Obserwuj nas na:

Nr 4/2020 (13)
Kwiecień 2020

UODO
URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

COVID-19 – OCHRONA DANYCH W CZASACH PANDEMII

Prezes UODO: Przepisy o ochronie danych osobowych nie mogą być stawiane jako przeszkoda w realizacji działań w związku z walką z koronawirusem.

Prezes UODO informuje, że kwestie związane z przetwarzaniem danych dotyczących zdrowia na skutek działań zapobiegających rozprzestrzenianiu się wirusa COVID-19 regulowane są w przepisach szczególnych, w tym przede wszystkim w tzw. specustawie.

Wskazane przepisy nie stoją w sprzeczności z zasadami przetwarzania danych i nie naruszają RODO, a korespondują z rozporządzeniem, które również przewidują sytuacje związane z ochroną zdrowia i zapobieganiem rozprzestrzeniania się chorób zakaźnych (art. 9 ust. 2 lit i art. 6 ust. 1 lit d).

Treść oświadczenia: https://uodo.gov.pl/pl/138/1456

OŚWIADCZENIE PRZEWODNICZĄCEJ EROD WS. PRZETWARZANIA DANYCH PODCZAS PANDEMII COVID-19

Europejska Rada Ochrony Danych 19 marca przyjęła oficjalne oświadczenie w sprawie przetwarzania danych osobowych w kontekście wybuchu wirusa COVID-19. W oświadczeniu przyjęto, że rządy, organizacje publiczne i prywatne w całej Europie podejmują środki mające na celu ograniczenie i złagodzenie skutków pandemii COVID-19. Może się to wiązać z przetwarzaniem różnego rodzaju danych osobowych.

Zasady ochrony danych (takie jak RODO) nie ograniczają środków podejmowanych w ramach walki z pandemią koronawirusa. Walka z chorobami zakaźnymi jest wspólnym celem dla wszystkich narodów i dlatego powinna być wspierana w najlepszy możliwy sposób. W interesie ludzkości leży ograniczenie rozprzestrzeniania się chorób i wykorzystanie nowoczesnych technik w walce z plagami dotykającymi znaczną część świata. Mimo to EROD chciałaby podkreślić, że nawet w tych wyjątkowych czasach administrator i podmiot przetwarzający muszą zapewnić ochronę danych osobowych osób, których dane dotyczą.

Treść oświadczenia została opublikowana na stronie EROD: https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en

Polskie tłumaczenie oświadczenia znajduje się na stronie UODO: https://uodo.gov.pl/pl/138/1463

OCHRONA DANYCH OSOBOWYCH PODCZAS PRACY ZDALNEJ

Środki kontroli i zapobiegania rozprzestrzenianiu się COVID-19 będą wymagały większej liczby osób pracujących zdalnie niż zwykle. Poniżej znajduje się kilka porad dotyczących bezpieczeństwa danych osobowych podczas pracy poza biurem.

Jak postępować podczas pracy zdalnej, aby nie naruszyć przepisów o ochronie danych? Jakie zabezpieczenia rekomendować pracownikom?

Wskazówki UODO: https://uodo.gov.pl/pl/138/1459

UODO DLA SZKÓŁ

Nadzwyczajna sytuacja spowodowała, że szkoły i nauczyciele musieli w bardzo krótkim czasie zorganizować efektywną komunikację z uczniami i ich rodzicami. Wiele szkół do tej pory nie wykorzystywało narzędzi umożliwiających prowadzenie zajęć zdalnych, teraz muszą szybko skorzystać z dostępnych i możliwych w tych warunkach rozwiązań. Korzystając z nich warto poznać rekomendacje i dobre praktyki, aby przetwarzanie danych było bezpieczne.

UODO przygotowało wskazówki dla przedstawicieli oświaty jak korzystając z metod nauczania online, dbać o bezpieczne przetwarzanie danych. A dzięki wsparciu Ministerstwa Edukacji Narodowej opracowanie trafi do wszystkich szkół i placówek oświatowych.

Poradnik do pobrania: https://uodo.gov.pl/pl/138/1473

POTRZEBNE REKOMENDACJE KNF CO DO ZASADNOŚCI KOPIOWANIA DOKUMENTÓW TOŻSAMOŚCI PRZEZ INSTYTUCJE ZOBOWIĄZANE

Prezes Urzędu Ochrony Danych Osobowych zwrócił się do przewodniczącego Komisji Nadzoru Finansowego o rozważenie wydania rekomendacji w zakresie wypełniania obowiązku weryfikacji tożsamości klienta przez instytucje obowiązane.

Instytucje zobowiązane to podmioty wskazane w art. 2 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, takie jak m.in. banki, spółdzielcze kasy oszczędnościowo-kredytowe czy krajowe instytucje płatnicze.

Prezes UODO wskazał, że otrzymuje liczne sygnały, iż praktyką wielu z tych instytucji jest kopiowanie -na potrzeby weryfikacji tożsamości klientów- dowodów osobistych przy niemal każdej czynności. Powołują się one przy tym na art. 34 ust. 4 wymienionej ustawy, w myśl którego instytucje obowiązane mogą przetwarzać informacje zawarte w dokumentach tożsamości klienta i osoby upoważnionej do działania w jego imieniu oraz sporządzać ich kopie.

Działania te budzą jednak zastrzeżenia Prezesa UODO, w opinii którego stosowanie przez instytucje obowiązane tego typu środków bezpieczeństwa powinno mieć miejsce jedynie w sytuacjach wskazanych w art. 35 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Prezes UODO zauważa ponadto, że art. 34 ust. 1 pkt 1 ustawy, określający środki bezpieczeństwa finansowego stanowi, że środkiem tym jest m.in. identyfikacja klienta oraz weryfikacja jego tożsamości, a nie kopiowanie dokumentu tożsamości. Kopiowanie, o którym mowa w art. 34 ust. 4 ustawy, należy uznać za uprawnienie przysługujące podmiotom obowiązanym. Nie można zatem uznać, że na podmiotach obowiązanych spoczywa obowiązek każdorazowego kopiowania dokumentów tożsamości, choć podmioty te – co do zasady, w zgodzie z powołanymi przepisami - mają prawo z takiego instrumentu korzystać.

W ocenie organu nadzorczego każdorazowa decyzja o skopiowaniu dokumentu tożsamości czy też żądanie przedstawienia takich kopii powinny być poprzedzone analizą i zweryfikowaniem, także z uwzględnieniem przepisów RODO, w tym określonych w nich zasad legalizmu, celowości, minimalizacji i ograniczenia czasowego, czy rzeczywiście taka czynność jest niezbędna.

Wobec tych wątpliwości, Prezes UODO już 10 września 2019 r. skierował do Generalnego Inspektora Informacji Finansowej zapytanie, czy organ ten oczekuje od instytucji obowiązanych przedkładania – jako potwierdzenie wypełnienia obowiązku identyfikacji klienta – kserokopii dokumentów tożsamości, ewentualnie innych dokumentów.

W odpowiedzi Generalny Inspektor Informacji Finansowej przyznał, że kopiowanie dokumentów tożsamości jest uprawnieniem przyznanym instytucjom obowiązanym na mocy ustawy (...) istnieją również inne, alternatywne sposoby udokumentowania dokonanej przez instytucję obowiązaną weryfikacji przeprowadzonej identyfikacji klienta czy osoby upoważnionej do działania w jego imieniu jak np. dokumentem zatwierdzonym podpisem pracownika, który spisał dane osobowe z dokumentu tożsamości na potrzeby konkretnej weryfikacji danych (...). Generalny Inspektor Informacji Finansowej nie wymaga od tych podmiotów obowiązanych w każdym przypadku przedkładania kopii dokumentów tożsamości jako potwierdzenia spełnienia obowiązku identyfikacji klienta określonej w art. 34 ust. 1 pkt 1 ustawy.

Ponieważ praktyka instytucji obowiązanych jest inna, w ocenie Prezesa UODO pomocne dla podmiotów obowiązanych byłyby zatem rekomendacje wydane przez odpowiedniego regulatora, które określiłyby, kiedy pozyskiwanie kopii dokumentów tożsamości jest zasadne, kiedy skorzystać na te potrzeby z innych i jakich narzędzi. Brak jednolitych standardów w tym obszarze generuje wątpliwości zarówno podmiotów obowiązanych, jak i klientów, którzy proszeni są o przedkładanie kopii dokumentów tożsamości na podstawie ustawy.

NIE KAŻDY POWINIEN MIEĆ DOSTĘP DO NUMERU PESEL ZAMIESZCZANEGO W CENTRALNYM REJESTRZE BENEFICJENTÓW RZECZYWISTYCH

Opiniowanie projektu ustawy o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw stało się dla Prezesa UODO okazją, by zwrócić uwagę na konieczność zmiany obowiązujących już przepisów tej ustawy, tak by zapewnić właściwą ochronę numeru PESEL.

Do Urzędu Ochrony Danych Osobowych wpływa wiele sygnałów dotyczących zakresu danych osobowych, które należy zamieszczać w Centralnym Rejestrze Beneficjentów Rzeczywistych. Ponieważ Rejestr ten jest jawny, oznacza to, że dostęp do niego jest nieograniczony. Zatem każdy może mieć dostęp do danych osobowych w nim zgromadzonych, w tym do numerów PESEL.

W opinii Prezesa UODO, przepisy krajowe - wdrażające unijne regulacje dotyczące przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu i nakładające na kraje członkowskie obowiązek utworzenia wspomnianego rejestru - powinny zapewniać właściwą ochronę danych osobowych przetwarzanych w tym rejestrze. Przewiduje to zresztą wprost motyw 14 Dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu. Stanowi on, że: Państwa członkowskie powinny również zagwarantować, by inne osoby mogące wykazać uzasadniony interes w odniesieniu do informacji dotyczących prania pieniędzy, finansowania terroryzmu i powiązanych przestępstw - takich jak korupcja, przestępstwa podatkowe i oszustwa – otrzymały dostęp do informacji o beneficjentach rzeczywistych, **z poszanowaniem zasad ochrony danych**.

W ocenie Prezesa UODO rozważenia wymaga wprowadzenie do ustawy o przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu takich zmian, aby zapewnić dostęp do danych z rejestru wyłącznie osobom posiadającym interes prawny czy faktyczny.

Pozwoliłoby to zapobiec niebezpieczeństwu pozyskiwania danych z rejestru, zwłaszcza numeru PESEL, w niezgodnych z prawem celach. Jednocześnie zapewniłoby zgodność krajowych przepisów z art. 87 RODO zobowiązującym do zapewnienia szczególnej ochrony krajowego numeru identyfikacyjnego, jakim w Polsce jest numer PESEL.

JAK NALEŻY WYWIĄZAĆ SIĘ Z OBOWIĄZKU INFORMACYJNEGO PRZY ZASTOSOWANIU FOTOPUŁAPEK?

DO UODO ze swoimi wątpliwościami zgłosił się inspektor ochrony danych w sprawie obowiązku informacyjnego przy zastosowaniu fotopułapek. Gmina w ramach walki z dzikimi wysypiskami śmieci planuje zakup kilku tzw. foto-pułapek z czujnikami ruchu, które uaktywnią się w momencie zarejestrowania ruchu i nagrają np. osoby które nielegalnie pozbywają się odpadów wysypując je np. na polu, na nieużytkach gminnych czy innych ustronnych miejscach. Nagrania takie będą przeglądane przez upoważnione osoby. Jeżeli zostanie zarejestrowany fakt nielegalnego pozbywania się odpadów nagranie zostanie wykorzystane jako dowód np. w postępowaniu mandatowym (stanowi to bowiem wykroczenie).

Czy w tej sytuacji należy wypełnić obowiązek informacyjny? Jeśli tak to w jakiej formie? Opublikowanie informacji na obszarze gminy mobilnych foto-pułapek wraz ze stosowną klauzulą informacyjną na stronie BIP oraz własnej stronie internetowej gminy? Upublicznienia informacji poprzez media lokalne (internet, radio, prasa)?

Przepisy RODO określają ogólne zasady przetwarzania i ochrony danych osobowych, zaś skonkretyzowanie tychże zasad ma miejsce w szczególnych wobec tej regulacji przepisach prawa. Kwestie stosowania monitoringu wizyjnego przez jednostki samorządu terytorialnego są regulowane następującymi przepisami: art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 4b ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym, art. 60a ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa. Każdy z ww. artykułów zawiera identycznie brzmiący ustęp, zgodnie z którym nieruchomości i obiekty budowlane objęte monitoringiem oznacza się w sposób widoczny i czytelny informacją o monitoringu, w szczególności za pomocą odpowiednich znaków.

W związku z powyższym trzeba uznać, iż stosowanie przez jednostki samorządu terytorialnego gminy i powiatu monitoringu wizyjnego w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, a w przypadku jednostek samorządu województwa w celu ochrony mienia, wymaga zawsze spełnienia obowiązku informacyjnego poprzez oznaczenie nieruchomości i obiektów budowlanych w sposób widoczny i czytelny informa-

cjami o monitoringu, w szczególności za pomocą odpowiednich znaków. Zwolnienie z tego obowiązku może nastąpić jedynie na mocy osobnych postanowień rangi ustawowej, ograniczających konieczność wypełniania obowiązku informacyjnego w przypadku przetwarzania danych osobowych za pomocą monitoringu wizyjnego w określonym celu.

Prawo do stosowania monitoringu posiadają straże gminne, które w ramach swoich uprawnień, wynikających z przepisów prawa, nie są zobowiązane do spełnienia obowiązku informacyjnego (przysługuje im bowiem uprawnienie do obserwowania i rejestrowania bez wiedzy i zgody osoby, której dane te dotyczą). Natomiast gmina - zgodnie z wyżej przytoczonymi zasadami - musiałaby spełnić obowiązek informacyjny w miejscu umieszczenia fotopułapki.

Cala treść odpowiedzi na pytanie znajduje się pod linkiem: https://uodo.gov.pl/pl/225/1447

POWIADOMIENIA DOTYCZĄCE IOD LUB JEGO ZASTĘPCY NALEŻY SKŁADAĆ TYLKO W POSTACI ELEKTRONICZNEJ

Przypominamy, że kierowane do UODO zawiadomienia dotyczące IOD lub zastępcy IOD muszą mieć postać elektroniczną. Przesłanie zgłoszenia w innej postaci jest bezskuteczne.

Podmiot, który wyznaczył inspektora ochrony danych ma obowiązek zawiadomić o tym Prezesa UODO w terminie 14 dni od dnia wyznaczenia w trybie określonym w art. 10 ustawy o ochronie danych osobowych. Ta sama zasada dotyczy powiadomień o zmianie zgłaszanych danych oraz do powiadomienia o odwołaniu inspektora. Analogicznie należy postąpić – zgodnie z art. 11a tej ustawy – w przypadku powiadomień dotyczących zastępcy inspektora ochrony danych.

W dalszym ciągu zdarza się, że kierowane do UODO zawiadomienia dotyczące inspektorów ochrony danych lub zastępców inspektorów ochrony danych (związane z wyznaczeniem, odwołaniem lub zmianą danych kontaktowych IOD lub zastępcy IOD) mają nieprawidłową postać. Tymczasem jedynym prawidłowym i skutecznym sposobem powiadomienia jest przesłanie zawiadomienia w postaci elektronicznej opatrzonego elektronicznym podpisem kwalifikowanym albo profilem zaufanym ePUAP przez osobę lub osoby upoważnione do reprezentowania administratora. Przesłanie zgłoszenia w innej postaci, nie jest traktowane jako wywiązanie się z obowiązku określonego w art. 10 ustawy o ochronie danych osobowych.

Odpowiednie elektroniczne formularze dostępne są na portalu biznes.gov.pl lub jako pismo ogólne w systemie ePUAP (linki do wszystkich formularzy dostępne są na dole naszej strony internetowej). Skutecznie dostarczone do UODO (za pośrednictwem powyższych portali) zawiadomienia są potwierdzane zgłaszającemu Urzędowym Poświadczeniem Przedłożenia generowanym automatycznie przez biznes.gov.pl lub epuap.gov.pl w postaci pliku UPP.xml.

EROD

Nowe terminy zakończenia konsultacji społecznych

Przewodnicząca EROD przedłużyła termin aktualnie prowadzonych konsultacji społecznych o sześć tygodni.

Decyzja ta związana jest z trwającą pandemią COVID-19. Przedłużenie terminów konsultacji społecznych dotyczy następujących wytycznych:

- wytyczne 1/2020 w sprawie przetwarzania danych osobowych w kontekście pojazdów połączonych, do 1 maja 2020 r.

- wytyczne 2/2020 w sprawie przekazywania danych osobowych między państwami trzecimi lub organizacjami międzynarodowymi z EOG i spoza EOG (art. 46 ust. 2 lit. a) i art. 46 ust. 3 lit. b) RODO) – do 18 maja 2020 r.

Więcej informacji na temat publicznych konsultacji znajduje się na stronie internetowej Europejskiej Rady Ochrony Danych: https://edpb.europa.eu/our-work-tools/public-consultations-art-704_en

MIĘDZYNARODOWE

Strategia przeprowadzenia kontroli przez CNIL na 2020 rok

W 2020 r., poza kontrolami wynikającymi ze skarg, CNIL skoncentruje swoje działania kontrolne na trzech priorytetowych zagadnieniach związanych z codziennymi problemami Francji: danych dotyczących zdrowia, geolokalizacji dla usług lokalnych oraz ciasteczek i innych technologii śledzących.

CNIL przeprowadza czynności dochodzeniowych, w szczególności poprzez rozpatrywanie skarg, zajmowanie się zgłoszeniami dotyczącymi naruszeń danych osobowych lub wszczynanie formalnych procedur kontrolnych. Te ostatnie, których jest 300 rocznie, umożliwiają bardziej dogłębne badanie skarg, reagowanie na aktualne kwestie, zapewnianie zgodności z wcześniejszymi środkami naprawczymi lub badanie niektórych tematów uznanych za priorytetowe.

Spośród tych formalnych procedur kontroli ponad pięćdziesiąt zostanie przeprowadzonych w ramach trzech tematów wybranych jako priorytetowe na rok 2020:

• **Bezpieczeństwo danych dotyczących zdrowia.** Najnowsze wiadomości w dziedzinie zdrowia wskazują na konieczność zwrócenia uwagi na bezpieczeństwo przetwarzania danych medycznych. CNIL pragnie skupić się na środkach bezpieczeństwa wdrażanych przez pracowników służby zdrowia lub w ich imieniu.

• **Urządzenia mobilne a usługi lokalne, nowe zastosowania danych geolokalizacyjnych.** Opracowywane są liczne rozwiązania mające na celu ułatwienie życia codziennego: rekomendowanie środków transportu dostosowanych według określonej trasy, optymalizacja tras podróży itp. Rozwiązania te najczęściej wykorzystują dane geolokalizacyjne i potencjalnie zwiększają zagrożenie dla prywatności. Kontrole będą

zatem obejmować w szczególności proporcjonalność danych gromadzonych w tym kontekście, określone okresy przechowywania danych, informacje przekazywane osobom fizycznym oraz wdrożone środki bezpieczeństwa.

• **Zgodność z przepisami mającymi zastosowanie do ciasteczek i innych technologii śledzących.** Działania kontrolne mają na celu zapewnienie pełnego przestrzegania obowiązków w zakresie śledzenia użytkowników Internetu za pomocą plików cookie lub innych technologii śledzących, zwłaszcza wykorzystywanych do targetowania reklam i profilowania użytkowników.

Kontrole dotyczące tych nowych obowiązków rozpoczną się zatem jesienią 2020 r. i będą kontynuowane w 2021 r.

Źródło: https://www.cnil.fr/fr/quelle-strategie-de-controle-pour-2020

KARY

Szwecja: Google z karą w wysokości 75 mln koron szwedzkich

Szwedzki organ ochrony danych osobowych nałożył na Google karę w wysokości 75 mln koron szwedzkich (w przybliżeniu 7 mln euro) za niestosowanie się do przepisów RODO. Google jako operator wyszukiwarki internetowej nie spełnił obowiązków związanych z prawem do usunięcia danych.

W 2017 roku szwedzki organ nadzorczy zakończył audyt dotyczący sposobu, w jaki Google uwzględnia prawo osób, których dane dotyczą, do usunięcia ich danych z wyników wyszukiwarki Google w przypadku np. braku prawidłowości, ich właściwości czy zbędności. W swojej decyzji organ nadzorczy stwierdził konieczność usunięcia szeregu wyników wyszukiwania i nakazał Google spełnienie powyższego.

W roku 2018, w związku ze stwierdzeniem, że Google nie zastosowało się w pełni do uprzednio wystosowanego nakazu, organ nadzorczy wdrożył kolejny audyt. Obecnie jest on finalizowany, zaś organ nadzorczy nakłada na Google karę pieniężną.

- Ogólne rozporządzenie o ochronie danych, RODO, podnosi poziom odpowiedzialności organizacji, które zbierają i przetwarzają dane osobowe oraz wzmacnia prawa jednostek. Istotną część tych praw stanowi możliwość usunięcia wyników wyszukiwania w internecie. Ustaliliśmy, że Google nie wykonuje w pełni swoich obowiązków w zakresie tych praw - stwierdza Lena Lindgren Schelin, Dyrektor Generalna szwedzkiego organu nadzorczego.

Organ ten w sposób krytyczny odniósł się do faktu, że Google nie usunęło w odpowiedni sposób dwóch z wyników wyszukiwania, które miało usunąć jeszcze w 2017 roku.

Google może złożyć apelację od decyzji szwedzkiego organu nadzorczego w terminie trzech tygodni. Jeśli zdecyduje się nie składać apelacji, decyzja wejdzie w życie wraz z zakończeniem ww. okresu.

Źródło: https://edpb.europa.eu/news/national-news/2020/swedish-data-protection-authority-imposes-administrative-fine-google_en

Pełna treść noty prasowej dostępna jest w języku szwedzkim: https://www.datainspektionen.se/nyheter/datainspektionen-utfardar-sanktionsavgift-mot-google/

Pełna treść decyzji (w języku szwedzkim) dostępna jest na stronie: https://www.datainspektionen.se/nyheter/datainspektionen-utfardar-sanktionsavgift-mot-google/

Kara za uniemożliwienie przeprowadzenia kontroli
Prezes UODO nałożył 20 tys. zł. kary na spółkę związaną z branżą telemarketingową, za uniemożliwienie przeprowadzenia kontroli. Dodatkowo właścicielowi spółki grozi za to odpowiedzialność karna.

Prezes UODO podjął decyzję o przeprowadzeniu czynności kontrolnych w ukaranej spółce, w związku z ustaleniami dokonanymi w toku innej przeprowadzonej kontroli w firmie, która prowadzi działalność telemarketingową. Ustalono, że firma ta ma podpisaną z Vis Consulting Sp. z o.o. umowę o współpracy w zakresie outsorcingu usług telemarketingowych. Dlatego też, organ nadzorczy uznał za konieczne przeprowadzenie czynności kontrolnych w podmiocie, który faktycznie wykonywał połączenia telefoniczne i przetwarzał dane.

Niestety, kontrolerzy UODO, pod wskazanym w KRS adresem i po uprzednim zawiadomieniu o planowanej kontroli, nikogo nie zastali. Na miejscu była jedynie firma, która wynajmowała na rzecz Vis Consulting Sp. z o.o. powierzchnię biurową (tzw. wirtualne biuro).

Kontrolerom udało się jednak telefonicznie skontaktować z Vis Consulting, a jej pełnomocnik poinformował, że kontrola się nie odbędzie.

Treść decyzji dostepna na stronie internetowej UODO: https://uodo.gov.pl/pl/138/1480

Szkoła z karą za odciski palców uczniów
Prezes Urzędu Ochrony Danych Osobowych nałożył karę w wysokości 20 tys. zł w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki.

Szkoła przetwarzała dane szczególnych kategorii (dane biometryczne) 680 dzieci bez podstawy prawnej, mogąc jednocześnie zastosować inne formy identyfikacji uczniów.

Za to naruszenie została nałożona administracyjna kara pieniężna na Szkołę Podstawową nr 2 z Gdańska. Ponadto Prezes UODO nakazał jej usunięcie danych osobowych przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci oraz zaprzestanie dalszego zbierania danych osobowych.

Więcej na temat nałożonej kary na stronie internetowej: https://uodo.gov.pl/pl/138/1453

Islandzki organ: Naruszenie ochrony danych osobowych w szkole ponadgimnazjalnej w Breiðholt
Islandzki organ nadzorczy podjął decyzję o nałożeniu kary administracyjnej w wysokości 1.300.000 koron islandzkich (8945 euro) na szkołę ponadgimnazjalną w Breiðholt w związku z naruszeniem ochrony danych osobowych.

Naruszenie nastąpiło, gdy jeden z nauczycieli wysłał e-mail do uczniów i ich rodziców/opiekunów (łącznie 57 osób). W załączniku e-maila znajdował się dokument, który – jak uważał nauczyciel – zawierać miał informacje w sprawie spotkań konsultacyjnych. Jednakże załącznik ten dotyczył innej grupy uczniów (łącznie 18) i mieścił dane dotyczące ich dobrostanu, wyników w nauce oraz warunków społecznych. W znaczącym stopniu informacje to odnosiły się do problemów uczniów. W jednym z przypadków dane miały związek z interwencją służb ochrony dzieci. Dane dotyczyły ponadto choroby jednego z uczniów oraz problemu psychicznego innego ucznia.

Po przeprowadzeniu postępowania w sprawie naruszenia organ nadzorczy stwierdził, że było ono wynikiem braku wprowadzenia przez administratora odpowiednich polityk ochrony danych oraz właściwych środków technicznych i organizacyjnych celem ochrony danych. Brak odpowiednich środków ochrony danych osobowych stanowił naruszenie m.in. art. 5 ust. 1 lit. f) oraz art. 32 RODO.

Przy ustaleniu wysokości kary organ nadzorczy wziął pod uwagę charakter ujawnionych danych osobowych, które dotyczyły zdrowia i innych spraw osobistych. Organ powołał się również na charakter szkoły ponadgimnazjalnej w Breiðholt jako instytucji non-profit.

Źródło: https://edpb.europa.eu/news/national-news/2020/personal-data-breach-breidholt-upper-secondary-school-administrative-fine_pl

Pełna treść decyzji w języku islandzkim dostępna jest na stronie: https://www.personuvernd.is/urlausnir/nr/2885

Cypryjski organ nadzorczy zakazał przetwarzania danych osobowych za pomocą narzędzia „Czynnik Bradford"
Komisarz Ochrony Danych Osobowych (cypryjski organ nadzorczy) nałożył na LGS Handling Ltd, Louis Travel Ltd oraz Louis Aviation Ltd (grupę firm Louis) karę w wysokości 82000 euro z powodu braku podstawy prawnej do wykorzystywania zautomatyzowanego narzędzia

służącego do pomiaru nieobecności pracowników spowodowanych chorobą, znanego jako „Czynnik Bradford".

Komisarz nakazał administratorowi zaprzestanie przetwarzania oraz usunięcie wszystkich zebranych danych. Ponadto nałożył kary pieniężne w wysokości 70000 euro na LGS Handling Ltd, 10000 euro na Louis Travel Ltd oraz 2000 euro na Louis Aviation Ltd w związku z naruszeniem art. 6 ust. 1 oraz art. 9 RODO.

Przy podejmowaniu decyzji o wysokości kar administracyjnych uwagę zwrócono na liczbę osób, których dane dotyczą (ogółem 818 pracowników), charakter oraz czas trwania naruszeń jak też obrót firm.

Komisarz wdrożył postępowanie po skardze złożonej przez związek zawodowy. Powodem, dla którego przedsiębiorstwo stosowało zautomatyzowany system pomiaru nieobecności chorobowych pracowników („Czynnik Bradford") było to, że ich krótkie, częste i nieplanowane absencje prowadziły do większej dezorganizacji pracy firmy niż dłuższe nieobecności.

Komisarz uznał, że administrator nie wykazał , że jego prawnie uzasadniony interes przeważył nad interesami, prawami i wolnościami jego pracowników, w konsekwencji czego nie zminimalizował ryzyka.

Podczas postępowania została wykorzystana możliwość zadawania pytań prawnych innym organom nadzorczym z obszaru EOG przez tak zwaną procedurę wzajemnej pomocy: uzyskano odpowiedzi od 25 organów. Potwierdziły one brak podstawy prawnej dla przedmiotowego przetwarzania oraz podkreśliły konieczność uregulowania tego typu kwestii w przepisach szczególnych, zgodnych z art. 88 RODO.

Po oszacowaniu wszystkich elementów zebranych podczas postępowania, Komisarz stwierdził, że tego rodzaju operacja przetwarzania odbywa się bez podstawy prawnej. Po pierwsze: nie zostało ustalone, że uzasadniony prawnie interes administratora przeważa nad interesami, prawami i wolnościami jego pracowników, co pozwoliłoby administratorowi oparcie się na art. 6 ust. 1 lit. f) RODO. Podobnie żaden z zapisów art. 9 ust. 2 RODO nie stosuje się w tym przypadku, nie pozwalając administratorowi na przetwarzanie danych związanych ze stanem zdrowia pracowników.

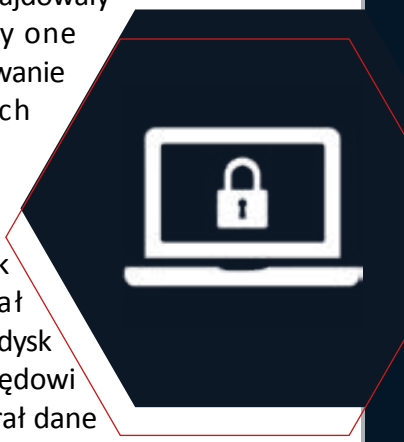
Źródło: https://edpb.europa.eu/news/national-news/2020/cypriot-supervisory-authority-banned-processing-automated-tool-used-scoring_pl

Pełna treść decyzji w języku greckim dostępna jest pod adresem: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2/$file/2019-apofasi%20bradford%20system%20ANΩNYMOΠ.pdf?openelement

Dania: Kary dla dwóch magistratów za brak odpowiedniego poziomu bezpieczeństwa danych

Duńska Agencja Ochrony Danych złożyła policji raport w sprawie magistratów Gladsaxe i Hørsholm ze względu na stwierdzenie, iż nie zapewniły one odpowiedniego poziomu bezpieczeństwa danych zgodnie z RODO. Dla magistratów Gladsaxe i Hørsholm zaproponowano kary w wysokości odpowiednio 100000 koron duńskich (około 13380 euro) oraz 50000 koron duńskich (około 6700 euro).

Agencja Ochrony Danych powzięła informację o obu sprawach na skutek powiadomień, złożonych przez same magistraty, które poinformowały organ o naruszeniach ochrony danych związanych z kradzieżą komputerów, na których dyskach znajdowały się dane osobowe. Nie były one zabezpieczone poprzez szyfrowanie i utrata danych osobowych stanowiła duże ryzyko dla obywateli.



W jednym z przypadków brak zabezpieczeń zaowocował poważnym naruszeniem, gdyż dysk komputera skradzionego Urzędowi Miejskiemu Gladsaxe zawierał dane dotyczące 20620 obywateli, w tym informacje wrażliwe i dane osobowe.

Do drugiego z naruszeń doszło, gdy komputer pracownika magistratu w Hørsholm został skradziony z jego samochodu. Na dysku znajdowały się dane około 1600 pracowników magistratu, w tym informacje wrażliwe i dane osobowe.

Magistrat przetwarza duże ilości danych osobowych dotyczących mieszkańców, w tym informacje wrażliwe. Jako obywatel nie mam możliwości wycofania swoich danych z przetwarzania przez magistrat, na którym spoczywa odpowiedzialność za niedopuszczenie do ujawnienia tych informacji,- stwierdził Frederik Viksøe Siegumfeld, Naczelnik Działu Nadzorczego Duńskiej Agencji Ochrony Danych. Wyjaśnia- Gdy dysk komputera nie jest zaszyfrowany, dostęp do danych przechowywanych na nim jest łatwy: na przykład poprzez przełożenie dysku do innego komputera. Stąd też jeżeli dane osobowe przechowywane były lokalnie na komputerze, bardzo nieroztropnym ze strony magistratu było niezaszyfrowanie komputerów.

Duńska Agencja Ochrony Danych zadecydowała o przedłożeniu policji raportu w sprawie magistratów Gladsaxe i Hørsholm oraz zaproponowała kary w wysokości odpowiednio 100000 koron duńskich oraz 50000 koron duńskich.

Źródło: https://edpb.europa.eu/news/national-news/2020/fines-proposed-two-municipalities_p

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 następujących kwestii:

- Czy szkoła może udostępnić dane na temat liczby uczniów i innych mieszkających pod danym adresem?

- Czy w przypadku kierowania ucznia na praktyki zawodowe konieczne jest powierzenie?

- Jaka jest podstawa prawna przetwarzania danych osób upoważnionych do odbioru dziecka?

- Czy przekazanie dokumentacji do fumigacji powoduje konieczność zawarcia umowy powierzenia?

Zachęcamy także do zapoznania się z zapisem debat przeprowadzonych podczas Dnia Otwartego UODO z okazji XIV Dnia Ochrony Danych Osobowych.

Pierwsza debata tego dnia dotyczyła najczęstszych problemów z jakimi w swojej pracy spotykają się inspektorzy ochrony danych. Drugi panel dyskusyjny dotyczył kwestii udostępniania danych dzieci w Internecie.

Pełen zapis obu debat jest do pobrania pod linkiem https://uodo.gov.pl/pl/451/1328

URZĄD OCHRONY DANYCH OSOBOWYCH