ODPOWIEDZIALNOŚĆ ZARZĄDU A KARY NAKŁADANE PRZEZ PREZESA UODO

Spotkanie tematyczne realizowane jest

w ramach projektu instytucjonalnego

„Rozwój FAOW - czyli wzmacniamy głos pozarządowej wsi”

Projekt Forum Aktywizacji Obszarów Wiejskich realizowany jest dzięki dotacji

otrzymanej od Narodowego Instytutu Wolności w ramach Programu Rozwoju Organizacji

Obywatelskich na lata 2018-2030 PROO

UODO I PREZES UODO

- **UODO tj. Urząd Ochrony Danych Osobowych** to organ nadzorczy zajmujący się ochroną danych osobowych.
- **Prezes Urzędu Ochrony Danych Osobowych** (**Prezes UODO**) jest organem nadzorczym, który stoi na straży prawa do ochrony danych osobowych osób fizycznych. Każda osoba fizyczna ma prawo do ochrony danych osobowych jej dotyczących.
- Prezes UODO odpowiada za monitorowanie i egzekwowanie przestrzegania przepisów o ochronie danych osobowych. W przypadku ich nieprzestrzegania przez administratorów, może skorzystać z przysługujących mu uprawnień naprawczych.

STATUS I KOMPETENCJE PREZESA UODO

- Jest niezależnym i jedynym organem umocowanym prawnie do wydawania wytycznych i interpretowania postanowień rozporządzenia o ochronie danych (RODO) i innych przepisów o ochronie danych osobowych.
- Stoi na straży gwarantowanych w Konstytucji RP oraz prawie UE praw podstawowych: prawa do ochrony danych osobowych i prawa do prywatności.
- Dba, by wykorzystywanie danych osobowych odbywało się zgodnie z zasadami przetwarzania danych.
- Podejmuje działania mające na celu podnoszenie świadomości w zakresie ochrony danych osobowych.

- Upowszechnia w społeczeństwie wiedzę o ryzyku, związanym z przetwarzaniem danych.
- Upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o spoczywających na nich obowiązkach związanych z przetwarzaniem danych osobowych.
- Monitoruje i egzekwuje przestrzeganie przepisów o ochronie danych osobowych.
- Rozpatruje skargi wniesione przez osoby, których dane dotyczą.

- Prezes UODO jest organem właściwym do podejmowania czynności w przypadku wystąpienia naruszenia przepisów o ochronie danych osobowych.
- Prezes UODO reaguje odpowiednio do wagi konkretnego naruszenia, korzystając z licznych uprawnień, jakie mu przysługują na podstawie RODO.

UPRAWNIENIA NAPRAWCZE PREZESA UODO

- wydaje ostrzeżenia dotyczące możliwości naruszenia RODO;
- udziela upomnień w przypadku naruszenia RODO;
- nakazuje administratorowi lub podmiotowi przetwarzającemu spełnienie żądania osoby, której dane dotyczą;
- wprowadza czasowe lub całkowite ograniczenia przetwarzania, w tym zakaz przetwarzania;
- nakłada administracyjną karę pieniężną.

ADMINISTRACYJNA KARA PIENIĘŻNA

- Nakładana jest przez Prezesa UODO.
- Zawsze jest zindywidualizowana.
- Poprzedzona jest analizą stanu faktycznego i prawnego na dzień jej wydania.
- Przy jej nałożeniu zawsze uwzględniane są specyficzne okoliczności dotyczące konkretnej sprawy.

- Nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na możliwość zastosowania przez Prezesa UODO innych uprawnień, czy też sankcji.

FUNKCJE KARY

- SKUTECZNA
- PROPORCJONALNA
- ODSTRASZAJĄCA

CZYNNIKI WARUNKUJĄCE WYMIERZENIE KARY

- charakter, waga i czas trwania naruszenia;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego;

- wszelkie stosowne wcześniejsze naruszenia;
- stopień współpracy z Prezesem UODO w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki Prezes UODO dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie (np. czy sam zgłosił „wyciek danych”).

SPOSÓB OBLICZENIA WYSOKOŚCI ADMINISTRACYJNEJ KARY PIENIĘŻNEJ

- Równowartość wyrażonych w euro kwot administracyjnych kar pieniężnych oblicza się według średniego kursu euro ogłaszanego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia każdego roku, kiedy obchodzony jest Dzień Ochrony Danych Osobowych.
- Środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa. Nie zasilają samego Urzędu.

WYSOKOŚĆ ADMINISTRACYJNEJ KARY PIENIĘŻNEJ

- do 10 000 000 euro lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa) za np.: nieprawidłowości w zakresie powierzenia przetwarzania danych; niewłaściwe prowadzenie rejestru czynności przetwarzania lub jego brak; czy niezgłoszenie naruszenia ochrony danych lub niezawiadomienie o naruszeniu osoby, której dane dotyczą.

- do 20 000 000 euro, a w przypadku przedsiębiorstwa - w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, np. za przetwarzanie danych osobowych niezgodnych z zasadami RODO, niedotrzymanie warunku wyrażenia zgody na przetwarzanie danych, niedotrzymanie warunków przetwarzania szczególnych kategorii danych osobowych (tj. np. danych o stanie zdrowia, wyznaniu, orientacji seksualnej), niedopełnienie obowiązku informacyjnego, czy prawa do sprostowania.

- do 100 000 złotych na jednostki sektora finansów publicznych, instytuty badawcze, czy Narodowy Bank Polski.
- do 10 000 złotych na państwowe i samorządowe instytucje kultury.

TERMIN UISZCZENIA KARY PIENIĘŻNEJ

- Administracyjną karę pieniężną uiszcza się **w terminie 14 dni** od dnia upływu terminu na wniesienie skargi do Wojewódzkiego Sądu Administracyjnego w Warszawie albo od dnia uprawomocnienia się orzeczenia sądu administracyjnego.
- Na wniosek podmiotu ukaranego Prezes UODO może odroczyć termin uiszczenia administracyjnej kary pieniężnej albo rozłożyć ją na raty jeżeli przemawia za tym ważny interes wnioskodawcy.

PRZYKŁADY KAR NAŁOŻONYCH PRZEZ PREZESA UODO

1.
KARA ZA NIEPRZESTRZEGANIE NAKAZU DECYZJI ADMINISTRACYJNEJ
sygn. akt: DKE.561.11.2020.

STAN FAKTYCZNY

- Do Urzędu Ochrony Danych Osobowych wpłynęło zgłoszenie naruszenia ochrony danych osobowych z lipca 2019 roku złożone przez Panią M. Z. prowadzącą działalność gospodarczą pod firmą K. W treści zgłoszenia Przedsiębiorca poinformował, że naruszenie polegało na nieuprawnionym skopiowaniu w dniu […] kwietnia 2019 roku danych osobowych stu pacjentów z systemu ([A]) przychodni przez byłego pracownika celem wykorzystania ich do marketingu własnych usług.

NARUSZENIE

- Naruszenie dotyczyło następujących kategorii danych osobowych pacjentów: numeru PESEL, imion i nazwisk, imion rodziców, daty urodzenia, adresu zamieszkania lub pobytu oraz numeru telefonu.

- **Urząd Ochrony Danych Osobowych (UODO) nakazał przedsiębiorcy zawiadomienie jego pacjentów o naruszeniu ich danych osobowych oraz przekazanie tym osobom zaleceń dotyczących zminimalizowania potencjalnych negatywnych skutków zaistniałego incydentu.** Administrator nie wykonał nakazu. W konsekwencji osoby, których dotyczyło naruszenie nic o nim nie wiedziały.
- Wszczęto postępowanie, którego celem było sprawdzenie, czy nałożone w decyzji UODO obowiązki zostały zrealizowane.

INFORMACJE, KTÓRE MIAŁY ZNALEŹĆ SIĘ W ZAWIADOMIENIU:

- opis charakteru naruszenia danych osobowych;
- imię i nazwisko oraz dane kontaktowe do inspektora ochrony danych osobowych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu – w tym środków w celu zminimalizowania jego ewentualnych skutków.

CEL ZAWIADOMIENIA

- Pomoc w zrozumieniu przez osoby, których naruszenie dotyczyło, na czym polegało naruszenie ochrony danych osobowych, poznanie możliwych konsekwencji takiego zdarzenia oraz działań, które można podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków.

CZYNNIKI OBCIĄŻAJĄCE UWZGLĘDNIONE PRZEZ ORGAN

- długotrwały okres trwania naruszenia, co spowodowało zwiększone ryzyko zaistnienia negatywnych konsekwencji po stronie osób dotkniętych naruszeniem;
- umyślny charakter naruszenia i niezadowalający stopień współpracy z organem nadzorczym w celu usunięcia naruszenia – przedsiębiorca nie stosował się do zaleceń Urzędu w trakcie postępowania.

2.
KARA ZA NIEWYSTARCZAJĄCE ZABEZPIECZENIA ORGANIZACYJNE I TECHNICZNE

Morele.net

kara w wysokości ponad 2.830.410,00 złotych.

STAN FAKTYCZNY

- W listopadzie 2018 r. Morele.net Sp. z o. o. z siedzibą w Krakowie przy ul. Fabrycznej 20A (dalej jako: „Spółka”), zgłosiła Prezesowi UODO dwa naruszenia ochrony danych osobowych, które dotyczyły uzyskania przez osobę nieuprawnioną dostępu do bazy danych klientów sklepów internetowych morele.net, hulahop.pl, amfora.pl, pupilo.pl, trenujesz.pl, motoria.pl, digitalo.pl, ubieramy.pl, meblujesz.pl, sklep-presto.pl, budujesz.pl oraz uzyskania przez osobę nieupoważnioną dostępu danych osobowych klientów realizujących zakupy w ww. sklepach internetowych.

NARUSZENIE

- Na podstawie zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Spółka, jako administrator, naruszyła przepisy o ochronie danych osobowych.
- Uchybienia te polegały na: naruszeniu przez Spółkę **zasady poufności danych** polegającym na niezapewnieniu bezpieczeństwa i poufności przetwarzanych danych osobowych co spowodowało, że dostęp do danych osobowych klientów Spółki uzyskały osoby nieuprawnione oraz na naruszeniu **zasady legalności, rzetelności i rozliczalności**, poprzez niewykazanie, że dane osobowe z wniosków ratalnych zbierane przed 25 maja 2018 r. były przetwarzane przez Morele.net Sp. z o. o. na podstawie zgody osoby, której dane dotyczyły.

ZAWIADOMIENIE

- W grudniu 2018 roku Spółka wysłała do klientów 2 200 000 (ok. dwóch milionów dwustu tysięcy) wiadomości mailowych zawierających zawiadomienie o nieuprawnionym dostępie do bazy danych klientów (treść zawiadomienia osób, których dane dotyczą została przesłana do Urzędu w uzupełnieniu zgłoszenia naruszenia). W powyższej informacji kierowanej do klientów Spółka poinformowała, że nie przetwarza danych pochodzących z wniosków kredytowych.

PONOWNE NARUSZENIE

- Mimo skutecznego wysłania zawiadomień w tym samym miesiącu, Spółka zidentyfikowała kolejny nieuprawniony dostęp do danych, wykorzystany do ponownej wysyłki fałszywych smsów, o czym zostało poinformowanych 600 osób, do których danych osoba nieuprawniona miała dostęp. Naruszenie to również zostało zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych.

PONOWNE ZAWIADOMIENIE

- Z uwagi na to, że powiadomienie osób, których dane dotyczą, nie spełniało wymogów, Prezes UODO skierował do Spółki wystąpienie nakazujące ponowne zawiadomienie osób, których dane dotyczą o naruszeniu ich danych osobowych oraz przekazanie tym osobom zaleceń odnośnie zminimalizowania potencjalnych skutków naruszenia.
- Spółka ponownie skierowała zawiadomienie o naruszeniu ochrony danych osobowych do 35 000 (trzydziestu pięciu tysięcy) osób.

CZYNNOSCI KONTROLNE

- W styczniu 2019 r. w celu kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych dokonano czynności kontrolnych w Morele.net Sp. z o. o.
- Zakresem kontroli objęto przetwarzanie danych osobowych klientów sklepów internetowych: morele.net, hulahop.pl, amfora.pl, pupilo.pl, trenujesz.pl, motoria.pl, digitalo.pl, ubieramy.pl, meblujesz.pl, sklep-presto.pl, budujesz.pl, których administratorem jest Spółka.

OCENA I DECYZJA PREZESA UODO

- Przedmiotowe naruszenie poufności, w ocenie Prezesa UODO, należy rozpatrywać z perspektywy dwóch zdarzeń: uzyskania nieuprawnionego dostępu do danych osobowych klientów oraz uzyskania danych wszystkich klientów z systemu bazodanowego Spółki.
- W stanie faktycznym przedmiotowej sprawy, w ocenie Prezesa UODO, nieskuteczny środek uwierzytelniania przyczynił się do zdarzenia polegającego na uzyskaniu nieuprawnionego dostępu danych osobowych klientów.

- Prezes UODO, korzystając z przysługującego mu uprawnienia, zgodnie z którym każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych, administracyjnej kary pieniężnej, mając na względzie okoliczności ustalone w przedmiotowym postepowaniu stwierdził, iż w rozpatrywanej sprawie zaistniały przesłanki uzasadniające nałożenie na Spółkę administracyjnej kary pieniężnej.
- **Decydując o nałożeniu administracyjnej kary pieniężnej Prezes UODO– wziął pod uwagę następujące okoliczności sprawy, wpływające obciążająco i mające wpływ na wymiar nałożonej kary finansowej**:

- Spółka nie dopełniła obowiązku zastosowania odpowiednich środków technicznych i organizacyjnych, by zapewnić stopień bezpieczeństwa odpowiadający ryzyku nieuprawnionego dostępu do danych osobowych jej klientów, co skutkowało dwukrotnym uzyskaniem dostępu do danych osobowych klientów przez osobę bądź osoby nieuprawnione, a w konsekwencji również i dostępu do bazy danych wszystkich klientów Spółki w łącznej liczbie około 2 200 000 (około dwóch milionów dwustu tysięcy) osób;
- W ocenie Prezesa UODO, działania Spółki zmierzające do zapewnienia bezpieczeństwa przetwarzania danych należy były nieskuteczne i nie przyczyniły się one do wyeliminowania ryzyka zaistnienia szkód;

- Spółka jako administrator tych danych powinna podjąć wszelkie niezbędne działania i dochować należytej staranności w doborze środków technicznych i organizacyjnych, zapewniających bezpieczeństwo i poufność danych; poczynione przez Prezesa UODO ustalenia faktyczne dowodzą, iż Spółka w chwili wystąpienia stwierdzonych naruszeń zadaniu temu nie sprostała.

DECYZJA PREZESA UODO

- Prezes Urzędu Ochrony Danych Osobowych uznał, iż nałożenie administracyjnej kary pieniężnej na Spółkę jest konieczne i uzasadnione wagą oraz charakterem i zakresem zarzucanych Spółce naruszeń. W ocenie organu zastosowanie wobec Spółki jakiegokolwiek innego środka naprawczego, w szczególności zaś poprzestanie na upomnieniu, nie byłoby proporcjonalne do stwierdzonych nieprawidłowości w procesie przetwarzania danych osobowych oraz nie gwarantowałoby tego, że Spółka w przyszłości nie dopuści się podobnych, co w sprawie niniejszej zaniedbań.

- Za naruszenia opisane w decyzji, Prezes UODO nałożył na Spółkę – stosując średni kurs euro z dnia 28 stycznia 2019 r. (1 EUR = 4.2885 PLN) – **administracyjną karę pieniężną w kwocie 2 830 410 PLN (co stanowi równowartość 660 000 EUR).**
- W ocenie Prezesa UODO, zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy swoją funkcję tzn. będzie w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

USTALENIE WYSOKOŚCI ADMINSITRACYJNEJ KARY PIENIĘŻNEJ

- **Prezes UODO uwzględnił okoliczności łagodzące, mające wpływ na ostateczny wymiar kary, tj.:**

- podjęcie przez Spółkę wszelkich możliwych działań, mających na celu usunięcie naruszenia;
- dobrą współpracę ze strony Spółki w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków; w wyznaczonym terminie Spółka przesłała wyjaśnienia i udzieliła odpowiedzi na wystąpienie Prezesa UODO – stopień współpracy pełny;

- brak dowodów, aby osoby, których dane dotyczą, doznały szkody majątkowej;
- brak stwierdzenia, żeby Spółka uprzednio dopuściła się naruszenia przepisów, które miałoby istotne znaczenie dla niniejszego postepowania.

Bisnode Sp. z o.o.

STAN FAKTYCZNY

- Kontrola Prezesa UODOA dotyczyła przetwarzania przez Spółkę danych osobowych pozyskiwanych ze źródeł publicznie dostępnych, w tym z rejestrów publicznych (m.in. Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej, Bazy REGON Głównego Urzędu Statystycznego).
- Prezes UODO, zawiadomił Spółkę o wszczęciu z urzędu postępowania administracyjnego w sprawie niedopełnienia obowiązku informacyjnego, o którym mowa w art. 14 rozporządzenia 2016/679 wobec tych osób fizycznych prowadzących działalność gospodarczą, co do których Spółka nie posiadała adresu e-mail w swojej bazie danych, przy czym dotyczy to zarówno przedsiębiorców, którzy aktualnie prowadzą działalność gospodarczą bądź tę działalność zawiesili, jak i o tych, którzy tej działalności już nie prowadzą, lecz prowadzili ją w przeszłości.

NARUSZENIE

- Naruszenie obowiązku informacyjnego wskazanego w art. 14 ust. 1-3 ogólnego rozporządzenia o ochronie danych osobowych, polegającego na niepodaniu informacji zawartych w art. 14 ust. 1 i 2 RODO wszystkim osobom fizycznym, których dane osobowe spółka przetwarza, prowadzącym aktualnie lub w przeszłości jednoosobową działalność gospodarczą oraz osobom fizycznym, które zawiesiły wykonywanie tej działalności.

KARA

- Zastosowanie znajduje art. 83 ust. 5 lit. b rozporządzenia 2016/679, zgodnie z którym naruszenia przepisów dotyczących praw osób, których dane dotyczą (w tym prawa do uzyskania informacji, o których mowa w art. 14 ust. 1 i 2 tego rozporządzenia), podlegają a administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa - w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

- Prezes UODO, na podstawie art. 83 ust. 5 lit. b rozporządzenia 2016/679, w związku z art. 103 Ustawy, za naruszenie opisane w sentencji niniejszej decyzji, **wymierzył Spółce – stosując średni kurs euro z dnia 28 stycznia 2019 r. (1 EUR = 4.2885 PLN) – administracyjną karę pieniężną w kwocie 943.470,00 PLN (co stanowi równowartość 220 000 EUR).**
- W ocenie Prezesa UODO, zastosowana kara pieniężna spełniła w ustalonych okolicznościach przedmiotowej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679 ze względu na powagę stwierdzonych naruszeń w kontekście podstawowych wymogów i zasad rozporządzenia 2016/679 – rzetelności i przejrzystości oraz prawa do informacji.

Dolnośląski Związek Piłki Nożnej

STAN FAKTYCZNY

- W lipcu 2018 r. Dolnośląski Związek Piłki Nożnej z siedzibą we Wrocławiu, zgłosił Prezesowi UODO, naruszenie ochrony danych osobowych polegające na niezamierzonej publikacji danych osobowych osób, którym przyznano licencje sędziowskie w roku 2015, w zakresie imienia, nazwiska, numeru PESEL oraz adresu zamieszkania na stronie internetowej Dolnośląskiego Związku Piłki Nożnej. W powyższym zgłoszeniu DZPN wskazał, że okres naruszenia trwał od października 2015 r. do lipca 2018 r. Przyczyną naruszenia były wewnętrzne działania niezamierzone. W zawiadomieniu wskazano, że osoby, których dane dotyczą zostaną powiadomione o naruszeniu.

- Z uwagi na to, że powiadomienie osób, których dane dotyczyły, nie spełniało wymogów określonych w art. 34 rozporządzenia 2016/679, Prezes UODO wystąpił do DZPN na podstawie art. 52 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, z późn. zm.), o podjęcie działań mających na celu zawiadomienie osób, których dane dotyczą, o naruszeniu ich danych, w tym przekazanie zaleceń odnośnie zminimalizowania potencjalnych negatywnych skutków zaistniałego naruszenia oraz o wyeliminowaniu podobnych nieprawidłowości w przyszłości.

NARUSZENIE

- art. 5 ust. 1 lit. f, art. 32 ust. 1 lit. b i art. 32 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zmianą ogłoszoną w Dz. Urz. UE L 127 z 23.05.2018, str. 2), polegające na niezapewnieniu bezpieczeństwa i poufności przetwarzanych danych osobowych osób, którym przyznano licencje sędziowskie w roku 2015, w zakresie numeru PESEL oraz adresu zamieszkania poprzez ich nieuprawnione ujawnienie na stronie internetowej Dolnośląskiego Związku Piłki Nożnej.

KARA

- Na podstawie art. 83 ust. 3, art. 83 ust. 4 lit. a i art. 83 ust. 5 lit. a rozporządzenia 2016/679, w związku z art. 103 Ustawy, nałożył na DZPN – stosując średni kurs euro z dnia 28 stycznia 2019 r. (1 EUR = 4.2885 PLN) – **administracyjną karę pieniężną w kwocie 55 750,50 PLN (co stanowi równowartość 13.000 EUR).**
- W ocenie Prezesa UODO, zastosowana kara pieniężna spełniła w ustalonych okolicznościach niniejszej sprawy przesłanki, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679 ze względu na wagę stwierdzonych naruszeń w kontekście podstawowych wymogów i zasad rozporządzenia 2016/679 – integralności i poufności.

ClickQuickNow

STAN FAKTYCZNY

- W lutym 2019 r. na podstawie art. 78 ust. 1, art. 79 ust. 1 pkt 1 oraz art. 84 ust. 1 pkt 1-4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych w zw. z art. 57 ust. 1 lit. a oraz h, art. 58 ust. 1 lit. b, e oraz f rozporządzenia 2016/679, w celu kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych, dokonano czynności kontrolnych w ClickQuickNow Sp. z o.o. Zakresem kontroli objęto przetwarzanie przez Spółkę danych osobowych, z wyłączeniem danych dotyczących osób zatrudnionych. Z informacji zawartych w KRS wynika, że przedmiotem prowadzonej przez Spółkę działalności gospodarczej jest przetwarzanie danych, zarządzanie stronami internetowymi (hosting). W procesie przetwarzania danych osobowych Spółka, jako administrator, naruszyła przepisy o ochronie danych osobowych

NARUSZENIE

- art. 5 ust 1 lit. a w zw. z art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. ogólnego rozporządzenia o ochronie danych (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) tj. zasady zgodności z prawem, rzetelności i przejrzystości przetwarzania danych osobowych, oraz art. 7 ust. 3, art. 12 ust. 2, art. 17 ust. 1 lit. b i art. 24 ust. 1 rozporządzenia 2016/679, poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych, które umożliwiałyby osobie, której dane dotyczą, łatwe i skuteczne wycofanie zgody na przetwarzanie swoich danych osobowych oraz realizację prawa do żądania niezwłocznego usunięcia swoich danych osobowych (prawa do bycia zapomnianym),

- art. 5 ust 1 lit. a w zw. z art. 5 ust. 2 rozporządzenia 2016/679, tj. zasady zgodności z prawem, oraz art. 6 ust. 1 rozporządzenia 2016/679, poprzez przetwarzanie bez podstawy prawnej danych osób, które nie są klientami ClickQuickNow Sp. z o.o., a od których ClickQuickNow Sp. z o.o., otrzymała żądania zaprzestania przetwarzania danych osobowych,

KARA

- **Kara pieniężna w kwocie 201 559,50 PLN, co stanowi równowartość 47. 000 EUR, według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia 2019 r.**

Burmistrz Aleksandrowa Kujawskiego

STAN FAKTYCZNY

- W dniach od 28 stycznia do 1 lutego 2019 r. przeprowadzono kontrolę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, tj. z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2) oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781). Zakresem kontroli objęty został sposób przetwarzania danych osobowych przez Burmistrza Aleksandrowa Kujawskiego w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP), a także sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych osobowych.

- W toku kontroli odebrano od pracowników Urzędu Miejskiego w Aleksandrowie Kujawskim ustne wyjaśnienia oraz dokonano oględzin systemów informatycznych służących do przetwarzania danych osobowych i oględzin strony BIP. Stan faktyczny został szczegółowo opisany w protokole kontroli, który został podpisany przez Burmistrza Aleksandrowa Kujawskiego.
- Na podstawie zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Burmistrz, jako administrator, naruszył przepisy o ochronie danych osobowych

NARUSZENIE

- art. 5 ust. 1 lit. a) oraz f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady zgodności z prawem i zasady poufności oraz art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych osobowych poprzez udostępnianie danych osobowych na rzecz T. Sp. z o.o. z siedzibą w T. oraz na rzecz konsorcjum podmiotów: W. S.A. z siedzibą w G. oraz C. S.A. z siedzibą w K. bez podstawy prawnej, tj. bez uprzedniego zawarcia z ww. podmiotami umów powierzenia danych osobowych, o której mowa w art. 28 ust. 3 ogólnego rozporządzenia o ochronie danych, w związku z prowadzeniem strony internetowej Biuletynu Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim,

- art. 5 ust. 1 lit. e) w zw. z art. 5 ust. 2, tj. zasady ograniczenia przechowywania, oraz art. 24 ogólnego rozporządzenia o ochronie danych poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w Biuletynie Informacji Publicznej Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych,
- art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady integralności i poufności, zasady prawidłowości, oraz art. 24 ogólnego rozporządzenia o ochronie danych poprzez nieprzeprowadzenie analizy ryzyka związanego z korzystaniem przez Burmistrza Aleksandrowa Kujawskiego z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta Aleksandrowa Kujawskiego,

- art. 5 ust. 1 lit. f) w zw. z art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady integralności i poufności, oraz art. 32 ogólnego rozporządzenia o ochronie danych poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta Aleksandrowa Kujawskiego wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim.

- art. 5 ust. 2 ogólnego rozporządzenia o ochronie danych, tj. zasady rozliczalności, oraz art. 30 ust. 1 lit. d) oraz f) ogólnego rozporządzenia o ochronie danych poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych, dla czynności związanych z publikacją informacji na stronie Biuletynu Informacji Publicznej Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania,

KARA

- **Administracyjna kara pieniężna w kwocie 40.000 zł.**
- Decydując, czy nałożyć administracyjną karę pieniężną, a także ustalając jej wysokość, za najistotniejsze Prezes UODO uznał poważny charakter naruszenia wynikający z udostępnienia danych osobowych bez podstawy prawnej innym podmiotom oraz naruszenie zasady rozliczalności.
- Ponadto, Prezes UODO wziął pod uwagę, iż oceniany organ jest jednostką sektora publicznego, a szacując wysokość kary wziął pod uwagę także wysokość jej budżetu na rok 2018 r., sposób jego realizacji oraz budżet na rok 2019 r.
- W tym miejscu wskazać również należy na treść art. 102 ustawy o ochronie danych osobowych, z którego wynika ograniczenie wysokości (do 100.000 zł) kary, jaka może zostać nałożona na jednostkę sektora publicznego.

East Power Sp. z o.o.

STAN FAKTYCZNY

- Do Urzędu Ochrony Danych Osobowych wpłynęła skarga Pana D. S., obywatela Niemiec, zamieszkałego w N. na przetwarzanie przez East Power Sp. z o.o. z siedzibą w Jeleniej Górze właściciela serwisu internetowego www. […].de, jego danych osobowych w celach marketingowych pomimo zgłoszonego sprzeciwu.
- W związku z nieudzieleniem przez Spółkę informacji niezbędnych do rozstrzygnięcia sprawy, Prezes UODO wszczął z urzędu wobec Spółki – w oparciu o art. 83 ust. 5 lit. e) Rozporządzenia 2016/679, w związku z naruszeniem przez Spółkę art. 58 ust. 1 lit a) i e) Rozporządzenia 2016/679 – postępowanie administracyjne w przedmiocie nałożenia na Spółkę administracyjnej kary pieniężnej.

NARUSZENIE

- art. 58 ust. 1 lit. e) Rozporządzenia 2016/679, polegające na niezapewnieniu dostępu do danych osobowych i innych informacji niezbędnych Prezesowi Urzędu Ochrony Danych Osobowych do realizacji jego zadań, to jest do rozpatrzenia skargi Pana D. S. na niezgodne z przepisami Rozporządzenia 2016/679 przetwarzanie przez East Power Sp. z o.o. z siedzibą w Jeleniej Górze jego danych osobowych,

KARA

- **administracyjna kara pieniężna w kwocie 15.000 PLN, co stanowi równowartość 3.505,16 EUR, według średniego kursu euro ogłoszonego przez Narodowy Bank Polski w tabeli kursów na dzień 28 stycznia 2020 r.**

Smart Cities Sp. z o.o.

STAN FAKTYCZNY

- Do Urzędu Ochrony Danych Osobowych wpłynęła skarga Pana K. T. na nieprawidłowości w procesie przetwarzania jego danych osobowych przez Smart Cities Sp. z o.o. W związku z nieudzieleniem przez Spółkę pełnych informacji niezbędnych do rozstrzygnięcia sprawy zainicjowanej skargą Skarżącego, Prezes UODO wszczął z urzędu wobec Spółki – w oparciu o art. 83 ust. 5 lit. e) Rozporządzenia 2016/679, w związku z naruszeniem przez Spółkę art. 31 oraz art. 58 ust. 1 lit a) i e) Rozporządzenia 2016/679 – postępowanie administracyjne w przedmiocie nałożenia na Spółkę administracyjnej kary pieniężnej.

- O wszczęciu postępowania Spółka poinformowana została pismem z września 2020 r., które w październiku 2020 r. zostało zwrócone do nadawcy z adnotacją „zwrot nie podjęto awizowanej przesyłki w terminie”. Pismem tym Spółka wezwana została również – celem ustalenia podstawy wymiaru kary, w oparciu o art. 101a ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) – do przedstawienia sprawozdania finansowego Spółki za rok 2019 lub – w przypadku jego braku – oświadczenia o wysokości obrotu i wyniku finansowego osiągniętego przez Spółkę w 2019 r.

NARUSZENIE

- art. 31 i art. 58 ust. 1 lit. e) Rozporządzenia 2016/679, polegające na braku współpracy z Prezesem UODO w ramach wykonywania przez niego jego zadań oraz na niezapewnieniu dostępu do danych osobowych i innych informacji niezbędnych Prezesowi UODO do realizacji jego zadań,

KARA

- **Administracyjna kara pieniężna w kwocie 12.838,20 PLN.**

Krajowa Szkoła Sądownictwa i Prokuratury

STAN FAKTYCZNY

- W kwietniu 2020 r. Krajowa Szkoła Sądownictwa i Prokuratury zgłosiła Prezesowi UODO naruszenie ochrony danych osobowych. W zgłoszeniu naruszenia wskazano, że w kwietniu 2020 r. administrator został powiadomiony przez Komendę Główną Policji o pojawieniu się w Internecie danych osobowych związanych z domeną kssip.gov.pl. Tego samego dnia administrator stwierdził naruszenie ochrony danych osobowych. Po zapoznaniu się z rodzajem danych ustalił, że są to dane z bazy danych witryny szkolenia.kssip.gov.pl powstałe w lutym 2020 r. w trakcie testowej migracji do nowej platformy szkoleniowej ekssip.kssip.gov.pl. Naruszenie dotyczyło danych osobowych 50 283 osób. Kategorie danych, których dotyczy naruszenie, zostały wskazane w zgłoszeniu obejmują: imię i nazwisko, adres e-mail, nazwa użytkownika, numer telefonu, jednostka, wydział, adres jednostki, miejscowość, dane o charakterze technicznym: adres IP, data pierwszego i ostatniego logowania, hasło (w postaci niejawnej).

NARUSZENIE

- art. 5 ust. 1 lit. f), art. 25 ust. 1, art. 28 ust. 3, art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 ze zm.), polegające na niezrealizowaniu obowiązków ciążących na administratorze, wynikających z rozporządzenia 2016/679, poprzez:

- niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, brak przetestowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury, a tym samym niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania,

- powierzenie przetwarzania danych osobowych z naruszeniem art. 28 ust. 3 rozporządzenia 2016/679, tj. bez umownego zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, a także bez określenia w umowie powierzenia przetwarzania danych osobowych kategorii osób oraz bez doprecyzowania rodzaju danych osobowych przez wskazanie ich kategorii.

KARA

- **Administracyjna kara pieniężna w wysokości 100 000 PLN.**
- W ocenie Prezesa UODO zastosowana administracyjna kara pieniężna spełnia w ustalonych okolicznościach niniejszej sprawy funkcje, o których mowa w art. 83 ust. 1 rozporządzenia 2016/679, tzn. jest w tym indywidualnym przypadku skuteczna, proporcjonalna i odstraszająca.

PODSUMOWANIE

- UODO, czyli Urząd Ochrony Danych Osobowych to organ nadzorczy zajmujący się ochroną danych osobowych. W praktyce jego prezes egzekwuje stosowanie postanowień unijnego rozporządzenia RODO oraz prowadzi związane z nimi postępowania. Jednym z jego uprawnień jest nakładanie kar administracyjnych
- Sankcje za złamanie RODO oraz innych regulacji chroniących prywatność obywateli i ich dane osobowe są nakładane w drodze decyzji administracyjnej.

- Każda sprawa rozpatrywana jest oddzielnie, z uwzględnieniem okoliczności popełnionego czynu.
- Decyzja Prezesa UODO powinna być dostosowana do wagi naruszenia
- W przypadku zasądzenia kary pieniężnej, ukarany musi uregulować ją w ciągu 14 dni od momentu uprawomocnienia się orzeczenia.
- Od decyzji prezesa UODO można się odwołać do sądu administracyjnego