francja: kara za umieszczanie reklamowych plików cookie bez zgody internautów
 - Francja: 1,75 mln euro kary dla ubezpieczyciela
- str. 9 **RADA EUROPY**
- Benin nowym obserwatorem przy Komitecie Konwencji 108
- str. 9 **TRWAJĄ KONSULTACJE PROJEKTU KODEKSU POSTĘPOWANIA DLA SEKTORA MARKETINGU**
- str. 10 **NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW**



KOMORNIK MA PRAWO UDOSTĘPNIĆ DANE OSOBOWE DŁUŻNIKA DŁUŻNIKOM WIERZYTELNOŚCI

Takie postępowanie ma umocowanie w przepisach Kodeksu postępowania cywilnego, a jednocześnie jest niezbędne ze względu na konieczność sprecyzowania, wobec kogo prowadzone jest postępowanie komornicze oraz określenia wierzytelności, która podlega zajęciu komorniczemu.

Takie rozstrzygnięcie znalazło się w decyzji Prezesa UODO wydanej w następstwie skargi złożonej na działalność komornika, który w związku z wnioskami uprawnionych wierzycieli wszczął trzy postępowania egzekucyjne przeciwko skarżącemu.

Udostępnienie danych przez komornika

W ich toku komornik dokonał dwóch zajęć wierzytelności przysługujących – jego zdaniem – skarżącemu od określonych osób, ustalonych przez komornika na podstawie akt innych postępowań. W skierowanych do nich w tej sprawie pismach komornik udostępnił takie dane osobowe skarżącego, jak: imię i nazwisko, numer PESEL, adres zamieszkania oraz informacje o zadłużeniu.

Ustawowe uprawnienia związane z prowadzeniem postępowania egzekucyjnego

Badając dopuszczalność takiego postępowania, Prezes UODO wziął pod uwagę m.in. przepisy ustawy z dnia 22 marca 2018 r. o komornikach sądowych oraz regulacje zawarte w ustawie z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (k.p.c.).

Wskazał, że stosownie do art. 2 ustawy o komornikach sądowych, komornik jest funkcjonariuszem publicznym działającym przy sądzie rejonowym i podlega nadzorowi sądu oraz nadzorowi odpowiedzialnemu prezesowi sądu rejonowego, przy którym działa. Ponadto przy wykonywaniu zadań komornik kieruje się dobrem wymiaru sprawiedliwości oraz interesem publicznym. Zgodnie natomiast z art. 3 ust. 1 powołanej ustawy, komornik jest organem władzy publicznej w zakresie wykonywania czynności w postępowaniu egzekucyjnym i zabezpieczającym. Czynności te wykonuje komornik, z uwzględnieniem wyjątków przewidzianych w ustawach.

Jednocześnie organ nadzorczy zaznaczył, że zgodnie z art. 799 § 1 k.p.c., wniosek o wszczęcie egzekucji lub żądanie przeprowadzenia egzekucji z urzędu umożli-

liwia prowadzenie egzekucji według wszystkich dopuszczalnych sposobów, z wyjątkiem egzekucji z nieruchomości. Skierowanie egzekucji do nieruchomości dłużnika oraz składników jego majątku, do których przepisy o egzekucji z nieruchomości stosuje się odpowiednio, jest możliwe tylko na wniosek wierzyciela. Wierzyciel może wskazać wybrane przez siebie sposób albo sposoby egzekucji. Organ egzekucyjny stosuje sposób egzekucji najmniej uciążliwy dla dłużnika. Stosownie zaś do treści art. 801 § 1 k.p.c., jeżeli wierzyciel albo sąd zarządzający z urzędu przeprowadzenie egzekucji albo uprawniony organ żądający przeprowadzenia egzekucji nie wskaże majątku pozwalającego na zaspokojenie świadczenia, komornik z urzędu: 1) ustala majątek dłużnika w zakresie znanym mu z innych prowadzonych postępowań albo na podstawie publicznie dostępnych źródeł informacji, albo rejestrów, do których ma dostęp drogą elektroniczną; 2) wzywa dłużnika do złożenia wykazu majątku. W myśl natomiast art. 803 k.p.c., tytuł wykonawczy stanowi podstawę do prowadzenia egzekucji o całe objęte nim roszczenie i ze wszystkich części majątku dłużnika, chyba że z treści tytułu wynika co innego.

Dla rozstrzygnięcia analizowanej sprawy istotne było też to, że zgodnie z art. 896 § 1 pkt 2 k.p.c., do egzekucji z wierzytelności komornik przystępuje przez jej zajęcie. W celu zajęcia komornik wzywa dłużnika wierzytelności, aby należnego od niego świadczenia nie uiszczał dłużnikowi, lecz złożył je komornikowi lub na rachunek depozytowy Ministra Finansów. Zgodnie natomiast z art. 896 § 2 k.p.c., jednocześnie z zajęciem wierzytelności komornik wzywa jej dłużnika, aby w ciągu tygodnia złożył oświadczenie: 1) czy i w jakiej wysokości przysługuje dłużnikowi zajęta wierzytelność, czy też odmawia zapłaty i z jakiej przyczyny; 2) czy inne osoby roszczą sobie prawa do wierzytelności, czy i w jakim sądzie lub przed jakim organem toczy się lub toczyła się sprawa o zajętą wierzytelność oraz czy i o jakie roszczenie została skierowana do zajętej wierzytelności egzekucja przez innych wierzycieli.

Organ nadzorczy podkreślił też, że komornik jest wręcz zobowiązany do wykonania obowiązku, o którym mowa we wskazanym art. 896 § 1 pkt 2 k.p.c. Sąd Najwyższy w wyroku z 14 stycznia 1998 r. (sygn. akt I CKN 406/97) wskazał bowiem, że niewykonanie przez komornika obowiązku z art. 896 § 1 pkt 2 k.p.c., polegającego na wezwaniu poddłużnika egzekwowanej wierzytelności, aby nie uiszczając objętego nią świadczenia dłużnikowi głównemu, lecz przekazał to świadczenie komornikowi lub do depozytu sądowego, może rodzić odpowiedzialność odszkodowawczą przewidzianą w art. 769 k.p.c.

Komornik nie naruszył przepisów o ochronie danych osobowych

Biorąc pod uwagę powyższe uregulowania, Prezes UODO uznał, że komornik był uprawniony do udostępnienia danych osobowych skarżącego na rzecz dłużników zajętych wierzytelności. Z jednej strony, jego działanie miało oparcie we wskazanych przepisach k.p.c.,

a udostępnienie danych osobowych skarżącego było niezbędne ze względu na konieczność sprecyzowania, wobec kogo prowadzone są postępowania komornicze oraz określenia wierzytelności, która podlegała zajęciu komorniczemu. Z drugiej strony, komornik przetwarzał dane osobowe skarżącego w zakwestionowany przez niego sposób w ramach sprawowania władzy publicznej powierzonej mu, jako administratorowi, m.in. na mocy przepisów ustawy o komornikach sądowych. Kwestionowane przez skarżącego przetwarzanie danych osobowych miało zatem oparcie w przesłance przetwarzania danych osobowych, o której mowa w art. 6 ust. 1 lit. e) RODO.

W tej sytuacji Prezes UODO uznał, że komornik nie naruszył przepisów o ochronie danych osobowych, w tym przede wszystkim RODO, w związku z czym odmówił uwzględnienia wniosku skarżącego.



JAKIE DANE MOŻNA UDOSTĘPNIĆ RZECZNIKOWI DYSCYPLINARNEMU I KOMISJI DYSCYPLINARNEJ W POSTĘPOWANIU WOBEC NAUCZYCIELA

W postępowaniu wyjaśniającym, a następnie dyscyplinarnym dotyczącym nauczyciela uprawnione podmioty mogą zbierać wszelkie dowody, które są konieczne dla wyjaśnienia sprawy. Jeśli jednak zwracają się one do administratora o udostępnienie określonych danych osobowych, to powinny swój wniosek starannie uzasadnić, a zadaniem administratora jest ustalenie, czy spełnione są przesłanki umożliwiające udostępnienie danych.

To ogólne zalecenie, które Prezes UODO sformułował w związku z wątpliwościami, czy komisja dyscyplinarna badająca sprawę zachowania nauczyciela może żądać od dyrektora szkoły udostępnienia takich dokumentów dotyczących konkretnego ucznia, jak: orzeczenie o potrzebie kształcenia specjalnego, wielospecjalistyczna ocena poziomu funkcjonowania, indywidualny program edukacyjno-terapeutyczny, które zawierają dane osobowe dziecka należące do kategorii szczególnych.

Organ nadzoru wskazał, że zgodnie z art. 85g ustawy z dnia 26 stycznia 1982 r. Karta Nauczyciela, w postępowaniu wyjaśniającym dowody są przeprowadzane przez rzecznika dyscyplinarnego, a w postępowaniu dyscyplinarnym – przez komisję dyscyplinarną. Nie wyłącza

to prawa do zgłoszenia wniosku dowodowego przez nauczyciela, którego dotyczy postępowanie wyjaśniające, lub obwinionego (ust. 1). W postępowaniu wyjaśniającym i postępowaniu dyscyplinarnym rzecznik dyscyplinarny lub komisja dyscyplinarna mogą przesłuchiwać świadków, zbierać i przeprowadzać wszelkie dowody konieczne dla wyjaśnienia sprawy, w tym zasięgać opinii biegłych, oraz przeglądać akta osobowe odpowiednio nauczyciela, którego dotyczy postępowanie wyjaśniające, lub obwinionego, a także sporządzać z nich notatki i kopie (ust. 2). Zgodnie natomiast z § 23 ust. 7 rozporządzenia Ministra Edukacji Narodowej z dnia 25 maja 2016 r. w sprawie szczegółowego trybu prowadzenia postępowania wyjaśniającego i dyscyplinarnego wobec nauczycieli oraz wznawiania

postępowania dyscyplinarnego, do zamknięcia rozprawy rzecznik dyscyplinarny, obwiniony i jego obrońca mogą zgłaszać wnioski o dopuszczenie nowych dowodów, w tym powołanie biegłych.

Rozstrzygając kwestię dopuszczalności przetwarzania, w tym udostępniania, danych osobowych na potrzeby postępowania wyjaśniającego lub dyscyplinarnego, pod uwagę brać należy również przepisy RODO. Zgodnie z nimi (art. 5), administrator zobowiązany jest przetwarzać dane osobowe zgodnie z prawem, zapewnić im poufność, a w razie ewentualnej kontroli organu nadzorczego – rozliczalność. Przetwarzanie, w tym również udostępnianie danych osobowych, może się zaś odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO, a w przypadku szczególnych kategorii danych osobowych – po spełnieniu przesłanek określonych w art. 9 RODO.

Każdy wniosek o udostępnienie danych wymaga indywidualnej analizy. Rozpatrujący go administrator musi wziąć pod uwagę: obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrze-

by posiadania danych przez podmiot, który występuje o ich udostępnienie, w tym wskazanie przez niego podstawy prawnej żądania. W przypadkach, gdy uzasadnienie prawne lub faktyczne wniosku budzi wątpliwości, celowe jest uzyskanie od wnioskującego wyjaśnień lub dodatkowych informacji. Każdy wniosek powinien bowiem zawierać niebudzącą wątpliwości podstawę prawną.

Jak wskazano wyżej, w postępowaniu wyjaśniającym, a następnie dyscyplinarnym nauczyciela uprawnione podmioty mogą zbierać wszelkie dowody, pod warunkiem że będą one konieczne dla wyjaśnienia sprawy. Zadaniem administratora będzie odpowiednia analiza składanych przez te podmioty wniosków. W przypadku wskazania w nich podstawy prawnej, która nie spełnia warunków określonych w art. 6 lub art. 9 RODO albo w razie całkowitego jej braku, administrator powinien odmówić realizacji wniosku, aby nie narazić się na naruszenie wymienionych wyżej zasad, tj. przetwarzania danych zgodnie z prawem, zapewnienia ich poufności i rozliczalności.



KIEDY PRACODAWCA MA PRAWO POZYSKAĆ ADRES ZAMELDOWANIA ORAZ ADRES DO KORESPONDENCJI OD ZATRUDNIANEGO PRACOWNIKA?

Pracodawca ma prawo do przetwarzania adresu zameldowania oraz adresu do korespondencji, które są niezbędne do wypełnienia formularza ZUS ZUA, dopiero po zawarciu stosunku pracy.

Jak wskazywaliśmy w [newsletterze 5/2021](#), „pracodawca ma prawo pozyskiwać adres zamieszkania od osoby, co do której została podjęta decyzja o zatrudnieniu, gdyż jest to niezbędne do skierowania jej na obowiązkowe, wstępne badania lekarskie”.

Na tym tle organowi nadzoru została zasygnalizowana inna wątpliwość, dotycząca tego, czy na etapie zatrudniania pracownika pracodawca może żądać od niego podania adresu zameldowania i adresu do korespondencji, które są potrzebne w związku z realizacją obowiązku zgłoszenia pracownika do ubezpieczenia. Pytający powoływali się na art. 36 ust. 10 ustawy

z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, który stanowi, że zgłoszenie do ubezpieczeń społecznych zawiera m.in. takie dane, jak:

- adres zameldowania na stałe miejsce pobytu, adres zamieszkania, jeżeli jest inny niż adres zameldowania na stałe miejsce pobytu,
- adres do korespondencji, jeżeli jest inny niż adres zameldowania na stałe miejsce pobytu,
- adres zamieszkania.

Wyjaśniając tę kwestię, Prezes UODO wskazał, że zgodnie z art. 22¹ § 4 Kodeksu pracy, pracodawca żąda podania danych osobowych innych niż określone w § 1 (dane wymagane od kandydata) i § 3 (dane wymagane od pracownika), gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Jak wskazuje art. 36 ust. 4 ustawy o systemie ubezpieczeń społecznych, pracodawca dokonuje zgłoszenia pracownika do ubezpieczeń społecznych w terminie 7 dni od daty powstania obowiązku ubezpieczenia, tj. od dnia nawiązania stosunku pracy.

Powyższe oznacza, że w procesie zatrudnienia możemy mówić o dwóch etapach – w pierwszym podmiotem danych jest kandydat do pracy, który dopiero może zostać pracownikiem, w drugim jest nim już osoba, z którą zawarto umowę o pracę. Zakres danych zbieranych przez pracodawcę na każdym z etapów określają przepisy odpowiednio art. 22¹ § 1 i § 3 Kodeksu pracy. O wyjątku wymienionym w art. 22¹ § 4 Kodeksu pracy możemy mówić, kiedy niezbędne jest rozszerzenie wskazanego zakresu danych ze względu na uprawnienie lub obowiązek wynikający z przepisów prawa.

Formularz ZUS ZUA przewiduje podanie szeregu danych wykraczających poza te wymienione w art. 22¹ § 1 i § 3 Kodeksu pracy, jak np. adres zameldowania, adres zamieszkania i adres do korespondencji. Artykuł 36 ust. 4 ustawy o systemie ubezpieczeń społecznych nie uniemożliwia podjęcia lub dopuszczenia do pracy przed zgłoszeniem pracownika do ZUS, jak to jest w przypadku badań lekarskich. Należy więc przyjąć, że względem danych zbieranych w celu zgłoszenia pracownika do ubezpieczenia społecznego, ich zakres może być rozszerzony po zawarciu z kandydatem umowy o pracę, ponieważ ze względu na termin zgłoszenia wynoszący 7 dni od dnia nawiązania stosunku pracy, nie można tutaj mówić o niezbędności do zrealizowania obowiązku na etapie przeprowadzania rekrutacji.

Reasumując powyższe i odpowiadając na zgłaszane wątpliwości, należy wskazać, że pracodawca będzie miał możliwość przetwarzania takich danych osobowych, jak: adres zameldowania, adres zamieszkania i adres do korespondencji, niezbędnych do wypełnienia formularza ZUS ZUA, dopiero po zawarciu z pracownikiem stosunku pracy. Żądanie ich podania na etapie rekrutacji jest przedwczesne, ponieważ obowiązek zgłoszenia do ZUS istnieje dopiero od dnia nawiązania stosunku pracy.

ZMIANA OSOBY LUB OSÓB UPRAWNIONYCH DO REPREZENTACJI PODMIOTU, KTÓRY WYZNACZYŁ IOD

Gdy w podmiocie, który wyznaczył IOD, zmieniają się jedynie dane osoby lub osób uprawnionych do jego reprezentacji, w tym także prezesa zarządu, nie ma potrzeby informowania o nich Prezesa UODO.

Zgodnie bowiem z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: u.o.d.o.) podmiot, który wyznaczył inspektora ochrony danych, ma obowiązek zawiadomić Prezesa UODO o każdej zmianie danych wskazanych w ustępach 1 i 3 art. 10 powołanej ustawy.

A zatem Prezesa UODO trzeba powiadomić o zmianach, które dotyczą takich danych, jak:

- imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora,

- imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna,

- firma przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą,

- pełna nazwa oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w dwóch powyższych punktach,

- numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

Prezesa UODO trzeba również zawiadomić o odwołaniu IOD. Analogiczne rozwiązania dotyczące powiadamiania Prezesa UODO odnoszą się do sytuacji, w której



podmiot wyznaczył osobę zastępującą inspektora (stosownie do art. 11a ust. 3 u.o.d.o.).

Administrator informacje o zmianach musi przekazać w ciągu 14 dni od dnia, w którym one nastąpiły, co wprost wskazane zostało w powołanym art. 10 ust. 4 u.o.d.o.

Powinien to zrobić, korzystając z elektronicznego formularza, ponieważ zawiadomienia należy składać tylko w postaci elektronicznej. Formularze dostępne są np. na platformie biznes.gov.pl. Alternatywnym sposobem zawiadomienia Prezesa UODO o danych kontaktowych inspektora ochrony danych oraz w przypadku niedających się rozwiązać problemów z wystaniem zawiadomienia przez platformę biznes.gov.pl, jest zawiadomienie, które można wysłać przez platformę epuap.gov.pl (użytkownik po zalogowaniu i wybraniu formularza jest przekierowywany na portal obywatel.gov.pl), załączając właściwy formularz spośród dostępnych **pod linkiem**.

Ponieważ przepisy u.o.d.o. nie zobowiązują administratora do zawiadamiania organu nadzoru o zmianach danych osoby (osób) uprawnionych do reprezentacji podmiotu, który wyznaczył IOD, nie ma potrzeby informowania Prezesa UODO o takich zmianach.

Warto nadmienić, że również przepisy ustawy z dnia

14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (dalej: ustawa z 14 grudnia 2018 r.) nie zobowiązują administratora do zawiadamiania organu nadzoru o zmianach danych osoby (osób) uprawnionych do reprezentacji podmiotu, który wyznaczył IOD.

Więcej informacji o zawiadomieniach Prezesa UODO związanych z IOD jest dostępnych na stronie internetowej UODO, np. w komunikacie pt. „**Powiadomienia dotyczące IOD lub jego zastępcy należy składać tylko w postaci elektronicznej**”, w zakładce **Zawiadomienia Prezesa UODO związane z IOD**, a także w materiałach odnoszących się do powoływania IOD na podstawie ustawy z dnia 14 grudnia 2018 r. – „**Wyznaczenie IOD w sądach powszechnych**” oraz „**Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną**”.

Szczególnie zachęcamy do lektury zakładki **Zawiadomienia Prezesa UODO związane z IOD**, gdzie znajdują się praktyczne podpowiedzi dotyczące zgłaszanych nam dotychczas problemów związanych z realizacją tego obowiązku (np. w jakiej formie należy dokonać zgłoszenia, czy może być ono dokonane przez pełnomocnika i jak powinno wyglądać pełnomocnictwo do takiej czynności). Przypominamy, iż nie tylko zawiadomienie związane z IOD powinno być dokonane w formie elektronicznej, ale również taką formę powinno mieć pełnomocnictwo.



PRAWIDŁOWA IDENTYFIKACJA ZAGROZEŃ POZWOLI NA WŁAŚCIWY DOBÓR ŚRODKÓW BEZPIECZEŃSTWA

Udzielenie upomnienia oraz dostosowanie operacji przetwarzania poprzez przeprowadzenia analizy ryzyka w celu oszacowania jego właściwego poziomu, wdrożenie odpowiednich środków technicznych i organizacyjnych dla zapewnienia zdolności do szybkiego przywrócenia dostępu do danych w razie incydentu oraz zapewnienia ich regularnego testowania, mierzenia i oceniania skuteczności – to główne postanowienia decyzji UODO upominającej podmiot z sektora publicznego.

Administrator dokonał zgłoszenia organowi nadzorczemu naruszenia ochrony danych, które polegało na złamaniu zabezpieczeń systemu informatycznego administratora, wykorzystywanego przez niego

do przetwarzania danych osobowych, a następnie zaszyfrowanie przetwarzanych w nim danych za pomocą złośliwego oprogramowania. Konsekwencją tego działania było pozbawienie administratora dostępu do sys-

temu oraz znajdujących się w nim danych osobowych. Administrator nie stwierdził wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w związku z czym nie zawiadomił osób, których dane dotyczą, o incydencie.

Biorąc pod uwagę charakter naruszenia, czas jego trwania, kategorie danych oraz liczbę osób, których dotyczyło naruszenie, organ nadzorczy uznał, że wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych i zwrócił się do administratora o wypełnienie tego obowiązku.

Należy pamiętać, że dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („poufność, integralność, dostępność”).

Obowiązek zapewnienia bezpieczeństwa przetwarzanych danych, stanowi fundament prawnej ochrony danych osobowych. RODO nie narzuca konkretnych działań, które należy podjąć, aby zapewnić bezpieczeństwo danych, pozostawiając w tej materii swobodę administratorowi danych.

Konkretyzując zasadę poufności, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Ustalenie ich jest procesem dwuetapowym. W pierwszej kolejności ważne jest określenie poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, a w dalszej kolejności należy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

W tej konkretnej sprawie, administrator nie dokonał identyfikacji zagrożeń, dokonując analizy ryzyka, co skutkowało niewłaściwym doбором środków bezpieczeństwa lub w ogóle nie zostały one przewidziane. Administrator nie dokonał także oceny, czy wprowadzone zasady bezpieczeństwa są odpowiednie przetwarzając dane osobowe. Przykładem w tym zakresie

jest wykorzystywanie przez administratora oprogramowanie. Administrator wskazał bowiem, że przed wystąpieniem naruszenia korzystał z oprogramowania serwera, które jednak straciło wsparcie producenta. Oznacza to, że dla wykorzystywanego systemu nie były wydawane aktualizacje oprogramowania oraz zabezpieczeń i poprawek. Brak wbudowanych oraz aktualizowanych zabezpieczeń zwiększa w szczególności ryzyko podatności na infekcję za pomocą złośliwego oprogramowania oraz ataków poprzez powstawanie nowych luk w zabezpieczeniach.

W następstwie nie przeprowadzenia analizy ryzyka, nie zidentyfikowania zagrożeń i nie wprowadzenia odpowiednich środków organizacyjnych i technicznych, doszło do naruszenia ochrony danych osobowych poprzez przełamanie zabezpieczeń systemu informatycznego administratora wykorzystywanego do przetwarzania danych osobowych, a następnie zaszyfrowanie przetwarzanych w nim danych z wykorzystaniem złośliwego oprogramowania.

Mimo że administrator posiadał wewnętrzne instrukcje zarządzania systemami informatycznymi, jednak były tam uwzględnione jedynie podstawowe informacje w zakresie sporządzania kopii zapasowych. Dokument nie określał w sposób szczegółowy zasad weryfikacji poprawności ich sporządzania czy nawet osoby odpowiedzialnej za ich sporządzenie. Brak takich procedur skutkowało brakiem możliwości szybkiego przywrócenia dostępności do danych.

W związku z tym UODO w decyzji stwierdzającej naruszenie polegające na doborze nieskutecznych zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych, postanowił nie tylko nakazać dostosowania operacji przetwarzania do przepisów RODO, ale także udzielił administratorowi upomnienia.



KARY

Francja: kara za umieszczanie reklamowych plików cookie bez zgody internautów

CNIL ukarała SOCIÉTÉ DU FIGARO karą pieniężną w wysokości 50 tys. euro za umieszczanie reklamowych plików cookie na stronie lefigaro.fr bez uzyskania wcześniejszej zgody użytkowników Internetu.

Kontrole CNIL wykazały, że gdy użytkownik odwiedzał stronę lefigaro.fr, pliki cookie były automatycznie umieszczane na jego komputerze przez partnerów spółki, bez jakiegokolwiek działania z strony użytkownika lub pomimo jego odmowy. Należy wskazać, że kilka z tych plików cookie miało cel reklamowy i powinno być przedmiotem zgody użytkownika.

Zdaniem CNIL, przedsiębiorstwo nie wypełniło swoich obowiązków, ponieważ nie zapewniało systematycznego uzyskiwania zgody użytkowników przed umieszczeniem reklamowych plików cookie oraz respektowania ich odmowy zgody na umieszczenie tych plików.

SOCIÉTÉ DU FIGARO, jako wydawca strony internetowej lefigaro.fr, jest częściowo odpowiedzialny za przestrzeganie przepisów dotyczących cookies (art. 82 francuskiej ustawy o ochronie danych) przez swoich partnerów, którzy umieszczają cookies na jego stronie. W szczególności musi dopilnować, aby nie umieszczać plików cookie wymagających zgody, zanim użytkownicy nie dokonają wyboru, czy chcą je zaakceptować, czy odrzucić. Musi również zapewnić, że będą one respektować odmowę wyrażoną przez tych ostatnich.

Według CNIL fakt, że pliki cookie pochodzą od partnerów, nie zwalnia wydawcy strony z jego własnej odpowiedzialności, o ile ma on kontrolę nad swoją stroną i swoimi serwerami.

Źródło: nieoficjalne tłumaczenie ze strony francuskiego organu ochrony danych

<https://www.cnil.fr/fr/cookies-sanction-de-50-000-euros-lencontre-de-la-societe-du-figaro>

Francja: 1,75 mln euro kary dla ubezpieczyciela

CNIL nałożyła na Towarzystwo Ubezpieczeń Wzajemnych AG2R LA MONDIALE (SGAM AG2R LA MONDIALE) karę za nieprzestrzeganie obowiązków wynikających z RODO w zakresie okresów zatrzymywania danych i informowania osób fizycznych.

CNIL przeprowadziła w 2019 roku kontrolę w grupie AG2R LA MONDIALE, która miała na celu sprawdzenie zgodności operacji przetwarzania danych przeprowadzonych w kontekście misji zarządzania dodatkowymi emeryturami pracowników sektora prywatnego oraz działalności ubezpieczeniowej.

CNIL stwierdziła, że SGAM AG2R LA MONDIALE – odpowiedzialne za koordynację działalności grupy w zakresie ubezpieczeń emerytalnych, na wypadek śmierci, zdrowotnych, oszczędnościowych i dodatkowych – przechowuje dane milionów osób przez nadmiernie długi okres i nie przestrzega swoich obowiązków informacyjnych w ramach telefonicznych kampanii akwizycyjnych.

CNIL uznała, że przedsiębiorstwo nie wypełniło dwóch podstawowych obowiązków wynikających z RODO w sprawie egzekwowania prawa. Przedsiębiorstwo nie wdrożyło do swoich systemów okresów przechowywania danych. W rezultacie przechowywało ono dane osobowe swoich potencjalnych klientów i klientów przez zbyt długi okres.

Jeśli chodzi o dane potencjalnych klientów, przedsiębiorstwo nie przestrzegało maksymalnego okresu przechowywania danych, wynoszącego trzy lata, określonego w swoim rejestrze i w rejestrze przetwarzania danych grupy. Przechowywano w ten sposób dane prawie dwóch tysięcy klientów, którzy nie mieli kontaktu z firmą przez ponad trzy lata, a czasem nawet pięć lat. W odniesieniu do danych klientów przedsiębiorstwo nie przestrzegało maksymalnych okresów przechowywania przewidzianych przepisami kodeksu ubezpieczeń i kodeksu handlowego.

Ponadto informacje przekazywane telefonicznie przez akwizytorów (przez podmioty przetwarzające) firmy nie zawierały wszystkich elementów wymaganych przez art. 13 i 14 RODO. Nie udzielono potencjalnym klientom żadnych informacji o przetwarzaniu ich danych osobowych ani o innych przysługujących im prawach.

Jednak firma wprowadziła środki mające na celu wpro-

wadzenie niezbędnych zmian, aby spełnić wymogi RODO, po przeprowadzeniu audytu i w trakcie procedury.

Źródło: nieoficjalne tłumaczenie ze strony francuskiego organu ochrony danych

<https://www.cnil.fr/fr/sanction-1-75-million-deuros-ag2r-la-mondiale>



RADA EUROPY

Benin nowym obserwatorem przy Komitecie Konwencji 108

Komitet Konwencji nr 108 Rady Europy 10 września 2021 r. pozytywnie odpowiedział na wniosek Urzędu Ochrony Danych Osobowych Republiki Beninu (APDP) i zdecydował, że umożliwi mu udziału w swoich posiedzeniach. Tym samym Benin stał się **36. obserwatorem** prac Komitetu Konwencji 108.

Nawet bez prawa głosu, uczestnicy Komitetu są cennym źródłem praktycznych doświadczeń z prac tere-

nowych nad kwestiami ochrony danych, a ich opinie i komentarze zasilają jego debaty i prace.

Źródło: nieformalne tłumaczenie ze strony Rady Europy

[https://www.coe.int/en/web/data-protection/-/the-personal-data-protection-authority-apdp-of-benin-at-the-committee-of-convention-108-](https://www.coe.int/en/web/data-protection/-/the-personal-data-protection-authority-apdp-of-benin-at-the-committee-of-convention-108)

TRWAJĄ KONSULTACJE PROJEKTU KODEKSU POSTĘPOWANIA DLA SEKTORA MARKETINGU

Do końca października 2021 roku można zgłaszać uwagi do projektu „Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego” przygotowanego przez Polskie Stowarzyszenie Marketingu SMB.



Polskie Stowarzyszenie Marketingu SMB skierowało do konsultacji społecznych projekt „Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego” (KODO). Dokument ten powstał, by pomóc przedsiębiorcom

z sektora marketingu w przestrzeganiu przepisów o ochronie danych osobowych m.in. poprzez wskazanie, w jaki sposób w praktyce, z uwzględnieniem branżowej specyfiki, stosować ogólne postanowienia RODO.

Jednocześnie może być on przydatny osobom, których dane osobowe są przetwarzane w celach marketingowych. Dzięki niemu będą one mogły zweryfikować, czy podmioty wykorzystujące ich dane osobowe przestrzegają obowiązujących standardów w tym zakresie.

W projekcie kodeksu uregulowano m.in. takie kwestie, jak:

- podstawa prawna przetwarzania danych osobowych do celów marketingu bezpośredniego,
- pozyskiwanie danych osobowych,
- realizacja obowiązku informacyjnego,
- przekazywanie danych osobowych do celów marketingu bezpośredniego,
- przechowywanie danych,
- prawa osób, których dane dotyczą,
- informowanie o naruszeniu ochrony danych osobowych.

Stowarzyszenie uruchomiło specjalną stronę internetową (www.kodo.smb.pl) mającą na celu informowanie o celach KODO, odpowiadającą na kluczowe pytania oraz umożliwiającą zapoznanie się z treścią kodeksu oraz wzięcie udziału w jego konsultacjach.

Ewentualne uwagi do projektu można przysyłać do 31 października 2021 r. na adres kodeks@kodo.smb.pl lub oliwia.prosianowska@smb.pl.

Warto przypomnieć, że choć Prezes UODO zachęca do tworzenia kodeksów postępowania, to nie uczestniczy w procesie konsultacji, który podlega ocenie organu nadzorczego po złożeniu wniosku o zatwierdzenie projektu kodeksu, zgodnie z art. 40 RODO i art. 27 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Dlatego prosimy o nieprzesyłanie uwag do UODO.

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych” w sekcji „Zadania IOD” została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy ze związkiem powiatowo-gminnym należy zawrzeć umowę powierzenia?

Czy przedsiębiorstwo wodociągowe może udostępnić gminie dane na temat ilości zużytej wody?

Jaki jest status rodziny sprawującej pieczę zastępczą?

