Jak reagować na incydenty w dni wolne od pracy?

Praktyczne porady na przerwę świąteczną

W TYM WYDANIU:

Incydenty i naruszenia ochrony danych osobowych w dni wolne od pracy i święta 1

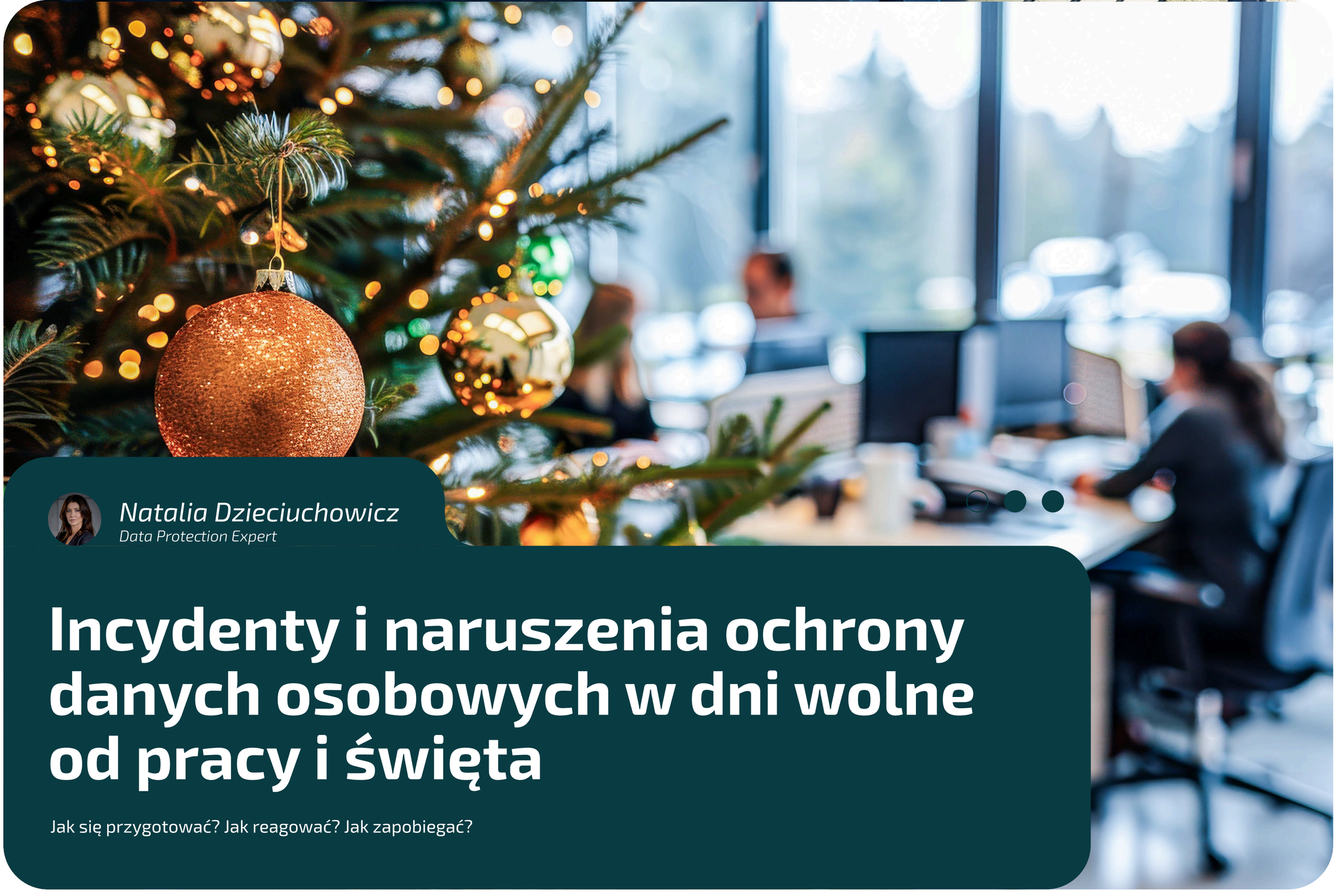
- Zarządzanie komunikacją 2
- Dokumentowanie działań 2

Posumowanie roku 2024 4

- Działalność EROD 5
- Przegląd decyzji nowego Prezesa UODO 6

LexDigital

lexdigital.pl



Natalia Dzieciuchowicz
Data Protection Expert

Incydenty i naruszenia ochrony danych osobowych w dni wolne od pracy i święta

Jak się przygotować? Jak reagować? Jak zapobiegać?

Reagowanie na incydenty w dni wolne, po godzinach pracy i w okresach świątecznych, kiedy urzędy nie działają, a kluczowe osoby są niedostępne, może być dużym wyzwaniem. Ważne jest, aby opracować odpowiednią strategię, plan awaryjny i komunikację, które pomogą w zarządzaniu sytuacją.

Należy podkreślić, że czas wymagany na dokonanie zgłoszenia naruszenia do Urzędu Ochrony Danych Osobowych (UODO) – 72 godziny od momentu zidentyfikowania naruszenia - nie uwzględnia dni wolnych od pracy (świąt, urlopów itp.).

Dokonanie zgłoszenia po wymaganym czasie związane jest z koniecznością przedłożenia powodów spóźnienia, do których nie można zaliczyć np. nieobecności/niedostępności osób decyzyjnych czy dni wolnych od pracy dla Urzędów Pocztowych czy firm kurierskich – zgłoszenia można bowiem dokonać online.

Urząd Ochrony Danych Osobowych (UODO) może zaakceptować opóźnienie tylko, jeśli organizacja przedstawi uzasadnione powody i udowodni, że podjęła wszelkie starania, aby zgłoszenie zostało dokonane na czas.

Poniżej proponujemy działania, które można podjąć, aby odpowiednio zareagować w warunkach ograniczonej aktywności przedsiębiorstwa w kontekście naruszeń potencjalnych lub takich, które faktycznie wystąpiły.

1. Przygotowanie i planowanie

- **Opracowanie planu awaryjnego**:
  Jako podmiot, który przetwarza dane osobowe (Administrator danych lub podmiot przetwarzający) postaraj się zidentyfikować potencjalne ryzyka, które mogą wystąpić w okresie świątecznym, weekendy itp. i opracuj plan zarządzania kryzysowego. Określ, kto i jakie decyzje będzie podejmować w sytuacjach awaryjnych, jeśli kluczowi decydenci będą niedostępni.

- **Ustalenie punktów kontaktowych:**
  Zaktualizuj listę osób dostępnych w czasie wolnym od pracy, w tym osoby pełniące dyżury

oraz alternatywne kontakty, które mogą podjąć działania w przypadku wystąpienia naruszenia.

- **Zabezpieczenie zasobów:**
  Zapewnij odpowiednią infrastrukturę i zasoby (np. wsparcie IT, zaplecze logistyczne), które będą działały w trybie awaryjnym, nawet jeśli nie wszystkie osoby będą dostępne.

- **Szkolenie pracowników:**
  Upewnij się, że zespół wie, jak zidentyfikować incydent i jak postępować w przypadku jego wystąpienia. Regularnie (a szczególnie przed okresami dłuższych nieobecności takich jak święta czy „długie weekendy") przypomnij pracownikom procedury identyfikacji i zgłaszania incydentów oraz procedury awaryjne.

2. Monitorowanie i wczesne wykrywanie incydentów

- **Zwiększenie monitoringu w kluczowych obszarach:**
  Upewnij się, że systemy monitorowania (np. IT, bezpieczeństwo, logistyka) są aktywne 24/7 i że są odpowiednio skonfigurowane, by wykrywać incydenty wcześnie.

- **Automatyczne alerty:**
  Skonfiguruj automatyczne powiadomienia, które mogą szybko poinformować odpowiedzialnych pracowników o incydencie, nawet w dni wolne.

3. Zarządzanie komunikacją

- **Jasne kanały komunikacji:**
  Ustal priorytetowe kanały komunikacji, które powinny być wykorzystywane w sytuacji wystąpienia incydentu (np. telefon awaryjny, e-mail, platformy komunikacyjne).

- **Komunikacja z klientami i partnerami:**
  Jeśli incydent dotyczy klientów lub zewnętrznych partnerów, zadbaj o przejrzyste komunikaty, które będą do nich kierowane, a mogą dotyczyć podejmowanych działań naprawczych czy koniecznych do podjęcia kroków minimalizujących skutki incydentów. Istotne jest, aby osoby odpowiedzialne za komunikację były w stanie szybko udzielać precyzyjnych i wyczerpujących informacji.

4. Działania w sytuacji kryzysowej

- **Decyzje na poziomie dyżurów:**
  Jeżeli kluczowe osoby są niedostępne, ważne jest, aby osoby pełniące dyżury miały jasno określony zakres uprawnień do podejmowania decyzji. Może to obejmować dostęp do niezbędnych zasobów, podejmowanie działań naprawczych czy informowanie osób dotkniętych naruszeniem.

- **Szybkie eskalowanie incydentu:**
  Jeśli incydent wymaga decyzji wyższej rangi, należy określić, w jaki sposób można uzyskać kontakt z osobami decyzyjnymi, np. przez systemy awaryjne, zewnętrzne konsultacje czy specjalne kontakty.

- **Priorytetyzacja incydentów:**
  Określ, które incydenty wymagają natychmiastowego działania (w tym zgłoszenia do organu nadzorczego – Urzędu Ochrony Danych Osobowych), a które mogą poczekać do powrotu kluczowych osób.

5. Dokumentowanie działań

- **Rejestracja incydentów:**
  Wszystkie działania związane z incydentem

powinny być szczegółowo dokumentowane, niezależnie od tego, czy incydent zostanie rozwiązany w ciągu kilku godzin, czy będzie trwał dłużej. Pomoże to w późniejszej analizie, ocenie reakcji i poprawie procesów na przyszłość. Jeśli zgłoszenie Prezesowi UODO nie jest możliwe w ciągu 72 godzin, administrator musi wyjaśnić w raporcie przyczyny opóźnienia.

- **Podsumowanie po incydencie:**
  Po zakończeniu incydentu, warto przygotować raport podsumowujący działania, jakie zostały podjęte, oraz ocenić skuteczność wdrożonych procedur awaryjnych.

6. Automatyzacja i narzędzia wspomagające

- **Wykorzystanie narzędzi do automatyzacji:**
  Jeśli to możliwe, zainwestuj w systemy, które mogą pomóc w automatyzowaniu reakcji na incydenty, takie jak systemy monitorowania, zarządzania incydentami, platformy komunikacyjne czy oprogramowanie do zdalnej obsługi.

- **Przygotowanie szablonów i procedur:**
  Miej przygotowane standardowe szablony komunikatów, raportów, decyzji do podjęcia w przypadku różnych typów incydentów.

Należy mieć świadomość, że pracownicy pełniący dyżury w czasie świąt (szczególnie w kontekście takich zdarzeń jak naruszenia ochrony danych osobowych) mogą odczuwać stres i presję. Ważne jest, aby zapewnić im odpowiednie wsparcie, być może w postaci dodatkowych zasobów czy możliwości konsultacji z podmiotem zewnętrznym doświadczonym w obsłudze takich procesów.
Reagowanie na incydenty w okresie świątecznym wymaga staranności, planowania i dobrze zorganizowanej komunikacji. Kluczowe jest przygotowanie zespołu, automatyzacja procesów oraz dostępność zasobów, które umożliwią szybką reakcję, nawet w czasie, gdy wielu decydentów jest niedostępnych.

Jakub Pawłowski
Radca prawny

Ochrona danych osobowych. Podsumowanie roku 2024

Rok 2024 był niezwykle dynamiczny dla sektora ochrony danych osobowych. Rozwój w obszarze nowych technologii (w szczególności sztucznej inteligencji) pokazał, jak ważny jest odpowiednio zaprojektowany i utrzymywany system ochrony danych. Mijający rok to również kulminacja inicjatyw ustawodawczych, tak na poziomie europejskim, jak i krajowym. AI Act, DORA, NIS 2 czy ustawa o ochronie sygnalistów – to tylko kilka przykładów aktów prawnych, które spędzały i nadal spędzają sen z powiek administratorom danych.

1. Nowy Prezes Urzędu Ochrony Danych Osobowych

Podsumowania 2024 r. nie sposób nie rozpocząć od zmiany na stanowisku Prezesa Urzędu Ochrony Danych Osobowych. Mirosław Wróblewski złożył ślubowanie 26 stycznia i zastąpił Jana Nowaka, który pełnił tę funkcję od 2019 r.

Według zapewnień nowego sternika, UODO ma bliżej współpracować ze specjalistami ds. ochrony danych osobowych i inspektorami ochrony danych, a nadto działać profilaktycznie i edukować.

Efekty tych zapowiedzi już widać. Został powołany Społeczny Zespół Ekspertów, który działać będzie przy Prezesie Urzędu Ochrony Danych Osobowych, a którego zadaniem będzie wspieranie Prezesa Urzędu w realizacji jego zadań określonych przepisami prawa, w szczególności w zakresie doradztwa i wyrażania opinii w sprawach przedstawionych Zespołowi.

Społeczny Zespół Ekspertów przy PUODO. W składzie znalazła się Mariola Więckowska z zespołu LexDigital.

Będzie rekomendował także inicjowanie działań w obszarze ochrony danych osobowych oraz przygotowywał w porozumieniu z PUODO ekspertyzy i stanowiska w zakresie dotyczącym ochrony danych osobowych. Członkowie Zespołu będą też promowali dobre praktyki oraz wykonywali inne zadania,

zlecone przez Prezesa Urzędu, dotyczące ochrony danych osobowych, szczególnie w obszarze nowych technologii.

Na uwagę zasługują również działania w zakresie weryfikacji kluczowych dla sektora poradników: tj. o zatrudnieniu oraz o zgłaszaniu naruszeń ochrony danych. Podjęte konsultacje, miejmy nadzieję, wpłyną na spójną praktykę, w szczególności w zakresie zgłaszania naruszeń.

źródło: GazetaPrawna.pl

Nowy Prezes, niezależnie od zapowiedzianych działań edukacyjnych i współpracy z sektorem, aktywnie prowadzi działania kontrolne oraz nakłada kary administracyjne za naruszenia.

2. Działalność Europejskiej Rady Ochrony Danych

Z wielu istotnych działań, które podjęła Europejska Rada Ochrony Danych (European Data Protection Board, EDPB) w 2024 warto odnotować przyjęcie strategii na lata 2024–2027, w której skupiła się na harmonizacji przepisów, współpracy w egzekwowaniu prawa, ochronie danych w zmieniającym się krajobrazie cyfrowym oraz globalnym dialogu o prywatności. Ważnym elementem jest również adaptacja do nowych ram regulacyjnych, takich jak akty o usługach i rynkach cyfrowych, oraz reagowanie na wyzwania związane w zmieniającym się krajobrazie cyfrowym oraz globalnym dialogu o prywatności. Ważnym elementem jest również adaptacja do nowych ram regulacyjnych, takich jak akty o usługach i rynkach cyfrowych, oraz reagowanie na wyzwania związane z AI. Strategia obejmuje także mechanizmy dochodzenia roszczeń w ramach Ram Ochrony Danych UE-USA.

Szerokim echem odbiła się również opinia EROD w sprawie modeli „zgoda lub zapłata” stosowanych przez platformy internetowe w kontekście przetwarzania danych do celów reklamy behawioralnej. EROD podkreśliła, że użytkownikom należy zapewnić rzeczywisty wybór, unikając warunkowania dostępu do usług wyłącznie zgodą na przetwarzanie danych lub uiszczaniem opłat. Takie praktyki mogą bowiem naruszać wymogi RODO, w szczególności dotyczące dobrowolności zgody. Opinia zawiera wskazówki, jak tworzyć alternatywy zgodne z zasadami ochrony danych

Jedną z ostatnich inicjatyw podjętych przez EROD jest również rozpoczęcie prac nad nowymi wytycznymi ws. przetwarzania danych osobowych na podstawie prawnie uzasadnionego interesu administratora. Z wielu kwestii poruszonych przez EROD w projekcie wytycznych na szczególną uwagę zasługuje stanowisko dotyczące przetwarzania danych osobowych w procesach marketingowych. EROD wskazała bowiem, że zgodnie z dyrektywą ePrivacy, wysyłanie niezamówionych komunikatów w celach marketingu bezpośredniego za pośrednictwem poczty e-mail, wiadomości SMS, MMS i innych podobnych aplikacji może mieć miejsce wyłącznie za uprzednią zgodą indywidualnego odbiorcy i dlatego w tym kontekście

przetwarzanie w celach marketingu bezpośredniego nie może być oparte o prawnie uzasadniony interes administratora. **Jest to zaskakujące stanowisko, bowiem dotychczasowa praktyka rynkowa pokazywała, że wielu przypadkach administratorzy zbierali zgody na konkretny kanał komunikacji, natomiast przetwarzanie danych osobowych opierali właśnie o prawnie uzasadniony interes.** Stanowisko EROD, o ile zostanie finalnie przyjęte, będzie miało istotny wpływ na organizację działań marketingowych.

3. Kary

Nowy Prezes Urzędu Ochrony Danych Osobowych niezależnie od zapowiedzianych działań edukacyjnych i współpracy z sektorem, aktywnie prowadzi działania kontrolne oraz nakłada kary administracyjne za naruszenia.

Niektóre z decyzji odbiły się dosyć szerokim echem i to nie tylko ze względu na ich wysokość, ale również ze względu na motywy, które legły u podstaw poszczególnych rozstrzygnięć. Do takich decyzji z pewnością należy decyzja nakładająca karę wysokości **4,05 mln zł na jeden z banków** za niezawiadomienie osób poszkodowanych wyciekiem danych osobowych. Prezes UODO uznał w tej sprawie, że brak powiadomienia zwiększa ryzyko dla osób dotkniętych naruszeniem, mimo że dane zostały jedynie omyłkowo przekazane. Rozstrzygnięcia nie zmieniło nawet to, że odbiorcą danych była instytucja finansowa objęta tajemnicą bankową. Na nic się zatem zdały argumenty, że odbiorca objęty tajemnicą bankową jest zaufanym odbiorcą, a przez to ryzyko naruszenia praw i wolności osób, których dane dotyczą nie jest wysokie.

Ciekawych wniosków dostarcza również decyzja ws. pewnej spółki medycznej, która została ukarana karą w wysokości **1,5 mln zł. za m.in. niewłaściwą ochronę danych osobowych po ataku hakerskim.** Naruszenie objęło dane 21 tys. osób, w tym informacje zdrowotne i finansowe. W toku postępowania Prezes UODO nie tylko zwrócił uwagę na niewystarczające środki bezpieczeństwa zastosowane przez administratora, ale również brak regularnego testowania systemów oraz niewłaściwą analizę ryzyka. Prezes UODO stwierdził, że Spółka przeprowadziła analizę ryzyka w sposób niewłaściwy, nie doszacowując ryzyka związanego z korzystaniem z oprogramowania bez wsparcia producenta (w tym braku aktualizacji), a także stosowaniem zbyt słabych haseł.

Prezes UODO nałożył również karę w wysokości **916,71 zł na stowarzyszenie sportowe za brak właściwej reakcji na ujawnienie danych osobowych, w tym w szczególności za brak zgłoszenia naruszenia.** Choć kara jest niska (pamiętać trzeba, że jej poziom zawsze jest dostosowany do wielkości podmiotu, a w przypadku przedsiębiorstw jego obrotów), to decyzja ta pokazuje dwie kwestie. Po pierwsze kontrola i ewentualna kara od Prezesa UODO może się przytrafić nie tylko dużym lub znanym podmiotom. Po drugie, przysłowiowe zamiatanie pod dywan spraw naruszeń nie jest dobrym rozwiązaniem.

Przytoczone powyżej decyzje i kary to jedynie wycinek bogatego orzecznictwa Prezesa UODO.

Skupiają jednak one jak w soczewce kluczowe aspekty budowania skutecznego systemu ochrony danych osobowych i pokazują, jak ważne jest podejście oparte na analizie ryzyka.

URZĄD OCHRONY DANYCH OSOBOWYCH

4. Przepisy

Pierwsze miejsce, a przynajmniej podium,
w konkursie na akt prawny roku 2024 z pewnością zajął AI Act, czyli *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) - tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).*

Przydługi tytuł rozporządzenia zwiastuje obszerność regulacji i tak w rzeczywistości jest. AI Act będzie bowiem kompleksowym aktem prawnym, który ma na celu uregulowanie rynku sztucznej inteligencji w Unii Europejskiej. Jego celem jest zapewnienie, aby systemy AI był bezpieczne i przejrzyste.

Chociaż AI Act nie zastępuje RODO, to oba akty są ze sobą ściśle powiązane i wzajemnie się uzupełniają. AI Act podobnie jak RODO wprowadza obowiązek przeprowadzenia szczegółowej oceny ryzyka dla systemów AI. Ocena ta obejmuje zarówno ryzyka związane z bezpieczeństwem danych, jak i ryzyka związane z dyskryminacją, manipulacją oraz innymi zagrożeniami dla praw podstawowych.

RODO nadal pozostaje głównym i podstawowym aktem prawnym regulującym przetwarzanie danych osobowych. AI Act natomiast uzupełnia RODO, wprowadzając dodatkowe wymagania dotyczące systemów AI, które przetwarzają dane osobowe. W niektórych przypadkach, np. przy ocenie skutków dla ochrony danych osobowych, może wystąpić pewne nakładanie się tych wymagań. Jednakże, oba akty prawne mają różne cele i powinny być stosowane łącznie.

Warto zwrócić uwagę, że AI Act swoim zakresem obejmuje nie tylko podmioty, które rozwijają systemy sztucznej inteligencji, ale również podmioty, które stosują takie systemy.

Dziękujemy za lekturę.

Grudzień 2024 nr 13/2024

To ostatnie wydanie Newslettera w mijającym, intensywnym dla branży roku.

Dziękujemy Państwu za lekturę i życzymy samych sukcesów w kolejnych 12 miesiącach.

W razie jakichkolwiek pytań czy wątpliwości jesteśmy do Państwa dyspozycji.

SKONTAKTUJ SIĘ Z NAMI

LexDigital