JUSTYNA JABŁONKA

Grudzień 2023
Nr 10/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI

Witajcie Drodzy Czytelnicy!

W grudniowym wydaniu Newslettera IOD wskazuję na orzeczenie Wojewódzkiego Sądu Administracyjnego, które rzuca światło na odpowiedzialność pracodawców za ochronę danych osobowych przechowywanych na prywatnych komputerach pracowników. W dobie rosnącej popularności pracy zdalnej, ta decyzja sądowa podkreśla konieczność wnikliwej analizy ryzyka i wdrażania skutecznych środków ochronnych przez każdego pracodawcę. Jeśli chodzi o pracowników wskażemy również na temat ich skrzynek mailowych i możliwości ich monitorowania. Dodatkowo, w osobnym wpisie, opiszę czym jest Deepfake, jak również wskażę w jaki sposób może nas to dotyczyć. Wyjaśnimy również jakie działania należy podjąć w przypadku naruszenia ochrony danych osobowych, oraz odpowiemy na pytanie czy każdorazowo o takim naruszeniu musimy zawiadomić Prezesa UODO?

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

Grudzień przedstawia się następująco:

I. Zagrożenia z Deepfake, czyli jak nowe technologie testują granice ochrony Twoich danych.

Czy zastanawialiście się Państwo kiedyś, jak to możliwe, że w internecie pojawiają się filmy ze znanymi osobistościami, mówiącymi rzeczy, których nigdy nie powiedzieli? Kluczem do tej zagadki jest technologia znana jako deepfake. Deepfake to metoda używająca sztucznej inteligencji (AI) do tworzenia fałszywych wideo i nagrań audio, które są na tyle realistyczne, że mogą wprowadzić w błąd nawet najbardziej uważnych widzów.

Wyobraźcie sobie, że odbieracie telefon od swojego męża, syna, czy córki, którzy proszą o pilne przelanie pieniędzy na ich konto. Głos brzmi znajomo, wydaje się być autentyczny. Może nawet przeprowadzacie rozmowę wideo, widząc ich twarze i słysząc ich głosy, które wydają się całkowicie realne. Jednakże w rzeczywistości nie jest to osoba, którą znacie, lecz doskonale wykonany deepfake, mający na celu wyłudzenie od Was pieniędzy. Takie sytuacje, choć mogą brzmieć jak scenariusz filmowy, stają się coraz bardziej realnym zagrożeniem w erze zaawansowanej technologii AI.

Przykłady wykorzystania deepfake w mediach są liczne. W jednym z najbardziej znanych przypadków stworzono film z CEO Facebooka, Markiem Zuckerbergiem, który wydaje się mówić **o kontrolowaniu skradzionych danych milionów ludzi** - co w rzeczywistości nigdy się nie wydarzyło. Film ten jest przykładem na to, jak zaawansowane stały się techniki deepfake i jak wielkie mogą stanowić wyzwanie dla naszej zdolności do rozróżniania rzeczywistości od fikcji.

Jak działa technologia Deepfake?

Deepfake to więcej niż tylko trik komputerowy - to zaawansowana technologia, która wykorzystuje algorytmy sztucznej inteligencji do kreowania zaskakująco realistycznych fałszywych wideo i nagrań audio. Ale jak dokładnie działa ta technologia? Rozumiem, że może to brzmieć skomplikowanie, ale postaram się wyjaśnić to w prosty sposób.

Zbieranie danych: wszystko zaczyna się od zebrania danych. Do stworzenia deepfake, potrzebne są zdjęcia i nagrania audio osoby, którą chcemy podrobić. Im więcej materiału, tym algorytm ma więcej informacji do nauki i lepiej może naśladować tę osobę.

Uczenie maszynowe: następnie algorytmy AI, zwłaszcza głębokie sieci neuronowe, analizują zebrane dane. Uczą się one charakterystycznych cech osoby, na przykład sposobu mówienia, ruchów twarzy, czy mimiki. Dzięki temu mogą one później tworzyć nowe, fałszywe materiały, które wydają się autentyczne.

Generowanie fałszywych treści: gdy algorytm „nauczy się" danej osoby, jest w stanie wygenerować nowe treści. Może to być wideo, na którym ta osoba mówi słowa, których nigdy nie wypowiedziała, lub nagranie audio, które brzmi jak jej głos, ale jest całkowicie sfabrykowane.

Dopasowywanie detali: ostatnim krokiem jest dopracowanie szczegółów. Algorytm dopasowuje ruchy ust, mimikę twarzy i inne detale, aby wszystko wyglądało jak najbardziej realistycznie. To wymaga zaawansowanych technik przetwarzania obrazu i dźwięku.

Kluczowe jest zrozumienie, że choć technologia deepfake może być fascynująca, niesie ze sobą również poważne zagrożenia. Fałszywe treści mogą być używane do wprowadzania w błąd, manipulacji i oszustw, co ma bezpośredni wpływ na nasze życie codzienne i **ochronę naszych danych osobowych.**

Potencjalne zagrożenia związane z Deepfake.

Rozumienie potencjalnych zagrożeń związanych z deepfake jest kluczowe, aby móc skutecznie bronić się przed tymi niebezpiecznymi technologiami. Oto kilka głównych obszarów, na które należy zwrócić uwagę:

1. Dezinformacja i manipulacja: jednym z największych zagrożeń z deepfake jest możliwość szerzenia dezinformacji. Fałszywe wideo czy nagrania audio mogą być wykorzystywane do wprowadzania w błąd opinii publicznej, manipulowania wyborami politycznymi czy nawet destabilizowania społeczeństw.

2. Wyłudzenia finansowe:jak wspomniano wcześniej, deepfake może być wykorzystywane do przekonujących oszustw finansowych. Przykładem mogą być telefony od rzekomych członków rodziny proszących o przekazanie środków finansowych, co w rzeczywistości jest próbą wyłudzenia.

3. Naruszenie prywatności i tożsamości: wykorzystanie wizerunku osób bez ich zgody w deepfake może prowadzić do poważnych naruszeń prywatności i tożsamości. Może to obejmować nieautoryzowane wykorzystanie wizerunków osób publicznych, ale również prywatnych osób w różnych, często kompromitujących kontekstach.

4. Kwestie prawne i etyczne: deepfake stwarza także wiele wyzwań prawnych i etycznych. Przykłady obejmują prawo do wizerunku, autorskie prawa do treści cyfrowych oraz moralne aspekty wykorzystania wizerunku osób do celów, na które nie wyraziły zgody.

5. Ochrona Danych Osobowych: w kontekście ochrony danych osobowych, deepfake stwarza wyzwanie w zakresie identyfikacji autentyczności informacji. Osoby mogą nie być świadome, że ich dane osobowe, takie jak wizerunek czy głos, są wykorzystywane do tworzenia fałszywych treści.

Co powinniśmy robić aby nie dać się nabrać?

Po raz kolejny wskażę, iż edukacja – szkolenia pracowników i podnoszenie świadomości na temat cyberbezpieczeństwa są niezwykle ważne w ochronie naszej prywatności i danych osobowych. Z pewnością przyczyniają się do zwiększenia świadomości wśród społeczeństwa oraz pracowników, czyniąc ich bardziej odpornymi na potencjalne cyberataki.

Nauka rozpoznawania potencjalnych deepfake, obejmująca zwracanie uwagi **na niespójności w obrazie i dźwięku, takie jak nienaturalne ruchy twarzy, błędy w oświetleniu czy niezgodności między mową a ruchami ust, może być a niejednokrotnie już jest kluczowa.**

Ważne jest, aby rozwijać umiejętności krytycznego myślenia, szczególnie w kontekście łatwej manipulacji treściami multimedialnymi. Przyjmowanie informacji bez uprzedniej analizy i weryfikacji źródła może prowadzić do dezinformacji i błędnych przekonań.

adw. Justyna Jabłonka
Inspektor Ochrony Danych

II. Jak zgłosić naruszenie ochrony danych osobowych

23 listopada 2023 r. Prezes UODO poinformował o nałożeniu na jedno ze znanych towarzystw ubezpieczeniowych administracyjnej kary pieniężnej za niedopełnienie wynikającego z art. 33 RODO obowiązku zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych. Naruszenie polegało na wysłaniu do nieuprawnionego odbiorcy wiadomości e-mail z dokumentem potwierdzającym przyznanie odszkodowania. W wiadomości znajdowały się m.in. imię, nazwisko, adres do korespondencji, dane wskazujące markę, model, numer rejestracyjny samochodu, a także numer polisy, numer wartość szkody i kwota uznanego roszczenia. Odbiorca wiadomości poinformował towarzystwo ubezpieczeń o otrzymaniu wiadomości z cudzymi danymi osobowymi, jednak ubezpieczyciel nie zareagował na tę informację, a w szczególności nie dopełnił obowiązku zawiadomienia o zaistniałym naruszeniu Prezesa UODO. Konsekwencją niedopełnienia obowiązku zawiadomienia było nałożenie na towarzystwo ubezpieczeń kary w wysokości 103 752 zł. Aby uniknąć takich konsekwencji warto pamiętać o obowiązku zawiadamiania organu nadzorczego o stwierdzonym naruszeniu oraz zwrócić uwagę na kilka elementów, które są niezbędne, aby zawiadomienie było prawidłowe.

Kiedy konieczne jest zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych

Zgodnie z art. 33 ust. 1 RODO obowiązek zgłoszenia naruszenia Prezesowi UODO pojawia się za każdym razem gdy dojdzie do naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W tym zakresie należy wskazać, że w zależności od poziomu ryzyka naruszenia praw lub wolności osób fizycznych można wyróżnić trzy poziomy naruszeń: po pierwsze takie, z którymi nie wiąże się ryzyko naruszenia praw lub wolności osób fizycznych bądź jest mało prawdopodobne, by naruszenie skutkowało takim ryzykiem; po drugie takie, w przypadku których takie ryzyko istnieje, ale nie jest wysokie oraz po trzecie takie, w przypadku których ryzyko to jest wysokie. Obowiązek zgłoszenia naruszenia Prezesowi UODO dotyczy dwóch ostatnich sytuacji. Aby ocenić poziom ryzyka naruszenia praw lub wolności osób fizycznych administrator powinien przeprowadzić analizę uwzględniającą kontekst i okoliczności zaistniałego

zdarzenia. PUODO wskazuje, że każdy administrator, niezależnie od zaistnienia naruszenia ochrony danych osobowych, ma obowiązek wprowadzić procedurę umożliwiającą stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych, przy czym stopień dotkliwości skutków naruszenia powinien być oceniany z perspektywy osób, których dane są przetwarzane (UODO, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych Wersja 1.0, 2019). Analizę ryzyka związanego z naruszeniem można dokonać np. w oparciu o metodologię ENISA, która jest rekomendowana przez UODO.

Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodą taką może być m.in.: dyskryminacja osoby, której dane dotyczą, kradzież tożsamości, strata finansowa lub naruszenie dobrego imienia. Jeżeli naruszenie dotyczy danych osobowych wrażliwych, należy uznać, że występuje duże prawdopodobieństwo takiej szkody. Warto przy tym podkreślić, że obowiązek zgłoszenia przez administratora naruszenia ochrony danych osobowych, nie jest uzależniony od zaistnienia naruszenia praw lub wolności osób fizycznych a konieczność dokonania zgłoszenia uzasadnia samo ryzyko zmaterializowania się takiego naruszenia. Jeżeli prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych nie zaistniało, bądź jest małe konieczne jest odnotowanie naruszenia w wewnętrznej ewidencji naruszeń oraz zastosowanie środków zaradczych mających na celu zminimalizowanie ryzyka i zabezpieczenie danych osobowych. Jeżeli prawdopodobieństwo zaistnienia ryzyka nie może być kwalifikowane jako małe należy zgłosić naruszenie PUODO, a gdy jest ono wysokie, dodatkowo należy poinformować o naruszeniu osobę, której dane dotyczą.

Wielość naruszeń

Co do zasady każde pojedyncze naruszenie należy zgłosić osobno. Aby uniknąć nadmiernego obciążania administratorów dopuszcza się jednak możliwość „zbiorczego" zgłoszenia kilku naruszeń, do których doszło do w stosunkowo krótkim odstępie czasu i pod warunkiem, że dotyczą one tego samego rodzaju danych osobowych, a ich ochrona została naruszona w taki sam sposób (Grupa Robocza Art. 29, Wytyczne dotyczące zgłaszania naruszeń, WP 250 rev. 01). Jeżeli w danym przypadku doszło do kilku dotyczących różnych rodzajów danych osobowych, których ochrona została naruszona w różny sposób, zgłoszenia należy dokonać osobno w standardowym trybie.

Forma zgłoszenia

Zgodnie z art. 33 ust. 3 RODO zgłoszenie naruszenia powinno określać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; opisywać możliwe konsekwencje naruszenia ochrony danych osobowych oraz środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zgłoszenia naruszenia PUODO można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl. Skorzystanie z formularza ułatwia dokonanie zgłoszenia i pozwala uniknąć błędów jednak nie jest obowiązkowe. Jeżeli z jakichś względów administrator nie chce lub może skorzystać z formularza, może zawrzeć wszystkie informacje wskazane w art. 33 ust. 3 RODO w piśmie kierowanym do Prezesa UODO.

Zgłoszenie można wypełnić bezpośrednio na platformie biznes.gov.pl. Wypełniony formularz można też wysłać na elektroniczną skrzynkę podawczą ePUAP UODO lub jako pismo ogólne za pomocą platformy biznes.gov.pl. Możliwe jest również wysłanie zgłoszenia tradycyjną pocztą na adres UODO.

Termin zgłoszenia

Administrator powinien dokonać zgłoszenia bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

To czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem charakteru i wagi naruszenia, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą (UODO, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych Wersja 1.0 , 2019)

O stwierdzeniu naruszenia można mówić, kiedy administrator ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych. Warto przy tym zauważyć, że zgodnie ze stanowiskiem Grupy Roboczej Art. 29 z przepisów RODO wynika obowiązek wdrożenia przez administratora wszelkich odpowiednich technicznych i organizacyjnych, by móc od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ

nadzorczy i osoby, których dane dotyczą (Grupa Robocza Art. 29, Wytyczne dotyczące zgłaszania naruszeń, WP 250 rev. 01). Spóźnione wykrycie naruszenia i zwlekanie z jego zgłoszeniem PUODO może być potraktowane jako naruszenie tego obowiązku i działać na niekorzyść administratora.

Zgłoszenie wstępne i uzupełniające

Jeżeli przed upływem 72 od stwierdzenia naruszenia administrator nie dysponuje wszystkimi wymaganymi informacjami, może dokonać zgłoszenia wstępnego przekazując te informacje, które udało mu się zebrać a następnie przekazywać sukcesywnie kolejne informacje w ramach zgłoszeń uzupełniających. W takim przypadku administrator powinien przekazać brakujące informacje, jak tylko wejdzie w ich posiadanie. Takie „sukcesywne" zawiadomienie jest dopuszczalne, pod warunkiem że administrator poda organowi nadzorczemu przyczyny opóźnienia.

r. pr. Grzegorz Lubeńczuk

III. Poczta mailowa służbowa, czyli kilka słów o wyważeniu interesów pracodawcy oraz pracownika.

W dzisiejszym wpisie chciałabym omówić temat skrzynki mailowej służbowej. Jak wiadomo, jest to niejednokrotnie składnica ogromnej wiedzy. Terminarze, dokumenty, czynności, dane osobowe etc. Czy zastanawialiście się Państwo kiedykolwiek nad tym, czy służbowe maile pracownika mogą być wykorzystywane do celów prywatnych, oraz nad tym, co się dzieje z takimi skrzynkami mailowym po odejściu z pracy, bądź w trakcie dłuższego urlopu czy L4 pracownika?

Skrzynka mailowa służbowa, służy do wykonywania czynności służbowych, jednak każdy z nas ma prawo do poszanowania prywatności.
Korzystanie ze skrzynki służbowej, jest co do zasady uzależnione od zasad ustalonych u pracodawcy. Jeśli aktywność na skrzynce ma być ograniczona wyłącznie do czynności służbowych, pracownik powinien zostać o tym jasno poinformowany. Ewentualne wyciąganie konsekwencji, również, w moim przekonaniu, powinno być uzależnione od tego, czy pracownik otrzymał wyraźne wytyczne, czy też nie. Takie stanowisko zresztą reprezentują także sądy pracy.

elementów, które są niezbędne, aby zawiadomienie było prawidłowe.

Kiedy konieczne jest zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych

Nieobecność w pracy - czy można przekierowywać wiadomości e-mail do przełożonego?
Pytanie, czy będzie to uzasadnione? Podobnie przecież możemy ustawić autoresponder na czas naszej nieobecności: nadawca, który będzie chciał przekazać swoją wiadomość do wskazanej osoby, zrobi to we własnym zakresie, bez wymuszonego przekierowania. Problem jest intensywniejszy wówczas, gdy pracownik korzysta z poczty służbowej do celów prywatnych – w takiej sytuacji nikt nie chciałby, aby jego poczta trafiała na skrzynkę mailową szefa.
O ile w procedurach zakładu pracy znajdują się rozwiązania, że skrzynka mailowa służy wyłącznie do celów służbowych, przekierowanie poczty do przełożonego nie powinno stanowić większego problemu. Pozostaje inna kwestia: gdyby na taką skrzynkę „wpadła”

prywatna korespondencja, to czy pracodawca mógłby się z nią zapoznać? Oczywiście, że nie.

Europejski Inspektor Ochrony Danych w swoich wytycznych (str. 14-15), wskazał, że dostęp do skrzynki nieobecnego pracownika jest możliwy, natomiast: 1) tryb dostępu powinien być opisany w procedurach, 2) powinniśmy zastanowić się, czy są inne sposoby wejścia w posiadanie informacji ze skrzynki pracownika, czyli – przykładowo – warto rozważyć ustawienie autorespondera, 3) dostęp do skrzynki nieobecnej osoby powinien być odpowiednio „dawkowany".

Gdy pracownik jest zatrudniony i korzysta na co dzień ze swojej skrzynki, może usuwać wiadomości, jeśli nie chce, aby pracodawca uzyskał do nich dostęp.

Udostępnienie skrzynki mailowej pracownika innemu pracownikowi jest co do zasady niedozwolone. I nie jest to jedynie kwestia ochrony danych osobowych. Przyjmuje się, że stosując takie niedozwolone rozwiązania jak udostępnienie skrzynki, naraża się pracownika np. na to, że ZUS zakwestionuje jego uprawnienie do zwolnienia i zasiłku chorobowego, albowiem wiadomości podpisane przez pracownika na zwolnieniu będą świadczyły o tym, że ten pracownik jednak jest w pracy i świadczy pracę na rzecz pracodawcy.

Z punktu widzenia przepisów z zakresu ochrony danych osobowych, osoby które zastępują nieobecnego pracownika, nie zawsze są odpowiednio upoważnione do przetwarzania danych osobowych i tym samym pracodawca naraża się na zarzut naruszenia ochrony danych osobowych - nieuprawnionego ujawnienia/nieuprawnionego dostępu do danych osobowych.

Zauważyć trzeba, że konieczność dostępu do skrzynki pocztowej byłego czy nieobecnego pracownika jest co do zasady uzasadniona. Biorąc pod uwagę rozwój przedsiębiorstwa, obowiązki wykonywane przez pracownika, projekty, za które odpowiada osobiście itp. Jednakże pracodawca, jako administrator, musi zawsze wyważać dwa dobra – swoje i pracownika. Dostęp do skrzynki pracownika powinien być zorganizowany w taki sposób, aby nie naruszać jego prywatności, nie zaprzeczać zasadzie minimalizacji danych, ograniczenia ich przechowywania, a także wiedzy koniecznej.

Podsumowanie

Monitorowanie skrzynki pocztowej pracowników może być spowodowane różnymi pobudkami. Pracodawca może kierować się chęcią sprawdzenia, czy pracownik w czasie pracy wykonuje tylko zadania służbowe, czy może rozprasza go prywatna korespondencja w czasie pracy. Ponadto, obowiązkiem pracodawcy jako administratora, jest odpowiednie zadbanie o to, aby w czasie nieobecności pracownika skrzynka mailowa była odpowiednio „zaopiekowana". Pracodawca musi mieć możliwość zapewnienia sobie ciągłości działania.

Wydaje się zatem, że najbardziej stosownym rozwiązaniem jest po prostu stworzenie procedur, które określają powyższe kwestie. Jeśli pracodawca stworzy procedury, w których jasno określi, że korzystanie ze skrzynki mailowej do celów prywatnych jest zabronione, pracownik nie będzie miał większych obaw, aby w czasie jego nieobecności zrobić przekierowanie poczty. Pracownik, który korzysta ze swojej skrzynki mailowej do celów prywatnych, musi być świadomy tego, że po pierwsze, skrzynka ta może być monitorowana przez pracodawcę, jeśli takie wprowadził rozwiązanie, a po wtóre, że w czasie jego nieobecności ktoś będzie miał do niej dostęp, czy to pracodawca, czy to inny pracownik.

adw. Justyna Cybulska

IV. Ostrzeżenie dla Administratorów - Pracodawców: nowy wyrok WSA podkreśla ryzyko niezabezpieczonych prywatnych komputerów pracowników.

Obecnie u wielu pracodawców praca zdalna czy hybrydowa stała się normą, zatem kwestia ochrony danych osobowych nabrała przy tym nowego znaczenia. W związku z czym, tym bardziej należy wskazać na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 października 2023 roku, który stanowi przełomowe orzeczenie w tej materii, podkreślając odpowiedzialność pracodawców za bezpieczeństwo danych osobowych przechowywanych na prywatnych urządzeniach pracowników.

Opis sytuacji.

Podstawą wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie był incydent związany z kradzieżą prywatnego komputera byłego pracownika Rzecznika Finansowego. To zdarzenie ujawniło poważne luki w ochronie danych osobowych, stawiając pod znakiem zapytania praktyki i procedury bezpieczeństwa obowiązujące w tej instytucji.

Komputer, na którym przechowywane były dane osobowe, był używany do pracy zdalnej. Niestety, nie przeprowadzono adekwatnej analizy ryzyka związanego z korzystaniem przez pracowników z prywatnych urządzeń, co doprowadziło do braku odpowiednich środków ochronnych. Brakowało procedur i zabezpieczeń, które byłyby skuteczne w przypadku kradzieży takiego urządzenia.

W wyniku tego zaniedbania, po kradzieży komputera, dane osobowe stały się narażone na potencjalne nieuprawnione ujawnienie. To zdarzenie stało się punktem zwrotnym, który skłonił UODO do podjęcia działań i nałożenia kary upomnienia na Rzecznika Finansowego. Wyrok WSA, podtrzymując decyzję UODO, potwierdził, że odpowiedzialność za zapewnienie bezpieczeństwa danych osobowych spoczywa na administratorze danych, w tym przypadku na Rzeczniku Finansowym.

Analiza Ryzyka i Środki Zapobiegawcze: kluczowe aspekty ochrony danych.

Przypadek naruszenia ochrony danych w Rzecznictwie Finansowym podkreśla znaczenie przeprowadzenia dogłębnej analizy ryzyka związanego z wykorzystaniem prywatnych komputerów przez pracowników do pracy zdalnej. Analiza ta powinna obejmować potencjalne zagrożenia dla danych osobowych oraz skuteczność obecnych środków ochronnych.

Wyroki WSA i decyzje UODO wyraźnie wskazują, że pracodawcy muszą rozważyć szereg czynników, takich jak możliwość nieautoryzowanego dostępu, ryzyko utraty urządzeń czy potencjalne naruszenia bezpieczeństwa danych. Należy również brać pod uwagę ryzyko związane z brakiem kontroli nad środowiskiem, w jakim pracownik wykonuje pracę zdalną, w tym bezpieczeństwo sieci, z której korzysta.

Oprócz analizy ryzyka, kluczowe jest wdrożenie odpowiednich procedur i zabezpieczeń, aby zapewnić skuteczną ochronę danych. Obejmuje to wdrożenie polityk dotyczących korzystania z prywatnych urządzeń, regularne szkolenia pracowników z zakresu bezpieczeństwa danych, stosowanie silnych haseł, szyfrowanie danych oraz zapewnienie zdalnego dostępu do danych w bezpieczny sposób, np. poprzez sieci VPN.

Ten przypadek pokazuje, że brak adekwatnych środków zapobiegawczych może prowadzić do poważnych konsekwencji prawnych i finansowych dla organizacji, podkreślając, że odpowiedzialność za ochronę danych spoczywa na pracodawcy, nawet jeśli dane są przetwarzane na prywatnym sprzęcie pracownika.

Odpowiedzialność pracodawcy w świetle ostatnich orzeczeń.

Wyroki Wojewódzkiego Sądu Administracyjnego i decyzje Prezesa UODO rzucają światło na rozszerzającą się odpowiedzialność pracodawców w kontekście ochrony danych osobowych. Kluczowym aspektem jest tutaj rozpoznanie, że odpowiedzialność za bezpieczeństwo danych osobowych nie kończy się na ścianach biura, ale rozciąga się również na prywatne urządzenia pracowników używane do pracy zdalnej.

WSA w Warszawie jednoznacznie wskazał, że w przypadku Rzecznika Finansowego to właśnie on, jako administrator danych, ponosi odpowiedzialność za naruszenie ochrony danych osobowych, nawet jeśli doszło do tego na skutek zdarzeń związanych z prywatnym komputerem pracownika. Sąd podkreślił, że pracodawca powinien zapewnić, iż dane są przetwarzane w sposób bezpieczny, niezależnie od lokalizacji sprzętu.

To orzeczenie ma dalekosiężne konsekwencje dla wszystkich pracodawców, podkreślając potrzebę przestrzegania zasad RODO i wdrożenia odpowiednich polityk dotyczących korzystania z prywatnych urządzeń do pracy. Wymaga to od organizacji nie tylko zrozumienia prawnych aspektów ochrony danych, ale także aktywnego zarządzania ryzykiem i wdrażania skutecznych strategii zabezpieczeń.

Konsekwencje dla pracodawców: dlaczego należy poważnie traktować ochronę danych?

Orzeczenie Wojewódzkiego Sądu Administracyjnego w Warszawie stanowi ważne przypomnienie dla wszystkich pracodawców o konsekwencjach niewystarczającej ochrony danych osobowych. W świetle tego wyroku, brak odpowiednich środków ochrony danych, zwłaszcza w kontekście pracy zdalnej i korzystania z prywatnych urządzeń, może prowadzić do poważnych konsekwencji prawnych i finansowych.
Kara upomnienia nałożona na Rzecznika Finansowego przez Prezesa UODO, a następnie podtrzymana przez WSA, stanowi jasny sygnał, że organy nadzorcze są gotowe egzekwować przestrzeganie przepisów RODO. To nie tylko możliwość nałożenia grzywien i kar, ale także ryzyko utraty zaufania klientów i negatywnego wpływu na reputację firmy.

Dla pracodawców ważne jest zrozumienie, że odpowiedzialność za ochronę danych osobowych leży u nich, niezależnie od tego, czy dane są przetwarzane na służbowym czy prywatnym sprzęcie pracowników. Wymaga to nie tylko wdrożenia odpowiednich polityk i procedur, ale także regularnego przeglądu i aktualizacji tych środków, aby zapewnić ich skuteczność i zgodność z obowiązującym prawem.

Wnioski

Wnioski płynące z wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie są jasne: pracodawcy muszą przyjąć proaktywne podejście do ochrony danych osobowych, niezależnie od miejsca ich przetwarzania. To zobowiązanie nie ogranicza się do korporacyjnych sieci i urządzeń, ale obejmuje także prywatne komputery pracowników wykorzystywane do pracy zdalnej.

Poniżej wskazuję na kilka kluczowych rekomendacji dla pracodawców w celu zwiększenia ochrony danych osobowych:

1. **Przeprowadzaj regularne analizy ryzyka:** regularnie oceniaj potencjalne zagrożenia dla danych osobowych przechowywanych i przetwarzanych przez Twoją organizację, w tym na prywatnych urządzeniach pracowników.
2. **Aktualizuj Politykę Ochrony Danych**: opracuj jasne zasady dotyczące korzystania z prywatnych urządzeń do pracy i regularnie je aktualizuj, aby były zgodne z najnowszymi standardami bezpieczeństwa.
3. **Wprowadzaj szkolenia dla pracowników**, podnoś ich świadomość: inwestuj w regularne szkolenia dla pracowników na temat bezpieczeństwa danych, podkreślając ich rolę w ochronie informacji.
4. **Monitoruj i reaguj na incydenty**: Ustal procedury monitorowania i reagowania na incydenty związane z bezpieczeństwem danych, aby szybko identyfikować i łagodzić potencjalne zagrożenia.
5. **Co, do technicznych środków ochrony**: zastosuj odpowiednie technologie, takie jak szyfrowanie i bezpieczne połączenia VPN, aby zabezpieczyć dane przetwarzane na prywatnych urządzeniach.

adw. Justyna Jabłonka
Inspektor Ochrony Danych

JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy