Nr 11/2021 (32)
Listopad 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

PESEL JAKO LOGIN DO SYSTEMU INFORMATYCZNEGO

PESEL nie powinien być wykorzystywany jako login do systemu informatycznego czy portalu. Mimo że stanowisko polskiego organu ds. ochrony danych osobowych dotyczące wykorzystywania numeru PESEL jako loginu do systemu informatycznego czy portalu jest niezmienne, wciąż zdarza się wprowadzanie tego typu budzących zastrzeżenia rozwiązań.

Dlatego warto przypomnieć, że numer PESEL jest jedenastocyfrowym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, zawierającym datę urodzenia, numer porządkowy, oznaczenie płci oraz liczbę kontrolną. Jest to więc krajowy numer identyfikacyjny w rozumieniu art. 87 ogólnego rozporządzenia o ochronie danych (RODO), zatem jego przetwarzanie powinno odbywać się z zachowaniem odpowiednich, przewidzianych w RODO zabezpieczeń praw i wolności osoby, której dane dotyczą.

Zbyt duża dostępność

Nie można przy tym pominąć, że choć ustawa z dnia 24 września 2010 r. o ewidencji ludności nie przewiduje jawności i powszechnej dostępności numeru PESEL, a wręcz przeciwnie, zawiera szereg warunków co do jego udostępnienia, to w praktyce, w następstwie unormowań zawartych w przepisach szczególnych, numer PESEL konkretnej osoby fizycznej stał się daną osobową dostępną bez żadnych ograniczeń, co było przedmiotem wielu wystąpień organu nadzorczego kierowanych do twórców tych przepisów.

Ponadto możliwość powiązania informacji z wielu powszechnie dostępnych baz danych czy rejestrów przy wykorzystaniu numeru PESEL stwarza ryzyko tworzenia profili osobowych, co, jeśli odbywa się bez wiedzy tej osoby, może stanowić zagrożenie dla jej prywatności.

Słabe zabezpieczenie

Wykorzystanie numeru PESEL, którego pozyskanie nie stanowi w chwili obecnej szczególnego problemu, w charakterze loginu rodzić może szereg ryzyk dla danych osobowych przetwarzanych w systemie informatycznym, takich jak uzyskanie dostępu do nich przez osoby nieuprawnione.

W tym kontekście warto pamiętać, że to podmiot tworzący system informatyczny ponosi odpowiedzialność za takie ukształtowanie zasad dostępu do niego, by minimalizować ryzyko dla przetwarzanych w nim danych osobowych.

Na kwestię tę zwrócił też uwagę prawodawca unijny, nakładając w art. 25 ust. 1 RODO obowiązek uwzględnienia ochrony danych w fazie projektowania (tzw. privacy by design), czyli przyjmowania tylko takich rozwiązań technicznych i organizacyjnych odnoszących się do przetwarzania danych osobowych, które zapewniają skuteczną realizację zasad ochrony danych, przy uwzględnieniu ryzyka naruszenia praw i wolności osób fizycznych o różnym stopniu prawdopodobieństwa i wadze. Istotne jest także zastosowanie instrumentu oceny skutków dla ochrony danych w przypadku wystąpienia warunków, o których mowa w art. 35 ust. 3 lit. b RODO. Przepis ten wprost wskazuje, iż ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO. Wydaje się, że prawidłowo przeprowadzona ocena skutków dla ochrony danych unaoczniłaby podmiotowi odpowiadającemu za architekturę systemu informatycznego czy portalu ryzyka wiążące się z ustanowieniem numeru PESEL jako loginu do nich. Skoro bowiem login jest narzędziem mającym utrudnić osobie nieuprawnionej uzyskanie dostępu do danego systemu informatycznego, powinien być informacją znaną tylko osobie uprawnionej, która chce z niego skorzystać.

Naruszenie zasad RODO

Jednocześnie wykorzystywanie numeru PESEL jako loginu budzi wątpliwości w kontekście zasady minimalizacji, o której mowa w RODO.

Jak bowiem stanowi motyw 39 RODO, „Dane osobowe powinny być przetwarzane tylko w przypadkach,

gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami".

Jeżeli administrator nie może osiągnąć swojego celu innymi sposobami i zdecyduje się na przetwarzanie danych osobowych, wówczas musi kierować się zasadami określonymi w art. 5 RODO, zwłaszcza zasadą minimalizacji danych (lit. c), zgodnie z którą przetwarzane dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Ponadto narzucanie użytkownikom systemu informatycznego czy portalu obowiązku wykorzystywania numeru PESEL jako loginu godzi w prawa obywateli do samostanowienia w zakresie wykorzystywania ich danych osobowych. Każdy podmiot mający kontakt ze swoim klientem posiada wiele innych danych, które może wykorzystać jako identyfikator dostępu do systemu informatycznego czy portalu, takie jak chociażby numer klienta czy numer umowy, które nie ujawniają same w sobie danych osobowych.

Wykorzystywanie w tym celu numeru PESEL naraża administratora na odpowiedzialność, o której mowa w przepisach RODO.

WIELU PEŁNOMOCNIKÓW BŁĘDNIE, A PRZEZ TO NIESKUTECZNIE, ZAWIADAMIA O WYZNACZENIU IOD

O wyznaczeniu (zmianie danych lub odwołaniu) IOD lub jego zastępcy administratorzy/podmioty przetwarzające mogą zawiadomić przez pełnomocnika. Jednak, aby zawiadomienie było skuteczne, pełnomocnik musi pamiętać o spełnieniu warunków związanych z elektroniczną postacią zawiadomienia oraz elektroniczną formą pełnomocnictwa, a także o przesłaniu opłaty skarbowej od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia). Przed przystąpieniem do wysłania zawiadomienia warto przygotować sobie pełnomocnictwo oraz dowód dokonania opłaty skarbowej.

Niestety nie wszyscy pełnomocnicy są tego świadomi, a wiele składanych przez nich zawiadomień jest nieprawidłowych.

Dlatego warto poznać te zasady, by umieć ocenić, czy przesłane zawiadomienie o wyznaczeniu/odwołaniu/zmianie danych inspektora ochrony danych (IOD) lub jego zastępcy (na podstawie ustawy o ochronie danych osobowych lub ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości) jest poprawne. Takiej oceny poprawności zawiadomienia powinien dokonać zgłaszający (w tym pełnomocnik). Jeśli zawiadomienie nie spełnia wymagań, trzeba je ponowić.

Do zawiadomienia trzeba dołączyć pełnomocnictwo

Zarówno przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 10 ust. 2), jak i przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (art. 46 ust. 9) przewidują, że podmiot, który wyznaczył inspektora (zastępcę IOD), może zawiadomić o tym fakcie Prezesa UODO przez pełnomocnika. Do zawiadomienia musi być jednak dołączone pełnomocnictwo udzielone w formie elektronicznej. Przesłanie jedynie pełnomocnictwa bez załączenia stosownego zawiadomienia dotyczącego IOD (zastępcy IOD) jest nieprawidłowe.

Pełnomocnictwa musi udzielić właściwa osoba

Urząd Ochrony Danych Osobowych nie narzuca konkretnego wzoru pełnomocnictwa udzielonego osobie zawiadamiającej o wyznaczeniu IOD (zastępcy IOD). Ważne jest, aby z treści pełnomocnictwa wynikało upoważnienie do wykonania takiej czynności. Pełnomocnictwo może mieć charakter ogólny i obejmować

wiele różnych czynności dokonywanych przed organem lub dotyczyć tej konkretnej czynności (przesłania zawiadomienia dot. IOD lub jego zastępcy). W każdym przypadku musi być ono udzielone przez osobę uprawnioną do reprezentowania administratora/podmiotu przetwarzającego.

Obowiązkowa forma elektroniczna

Natomiast to, że pełnomocnictwo musi być udzielone w formie elektronicznej oznacza, że powinno być ono (np. dokument w formacie DOC) opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP złożonym przez osobę lub osoby udzielające pełnomocnictwa (zgodnie z reprezentacją administratora/podmiotu przetwarzającego).

Co istotne, dokument podpisany własnoręcznie i zeskanowany nie jest uznany za prawidłową formę pełnomocnictwa.

Ważna opłata skarbowa

Gdy zawiadomienia o wyznaczeniu IOD (zastępcy IOD) dokonuje się przez pełnomocnika, trzeba też pamiętać o uiszczeniu opłaty skarbowej. Można to zrobić w kasie Urzędu Dzielnicy Śródmieście m. st. Warszawy lub na konto bankowe, którego numer dostępny jest na stronie internetowej tego Urzędu (http://mobile.srodmiescie.warszawa.pl/strona-21-konta_bankowe.html). W tytule wpłaty, wraz z treścią „opłata skarbowa za pełnomocnictwo", należy zamieścić skrót „Prezes UODO", zaś dowód uiszczenia tej należności – w postaci dokumentu wykonania zlecenia przelewu przez system bankowości elektronicznej lub w postaci skanu otrzymanego dowodu wpłaty (w przypadku wpłaty za pośrednictwem poczty lub w kasie urzędu) – przesłać do UODO, łącznie z dokumentem pełnomocnictwa jako załącznik do zawiadomienia dotyczącego IOD/zastępcy IOD.

Wyjątki

Od powyższych zasad możliwe są pewne wyjątki. Opłaty od złożonego pełnomocnictwa nie uiszcza się m.in. w przypadku, gdy mocodawcą jest podmiot określony w art. 7 pkt. 1–5 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej, a więc np. jednostki budżetowe, jednostki samorządu terytorialnego, organizacje pożytku publicznego.

Inne z wyjątków dotyczą przesyłania pełnomocnictwa. Otóż dokonując zawiadomienia o wyznaczeniu IOD/zastępcy IOD, pełnomocnictwa nie musi przesyłać pełnomocnik ujawniony w Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG). Wystarczające bowiem jest to, że widnieje on w CEIDG.

Możliwe jest także dołączanie pełnomocnictwa uwierzytelnionego elektronicznie przez notariusza. W takim przypadku do zawiadomienia należy załączyć pełnomocnictwo poświadczone za zgodność przez notariusza i opatrzone jego kwalifikowanym podpisem elektronicznym (zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie).

Weryfikacja prawidłowości zawiadomienia należy do pełnomocnika

Jeśli zawiadomienie dotyczące IOD (zastępcy IOD) złożone przez pełnomocnika nie spełniało powyższych warunków, co pełnomocnik powinien zweryfikować samodzielnie, konieczne jest jego ponowne przesłanie. Należy też pamiętać, że wraz z ponownym zgłoszeniem i przedstawieniem do niego prawidłowego dokumentu pełnomocnictwa, należy ponownie wnieść opłatę skarbową. Artykuł 1 ust. 1 pkt 2 ustawy o opłacie skarbowej nie wiąże powstania obowiązku podatkowego w opłacie skarbowej z faktem ustanowienia pełnomocnika ani istnienia już w obrocie ważnego umocowania, ale z faktem złożenia tego dokumentu (jego odpisu, wypisu lub kopii). A zatem ustawa podatkowa jednoznacznie stanowi, że obowiązek ten powstaje „z chwilą złożenia dokumentu" (patrz wyrok WSA w Szczecinie z 6.02.2013 r., sygn. akt I SA/Sz 737/12).

Więcej informacji pomocnych w prawidłowym wywiązaniu się z obowiązku zawiadomienia dotyczącego IOD oraz formularze opracowane dla różnego rodzaju zawiadomień o wyznaczeniu/odwołaniu/zmianie danych IOD i wyznaczeniu/odwołaniu/zmianie danych zastępcy IOD zarówno na podstawie ustawy o ochronie danych osobowych, jak i ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości znajduje się na stronie internetowej Urzędu.

JAK EFEKTYWNIE PROWADZIĆ PRACE NAD KODEKSEM POSTĘPOWANIA

Z dotychczasowych doświadczeń Urzędu Ochrony Danych Osobowych zebranych w czasie prac na projektami kodeksów postępowania wynika, że środowiska inicjujące prace nad tymi dokumentami popełniają różnego rodzaju błędy.

Błędy rodzą często poważne konsekwencje:
– powodują wydłużenie procedury zatwierdzenia kodeksu,
– prowadzą do zawieszenia prac nad projektem,
– skutkują całkowitym zaniechaniem przygotowania takiego dokumentu.

Stąd inicjatywa UODO, by wskazać te problemy i podpowiedzieć, jak postępować, by szybko i bez problemów doprowadzić do zatwierdzenia kodeksu.

Temu celowi służy przygotowany i zamieszczony na stronie internetowej UODO cykl trzech publikacji:
– Jak efektywnie prowadzić prace nad kodeksem postępowania – rekomendacje UODO
– Najczęściej popełniane błędy przez środowiska pracujące nad projektami kodeksów postępowania
– Monitorowanie kodeksów. Jak stworzyć odpowiedni mechanizm? Na co zwrócić uwagę, a czego unikać

Zapraszamy do ich lektury.

KONSULTACJE KODEKSU POSTĘPOWANIA POWINNY BYĆ SZEROKIE, LECZ PODSUMOWANIE SYNTETYCZNE

Przeprowadzenie konsultacji projektu kodeksu postępowania to niezmiernie ważny etap poprzedzający złożenie wniosku o jego zatwierdzenie Prezesowi UODO. Konsultacje służą m.in. uzyskaniu - zarówno od podmiotów, które w przyszłości będą stosować uregulowania kodeksu, jak i od osób, których dane będą przetwarzane - informacji na temat ich oczekiwań co do przygotowanego projektu, jak również interpretacji jego uregulowań. Na ich podstawie możliwe jest dokonanie stosownych modyfikacji projektowanych postanowień, tak by były zgodne z przepisami, a jednocześnie jednoznaczne i zrozumiałe dla wszystkich odbiorców kodeksu.

Zarówno RODO, jak i ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako u.o.d.o.) jedynie ogólnie odnoszą się do kwestii tworzenia kodeksów postępowania. Dlatego pomocne we właściwym prowadzeniu prac nad takimi dokumentami są Wytyczne nr 1/2019 Europejskiej Rady Ochrony Danych (EROD) dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Co wynika z tych dokumentów?

Konsultacje to obowiązek

Powołane przepisy (motyw 99 RODO, art. 27 ust. 2 u.o.d.o.) ustanawiają obowiązek przeprowadzenia konsultacji projektu kodeksu postępowania. Jednocześnie jego spełnienie jest warunkiem formalnym umożliwiającym wszczęcie przez organ nadzorczy postępowania administracyjnego mającego na celu zatwierdzenie kodeksu postępowania.

Ważny szeroki zakres

Co istotne, konsultacje muszą mieć odpowiednio szeroki zakres. Powinny wziąć w nich udział nie tylko podmioty, które mają stosować przepisy kodeksu, ale również osoby, których dane te podmioty przetwarzają, czy też stowarzyszenia bądź organizacje działające na ich rzecz. W niektórych przypadkach zasadne może być skonsultowanie projektu kodeksu z regulatorem danego sektora.

Z kolei w powołanych wytycznych EROD wskazano, że „twórcy kodeksów powinni potwierdzić i wykazać przy przedkładaniu kodeksu do zatwierdzenia, że przeprowadzono właściwe konsultacje z odpowiednimi stronami, których sprawa dotyczy. W razie potrzeby obejmowałoby to informacje o innych kodeksach postępowania, którym mogą podlegać potencjalni członkowie, którzy zobowiązali się do stosowania kodeksu, oraz informację o tym, w jaki sposób ich kodeks uzupełnia inne kodeksy. Należy również określić poziom i charakter konsultacji, które odbyły się z udziałem członków, innych zainteresowanych stron i osób, których dane dotyczą, bądź zrzeszeń lub organów, które ich reprezentują. W praktyce zdecydowanie zaleca się przeprowadzenie konsultacji z członkami organizacji lub organu będących twórcami kodeksu, a także uwzględnienie czynności przetwarzania prowadzonych w stosunku do klientów tych członków".

Możliwa ocena cząstkowa

W opinii UODO, w niektórych sytuacjach, np. przy obszernych kodeksach, gdy duża ilość regulacji kodeksowych może zniechęcać do oceny całości materiału, dopuszczalne byłoby wskazywanie i konsultowanie najistotniejszych elementów projektowanych regulacji. Przykładowo organizacje konsumenckie mogłyby zostać poproszone głównie o ocenę tej części kodeksu, która odnosi się do realizacji praw osób, których dane dotyczą, czy spełniania obowiązku informacyjnego.

Niemniej zainteresowani powinni móc zgłosić uwagi do treści całego projektu kodeksu, o czym powinni być informowani przez jego twórców.

Brak musi zostać wyjaśniony

Warto zaznaczyć, że w Wytycznych EROD wskazano, że: „Jeżeli z odpowiednimi zainteresowanymi stronami, których sprawa dotyczy, nie przeprowadzono żadnych konsultacji ze względu na brak takiej możliwości, twórca kodeksu musi wyjaśnić tę sytuację".

Sprawozdanie

Podmiot wnioskujący o zatwierdzenie kodeksu postępowania powinien przedstawić Prezesowi UODO syntetyczne sprawozdanie z przeprowadzonych konsultacji, zawierające najważniejsze wnioski z nich płynące, wyjaśniające, jaką metodologię przyjęto, jakie uwagi były zgłaszane i jak się do nich ustosunkowano (przyjęcie wszystkich uwag wyrażonych w czasie konsultacji nie jest konieczne).

Należy podkreślić, że rolą Prezesa Urzędu nie jest analiza obszernej dokumentacji, stanowiącej odzwierciedlenie całego przebiegu przeprowadzonych konsultacji, a jedynie ocena tego, czy konsultacje zostały przeprowadzone w odpowiednim zakresie oraz czy i które przepisy projektu kodeksu postępowania zostały zmodyfikowane w efekcie przeprowadzonych konsultacji.

Wezwanie do przeprowadzenia ponownych konsultacji

Jeżeli organ nadzorczy, oceniając projekt kodeksu, uzna, że zakres konsultacji był niewystarczający, może (zgodnie z art. 27 ust. 4 u.o.d.o.) wezwać wnioskodawcę do przeprowadzenia ponownych konsultacji, wskazując ich zakres.

Procedura dotycząca odpowiedniego prowadzenia konsultacji i ich dokumentowania oraz potwierdzania ma zastosowanie również w przypadku zmiany zatwierdzonego kodeksu postępowania lub jego rozszerzenia (art. 27 ust. 5). Warto ją znać i odpowiednio stosować.

PRZEDŁUŻONE KONSULTACJE PROJEKTU KODEKSU POSTĘPOWANIA DLA SEKTORA MARKETINGU

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

Konsultacje społeczne to jeden z obowiązkowych etapów prac poprzedzających zatwierdzenie kodeksu postępowania. Więcej na ten temat można przeczytać w artykule „Konsultacje kodeksu postępowania powinny być szerokie, lecz podsumowanie syntetyczne" (str.5)

Polskie Stowarzyszenie Marketingu SMB, kierując do konsultacji społecznych projekt Kodeksu postępowania i dobrych praktyk w zakresie ochrony danych osobowych w działaniach marketingu bezpośredniego (KODO), podjęło wiele działań informacyjno-promocyjnych mających na celu włączenie w konsultacje szerokiego grona interesariuszy. Wśród nich wymienić można organizację specjalnej konferencji z udziałem przedstawiciela UODO, która odbyła się 26 października 2021 r., czy uruchomienie specjalnej strony internetowej (www.kodo.smb.pl) umożliwiającej m.in. zapoznanie się z treścią kodeksu oraz wzięcie udziału w jego konsultacjach.

Żeby umożliwić wszystkim zainteresowanym przedstawienie uwag do projektu kodeksu postępowania, podjęto decyzję o przedłużeniu czasu konsultacji do 31 grudnia 2021 r..

Opinie można przesyłać do na adresy:
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 u.o.d.o. Dlatego prosimy o nieprzesyłanie uwag do UODO.

KARY

Norwegia: kara upomnienia po uzyskaniu dostępu do konta e-mail

Norweski organ ochrony danych upomniał przedsiębiorstwo za naruszenie przepisów RODO dotyczących informacji podawanych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą i prawa dostępu do danych osobowych przysługujące osobie.

Organ nadzorczy nakazał przedsiębiorstwu ustanowienie pisemnych procedur dostępu do kont poczty elektronicznej.

Decyzja została wydana na skutek skargi byłego dyrektora zarządu, który odkrył, że spółka uzyskała dostęp do jego osobistego konta e-mail powiązanego z przedsiębiorstwem.

Po zbadaniu skargi organ ochrony danych stwierdził, że przedsiębiorstwo co prawda miało podstawę

prawną do uzyskania dostępu do konta, ale nie poinformowało skarżącego o uzyskaniu przez nie dostępu do konta.

Organ ochrony danych stwierdził również, że przedsiębiorstwo zbyt długo zwlekało z udzieleniem skarżącemu dostępu do jego danych osobowych, po tym jak skarżący zwrócił się o to.

Źródło: https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-reprimanded-after-accessing-e-mail-account_pl

Finlandia: policja z upomnieniem za nielegalne przetwarzanie danych osobowych

Fiński organ nadzorczy udzielił Krajowej Radzie Policji upomnienia za niezgodne z prawem przetwarzanie szczególnych kategorii danych osobowych podczas próbnego zastosowania technologii rozpoznawania twarzy.

Krajowa Rada Policji zgłosiła do biura rzecznika ochrony danych osobowych w kwietniu 2021 r. naruszenie ochrony danych osobowych związane z próbnym wykorzystaniem oprogramowania do rozpoznawania twarzy przez Narodowe Biuro Śledcze. Do zdarzenia doszło na początku 2020 roku. Jednostka Narodowego Biura Śledczego specjalizująca się w zapobieganiu wykorzystywania seksualnego dzieci, eksperymentowała z technologią rozpoznawania twarzy w identyfikacji potencjalnych ofiar.

Decyzja o wypróbowaniu oprogramowania została podjęta niezależnie przez jednostkę policji, a przetwarzanie danych osobowych odbywało się bez zgody administratora danych, czyli Krajowej Rady Policji.

W operacjach tych nie dopełniono obowiązku administratora danych, a podjęte przez niego środki nie zapobiegły bezprawnemu przetwarzaniu danych osobowych. Obowiązkiem Krajowej Rady Policji byłoby zapewnienie, aby pracownicy policji znali przepisy i wymagane procedury.

Policja nie uwzględniła również wymogów dotyczących przetwarzania szczególnych kategorii danych osobowych. Ponadto przetwarzanie danych rozpoczęto bez uzyskania informacji, w jaki sposób wykorzystywana usługa przetwarza dane osobowe. Na przykład policja nie ustaliła z góry, jak długo dane będą przechowywane i czy mogą być ujawnione osobom trzecim.

Oprócz upomnienia, organ nadzorczy nakazał Krajowej Radzie Policji zawiadomienie osób, których dane dotyczą, o naruszeniu danych osobowych, o ile możliwe jest ustalenie ich tożsamości. Krajowa Rada Policji musi również nakazać firmie, z usług której korzystano, usunięcie danych przekazanych przez policję z jej platform przechowywania danych.

Źródło: https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_pl

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

RADA EUROPY

Niemcy i Macedonia Północna ratyfikowały Konwencję 108+

Grono państw, które ratyfikowały zmodernizowaną Konwencję 108 (Konwencja 108+), tj. Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (CETS 223), powiększyło się o kolejne dwa państwa. Są to Niemcy i Macedonia Północna.

Jeśli chodzi o Niemcy, to uroczystość złożenia dokumentu ratyfikacyjnego do protokołu zmieniającego konwencję odbyła się 5 października 2021 r. na Węgrzech podczas Konferencji Ministrów Sprawiedliwości ds. Technologii Cyfrowej i Sztucznej Inteligencji – Nowe Wyzwania dla Sprawiedliwości w Europie. Niemcy są stroną konwencji nr 108 od 1 października 1985 r.

Z kolei Stały Przedstawiciel Macedonii Północnej przy Radzie Europy przekazał Sekretarzowi Generalnemu dokument ratyfikacji 13 października 2021 r. Państwo to pozostaje stroną konwencji nr 108 od 1 lipca 2006 r. Wejście w życie Konwencji 108+ ma kluczowe znaczenie w erze cyfrowej. Żeby jednak ten przełomowy dokument mógł w pełni odgrywać swoją rolę na arenie międzynarodowej, konieczne będzie ratyfikowanie go przez kolejne państw w tym roku i 2022 roku.

Źródło: nieformalne tłumaczenie ze strony Rady Europy:

https://www.coe.int/en/web/data-protection/-/german-ratifies-convention-108-

https://www.coe.int/en/web/data-protection/-/15th--ratification-of-convention-108-north-macedonia

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:

Jaka jest podstawa przetwarzania przez szkołę danych uczniów w celu wydania mLegitymacji?

Jakie dokumenty i przez jaki okres powinny być publikowane w BIP?

Czy przedstawiciel związku zawodowego może mieć dostęp do danych we wnioskach o przyznanie świadczeń z ZFŚS?

Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów?

URZĄD OCHRONY DANYCH OSOBOWYCH