
LEX ARTIST

RODO - aktualności

[24.09.2024]
[03.10.2024]

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01 UODO: Wyciek danych łagodniej potraktujemy na terenach powodziowych

02 Europa chce chronić media. Polska – inwigilować dziennikarzy?

03 WSA oddalił skargę Morele.net na decyzję Prezesa UODO

04 WSA o zasadach informowania o pracowniczych karach porządkowych

05 NSA: administrator musi posiadać dowód ustnej zgody

06 Urząd Ochrony Danych Osobowych chce podwoić liczbę kontroli

07 TSUE: Urząd Ochrony Danych nie ma obowiązku nakładać kar za każde naruszenie RODO

08 Certyfikat kwalifikowanego podpisu elektronicznego nie powinien ujawniać numeru PESEL

09 Opinia Rzecznika TSUE: prawo dostępu do danych nie dotyczy algorytmów profilujących

10 WSA uchyla upomnienie wobec Banku za atak ransomware na podmiot przetwarzający

11 Meta naruszyła RODO. Zapłaci 91 mln euro kary

12 NSA: To administrator, a nie pracownik, ustala sposób zabezpieczenia danych

01 UODO: Wyciek danych łagodniej potraktujemy na terenach powodziowych

- **Kontekst:** Urząd Ochrony Danych Osobowych (UODO) ogłosił, że zastosuje "taryfę ulgową" wobec administratorów danych z terenów dotkniętych powodzią, którzy mogą mieć trudności z dochowaniem terminów związanych z ochroną danych osobowych.
- **Obowiązki wynikające z RODO**: Zgodnie z przepisami RODO, zgłoszenie naruszeń ochrony danych osobowych musi nastąpić w terminie 72 godzin od momentu ich stwierdzenia, co w sytuacji kryzysowej może być utrudnione.
- **Sytuacja powodziowa**: UODO rozumie, że z powodu powodzi wielu administratorów danych w południowych regionach Polski może mieć problemy z zachowaniem wymaganych terminów oraz obowiązków związanych z ochroną danych osobowych.
- **Wyjątkowe podejście**: UODO wskazuje, że zgłoszenie naruszenia może być niemożliwe przed opanowaniem sytuacji kryzysowej i wstępnym oszacowaniem strat..
- **Przyczyny opóźnień**: Urząd zaleca, aby w przypadku opóźnionych zgłoszeń wskazać przyczyny związane z siłą wyższą, w tym sytuacją powodziową oraz innymi trudnościami.
- **Elastyczność w weryfikacji**: UODO zapewnia, że zgłoszenia będą weryfikowane z uwzględnieniem trudnych warunków, a pracownicy Urzędu w pełni rozumieją wyjątkowość sytuacji.

Źródło: https://www.prawo.pl/biznes/wyciek-danych-osobowych-na-terenach-powodziowych,529117.html

02 Europa chce chronić media. Polska – inwigilować dziennikarzy?

- **Europejski akt o wolności mediów (EMFA)**, przyjęty 11 kwietnia 2024 roku, ma na celu ochronę pluralizmu i niezależności mediów w Unii Europejskiej. Nowe przepisy mają zagwarantować, że media będą mogły działać swobodnie, bez nadmiernej presji.
- **W Polsce** za wdrożenie EMFA odpowiada Ministerstwo Kultury i Dziedzictwa Narodowego, które zapowiada przygotowanie „nowego ładu medialnego". Zmiany obejmą m.in. wydawanie prasy przez samorząd oraz zasady działania Krajowej Rady Radiofonii i Telewizji.
- Jednym z kluczowych aspektów rozporządzenia EMFA są przepisy dotyczące **użycia oprogramowania szpiegującego wobec dziennikarzy**. Celem regulacji jest ochrona źródeł dziennikarskich oraz poufnej komunikacji.
- EMFA dopuszcza stosowanie **oprogramowania inwigilacyjnego** – takiego jak Pegasus – w wyjątkowych przypadkach, np. gdy zagrożone są poważne przestępstwa. Jednak warunki te obejmują:
  - Potrzebę uzyskania zgody sądu lub niezależnego organu.
  - Zagwarantowanie inwigilowanym osobom dostępu do skutecznych środków prawnych, w tym prawo do bycia informowanymi o inwigilacji.
- Polskie przepisy **nie spełniają wymogów EMFA** w zakresie kontroli nad inwigilacją mediów. Osoby inwigilowane przez służby nie mają prawa do informacji o prowadzonej kontroli, a sądy często udzielają zgody na operacje inwigilacyjne bez rzetelnej kontroli..
- Polskie służby mają szerokie uprawnienia do prowadzenia kontroli operacyjnej, także w sprawach mniej poważnych przestępstw, co rozbiega się z wymogami narzuconymi przez EMFA.

Źródło: https://panoptykon.org/emfa-w-polsce-inwigilacja-dziennikarzy

02 cd. Europa chce chronić media. Polska – inwigilować dziennikarzy?

- Organizacje społeczne, takie jak Helsińska Fundacja Praw Człowieka czy Fundacja Panoptykon, krytykują przepisy dopuszczające używanie oprogramowania szpiegującego, apelując o skuteczniejsze regulacje ochronne.
- Na razie brak konkretnych działań polskiego rządu w sprawie reformy kontroli nad służbami. Deklaracje złożone przed wyborami w 2023 roku, dotyczące ograniczenia stosowania Pegasusa, nie zostały zrealizowane.
- W Polsce dziennikarze formalnie mają prawo do ochrony swoich źródeł, jednak w praktyce są narażeni na działania operacyjne ze strony służb, co podważa skuteczność tej ochrony.

Źródło: https://panoptykon.org/emfa-w-polsce-inwigilacja-dziennikarzy

03 WSA oddalił skargę Morele.net na decyzję Prezesa UODO

- **Wyciek danych w sklepie internetowym Morele.net**: Pod koniec 2018 r. doszło do wycieku danych prawie 2,2 mln osób.
- **UODO nałożył karę**: W styczniu 2023 r. Prezes Urzędu Ochrony Danych Osobowych nałożył na Morele.net karę 3,8 mln zł za naruszenie ochrony danych.
- **Uzasadnienie decyzji UODO**: Naruszenie ochrony danych spowodowane było brakiem odpowiednich zabezpieczeń, takich jak:
  - brak szyfrowania części danych,
  - niewystarczające uwierzytelnianie,
  - brak analizy ryzyka związanej np. z logowaniem z sieci publicznej,
  - brak monitorowania ruchu sieciowego i reagowania na podejrzane działania.
- **Orzeczenia sądów**: Po wcześniejszym uchyleniu decyzji przez NSA, UODO przeprowadził ponowną analizę i jeszcze zwiększył karę. Wojewódzki Sąd Administracyjny 16 września 2024 r. oddalił skargę Morele.net na nałożenie kary
- **Uzasadnienie WSA**: Sąd uznał, że UODO poprawnie uwzględnił ocenę prawną NSA, a pracownicy UODO mają wystarczającą wiedzę, aby ocenić środki zabezpieczeń technicznych i organizacyjnych stosowanych przez Morele.net.

Źródło: https://www.rp.pl/dane-osobowe/art41173491-ogromna-kara-za-wyciek-danych-jest-wyrok-w-sprawie-uodo-vs-morele-net

04 WSA o zasadach informowania o pracowniczych karach porządkowych

- Tematem artykułu jest uchylenie decyzji Prezesa UODO przez WSA w Warszawie z września 2023 r., dotyczącej naruszenia ochrony danych osobowych pracownika WORD.
- Sprawa dotyczy ujawnienia informacji o karze porządkowej M.N. - pracownika WORD, podczas negocjacji w związku ze sporem zbiorowym o warunki pracy i płacy.
- Kierownik działu technicznego WORD ujawnił informację o karze porządkowej M.N. przy okazji negocjacji, mimo że nie był bezpośrednim przełożonym M.N.
- WORD twierdziło, że M.N. sam przekazał tę informację Kierownikowi w trakcie prowadzenia likwidacji szkody związanej z nałożeniem kary porządkowej.
- Prezes UODO uznał, że ujawnienie tych danych stanowiło naruszenie art. 6 ust. 1 RODO, ponieważ informacje zostały przekazane osobom nieuprawnionym.
- Sąd zakwestionował decyzję Prezesa UODO, zauważając, że organ nie odniósł się w sposób wystarczający do wyjaśnień WORD, w szczególności do twierdzenia, że M.N. sam przekazał te informacje podczas "luźnej rozmowy".
- WSA wskazał na konieczność ponownego rozpatrzenia sprawy z uwzględnieniem wszystkich zebranych dowodów i ich rzetelnej oceny.

Źródło: https://judykatura.pl/wsa-o-zasadach-informowania-o-pracowniczych-karach-porzadkowych/

04 cd. WSA o zasadach informowania o pracowniczych karach porządkowych

- Sąd zaznaczył, że sprawa może być rozpatrywana w dwóch aspektach:
  - Jeżeli Kierownik Działu Administracyjno-Technicznego pozyskał te informacje od pracodawcy i następnie je ujawnił.
  - Jeżeli Kierownik pozyskał te informacje od samego M.N. i je przekazał w trakcie negocjacji.
- WSA zwrócił uwagę na konieczność jasnego uzasadnienia decyzji Prezesa UODO, wskazując, które fakty zostały uznane za udowodnione oraz jakie dowody miały decydujące znaczenie.

Źródło: https://judykatura.pl/wsa-o-zasadach-informowania-o-pracowniczych-karach-porzadkowych/

05 NSA: administrator musi posiadać dowód ustnej zgody

- Kontekst: Sprawa dotyczy przetwarzania danych osobowych i przesyłania korespondencji członkowi Spółdzielni Mieszkaniowej na nieprawidłowy adres, po upływie jego pierwotnej zgody na tę formę doręczania pism.
- Stan faktyczny:
  - W 2015 roku członek Spółdzielni Mieszkaniowej wskazał inny adres do doręczania korespondencji, co było związane z jego częstymi wyjazdami do szpitali.
  - W 2016 roku ustne upoważnienie do doręczania korespondencji wygasło, jednak Spółdzielnia przez kolejne lata wysyłała dokumenty na wskazany wcześniej adres.
  - Adresat złożył skargę do Prezesa UODO, wskazując na nieprawidłowe przetwarzanie jego danych osobowych (m.in. imię, nazwisko, wysokość opłat).
- Decyzja Prezesa UODO (2021):
  - Prezes UODO stwierdził, że Spółdzielnia popełniła naruszenie, wysyłając korespondencję na nieprawidłowy adres od stycznia 2016 r. do grudnia 2019 r.
  - Spółdzielnia została upomniana za nieuprawnione ujawnienie danych osobowych.

Źródło: https://judykatura.pl/nsa-administrator-musi-posiadac-dowod-ustnej-zgody/

05 cd. NSA: administrator musi posiadać dowód ustnej zgody

- Postępowanie sądowe:
  - WSA w Warszawie oddalił skargę Spółdzielni, wskazując, że nie przedstawiono dowodów potwierdzających zgodne z prawem przesyłanie korespondencji po 2015 roku.
  - NSA oddalił skargę kasacyjną Spółdzielni, podkreślając, że odpowiedzialność administratora danych osobowych nie zależy od działań operatora pocztowego, lecz od tego, czy administrator zgodnie z prawem przetwarza dane (art. 5 ust. 1 RODO).
- Kluczowe wnioski:
  - Administrator danych osobowych (w tym przypadku Spółdzielnia) ma obowiązek zapewnienia pełnej zgodności z przepisami RODO przy przetwarzaniu danych, w tym przy ustalaniu adresu korespondencyjnego.
  - Nieprawidłowe przetwarzanie danych osobowych (np. wysyłanie korespondencji na nieaktualny adres) stanowi naruszenie zasad ochrony danych osobowych.
  - Ustna zgoda na przetwarzanie danych musi być jednoznacznie i odpowiednio udokumentowana, co w tej sprawie nie miało miejsca.

Źródło: https://judykatura.pl/nsa-administrator-musi-posiadac-dowod-ustnej-zgody/

06 Urząd Ochrony Danych Osobowych chce podwoić liczbę kontroli

- Urząd Ochrony Danych Osobowych (UODO) podsumował swoją działalność za rok 2023 na specjalnym briefingu prasowym prowadzonym przez prezesa Mirosława Wróblewskiego.
- W 2023 roku UODO przeprowadził 33 kontrole, natomiast w 2024 do czasu briefingu było ich już 58, co ilustruje znaczący wzrost aktywności Urzędu.
- Wysokość kar nałożonych w 2023 roku wyniosła 1,23 mln zł, podczas gdy jedna kara w 2024 roku (nałożona na Morele.net) osiągnęła już 3,8 mln zł.
- W 2023 roku do UODO wpłynęło 6962 skarg na niezgodne z prawem przetwarzanie danych, co stanowi wzrost o 33 względem 2022 roku.
- Prezes wskazał, że w 2024 roku liczba skarg może być jeszcze wyższa (w momencie briefingu było ich już ponad 5890), a skargi są coraz bardziej złożone.
- UODO zidentyfikował 14069 przypadków naruszeń zgłoszonych przez administratorów danych osobowych, którzy coraz lepiej oceniają ryzyko naruszenia praw osób fizycznych.
- Prezes Wróblewski przypomniał o obowiązku zgłaszania naruszeń danych osobowych w ciągu 72 godzin zgodnie z przepisami RODO.
- Trwają prace nad stworzeniem jednego miejsca do zgłaszania incydentów naruszeń cyberbezpieczeństwa i ochrony danych, we współpracy z Ministerstwem Cyfryzacji oraz NASK.
- Problemem UODO są kwestie finansowe – w porównaniu do planu budżetowego na 2024 rok, Urząd otrzymał 11 mln zł mniej na realizację ustawowych obowiązków.
- Wewnętrznie rozważana jest także konieczność przeprowadzki UODO do nowej siedziby oraz dostosowanie przepisów o ochronie danych osobowych do regulacji dotyczących sztucznej inteligencji (AI Act).

Źródło: https://cyberdefence24.pl/cyberbezpieczenstwo/w-uodo-wiecej-zgloszen-mniej-pieniedzy

07 TSUE: Urząd Ochrony Danych nie ma obowiązku nakładać kar za każde naruszenie RODO

- Kontekst: Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał orzeczenie dotyczące interpretacji przepisów RODO w kontekście odpowiedzialności krajowych urzędów ochrony danych za naruszenia przepisów ochrony danych osobowych.
- Sprawa dotyczyła niemieckiej kasy oszczędnościowej, której pracownica w sposób nieuprawniony przeglądała dane jednego z klientów.
- Kasa oszczędnościowa, po odkryciu naruszenia, podjęła wewnętrzne środki dyscyplinarne wobec pracownicy oraz zobowiązała ją do przekazania pisemnego oświadczenia o nieprzekazywaniu danych osobom trzecim.
- Kasa oszczędnościowa poinformowała o zdarzeniu inspektora ochrony danych w kraju związkowym Hesja, ale nie poinformowała bezpośrednio klienta, uznając, że nie było wysokiego ryzyka naruszenia jego praw.
- Klient dowiedział się o sytuacji przypadkowo i złożył skargę, żądając nałożenia kary na kasę oszczędnościową.
- Inspektor ochrony danych kraju związkowego zdecydował, że kary nie są konieczne, ponieważ zakład podjął odpowiednie działania naprawcze.
- TSUE orzekł, że krajowe urzędy nie muszą nakładać kar za każde naruszenie RODO, zwłaszcza jeśli instytucje, w których doszło do naruszenia, same zastosowały odpowiednie środki eliminujące naruszenie.
- Trybunał podkreślił, że RODO daje organom nadzorczym pewną swobodę w podejmowaniu decyzji dotyczących działań naprawczych, by zapewnić wysoką ochronę danych osobowych.
- TSUE pozostawił ocenę szczegółowych działań w tej sprawie niemieckiemu sądowi, który teraz musi zbadać, czy inspektor ochrony danych postąpił zgodnie z wytycznymi RODO.

Źródło: https://www.prawo.pl/biznes/urzad-ochrony-danych-nie-musi-nakladac-kar-za-kazde-naruszenie-rodo-wazny-wyrok-tsue,529219.html

08 Certyfikat kwalifikowanego podpisu elektronicznego nie powinien ujawniać numeru PESEL

- Kontekst: Prezes Urzędu Ochrony Danych Osobowych (UODO) zwrócił się do Ministra Cyfryzacji z prośbą o zmianę przepisów dotyczących usług zaufania oraz identyfikacji elektronicznej, aby chronić numer PESEL przed publicznym ujawnieniem w certyfikatach kwalifikowanego podpisu elektronicznego.
- Cel interwencji: Prezes UODO podnosi potrzebę zmiany ustawy, ponieważ obecne przepisy nie przewidują wymogu upubliczniania numeru PESEL, a mimo to jest on umieszczać w certyfikatach, co stanowi zagrożenie dla prywatności.
- Wnioski UODO: Numer PESEL nie musi być jedynym identyfikatorem w certyfikacie kwalifikowanego podpisu elektronicznego. Jako identyfikator można użyć innego numeru z rejestru publicznego, co poprawiłoby ochronę danych osobowych.
- Problem z PESEL-em: PESEL, jako numer wyjątkowy, zawiera informacje o konkretnej osobie, takie jak płeć czy wiek, co czyni go danymi wrażliwymi, które nie powinny być ujawniane osobom postronnym w procesie korzystania z podpisu elektronicznego.
- Obecne przepisy: Rozporządzenie eIDAS (910/2014) oraz ustawa o usługach zaufania z 2016 roku nie nakładają na dostawców kwalifikowanego podpisu elektronicznego obowiązku upubliczniania PESEL-u w certyfikatach.
- Stanowisko UODO: Sytuacja dotycząca niezgodnego z przepisami ujawniania numerów PESEL narusza zasady wynikające z RODO, zwłaszcza w kontekście przetwarzania danych osobowych, które powinno być dopuszczalne tylko wtedy, gdy jest niezbędne do realizacji prawa ciążącego na administratorze.
- Podsumowanie: Wnioskowanie UODO o zmianę przepisów dotyczących używania numeru PESEL w certyfikatach kwalifikowanego podpisu elektronicznego ma na celu lepszą ochronę danych osobowych i dostosowanie legislacji do rzeczywistych potrzeb weryfikacji tożsamości.

Źródło: https://uodo.gov.pl/pl/138/3373

09 Opinia Rzecznika TSUE: prawo dostępu do danych nie dotyczy algorytmów profilujących

- Obywatel Austrii nie mógł zakupić telefonu na abonament przez decyzję opartą na zautomatyzowanej ocenie kredytowej, zleconej przez podmiot doradczy.
- Obywatel skontaktował się z organem nadzorczym, by uzyskać dostęp do informacji o zasadach tej decyzji, lecz podmiot dostarczający ocenę kredytową nie ujawnił wystarczających informacji.
- Decyzja krajowego sądu administracyjnego utrzymała w mocy prawo obywatela do uzyskania istotnych informacji o zautomatyzowanym podejmowaniu decyzji.
- Firma oceniająca kredyt zaskarżyła decyzję pod kątem tajemnicy przedsiębiorstwa i ochrony danych, co doprowadziło do zadania TSUE pytań prejudycjalnych.
- Rzecznik Generalny TSUE wskazał, że:
    - Administrator danych ma obowiązek dostarczenia "istotnych informacji" o metodzie i kryteriach zastosowanych przy zautomatyzowanej decyzji.
    - Informacje te muszą być zrozumiałe, jasne i dostępne dla osoby, której dane dotyczą, aby mogła ona skutecznie skorzystać z przysługujących jej praw.
    - Administrator nie musi jednak ujawniać złożonych technicznie danych, takich jak algorytmy, które wymagałyby specjalistycznej wiedzy do zrozumienia.

Źródło: https://judykatura.pl/opinia-rzecznika-tsue-prawo-dostepu-do-danych-nie-dotyczy-algorytmow-profilujacych/

09 Opinia Rzecznika TSUE: prawo dostępu do danych nie dotyczy algorytmów profilujących

- Jeśli ujawnienie informacji mogłoby naruszyć prawa innych osób lub tajemnice przedsiębiorstwa, te informacje powinny być przekazane sądowi lub organowi nadzorczemu, który oceni interesy i zdecyduje o zakresie dostępu.

- Ostatecznym wnioskiem jest, że informacje przekazywane w ramach prawa dostępu muszą umożliwiać zrozumienie związków przyczynowych między przetwarzaniem danych a wynikiem decyzji, ale bez ujawniania szczegółów technicznych.

Źródło: https://judykatura.pl/opinia-rzecznika-tsue-prawo-dostepu-do-danych-nie-dotyczy-algorytmow-profilujacych/

10 WSA uchyla upomnienie wobec Banku za atak ransomware na podmiot przetwarzający

- Temat artykułu dotyczy decyzji Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie, który uchylił decyzję Prezesa Urzędu Ochrony Danych Osobowych (UODO) dotyczącą naruszenia przepisów RODO przez Bank w związku z cyberatakiem.
- Prezes UODO w decyzji z października 2023 r. nałożył na Bank upomnienie za udostępnienie danych osobowych pracownika Banku (m.in. imienia, nazwiska, numeru PESEL) osobom nieuprawnionym w wyniku ataku hakerskiego na firmę outsourcingową zajmującą się kadrami i płacami.
- UODO stwierdził naruszenie art. 5 ust. 1 lit. a RODO (zasada legalności, rzetelności i przejrzystości) oraz art. 6 ust. 1 RODO (brak podstawy prawnej dla przetwarzania danych).
- Bank, we współpracy z podmiotem przetwarzającym dane, podjął działania mające na celu minimalizację skutków ataku i zapobieżenie jego przyszłym powtórzeniom.
- WSA uchylił decyzję UODO, argumentując, że organ nie wykazał jednoznacznie, iż doszło do przekazania danych osobom nieuprawnionym. Brak było dowodów na faktyczne udostępnienie danych osobowych na rzecz osób trzecich.
- Sąd uznał, że UODO nie precyzował, na czym polegało "udostępnienie" danych w kontekście incydentu hakerskiego, co było kluczowe dla rozstrzygnięcia sprawy.
- WSA podkreślił, że UODO nie wyjaśnił ani w sferze faktów, ani w sferze prawa, dlaczego operacja przetwarzania danych miałaby być uznana za naruszenie przepisów RODO, które uzasadniałoby nałożenie środka naprawczego.
- Sprawa została skierowana do ponownego rozpoznania przez UODO, który będzie musiał uzupełnić dowody i jednoznacznie stwierdzić, czy doszło do naruszenia przepisów RODO.

Źródło: https://judykatura.pl/wsa-uchyla-upomnienie-wobec-banku-za-atak-ransomware-na-podmiot-przetwarzajacy/

11 Meta naruszyła RODO. Zapłaci 91 mln euro kary

- **Temat**: Irlandzki organ ochrony danych osobowych (DPC) nałożył na firmę Meta karę w wysokości 91 mln euro za naruszenie przepisów RODO.
- **Powód kary**: Kara dotyczy wykrycia, że hasła użytkowników Facebooka i Instagrama były przechowywane w postaci zwykłego tekstu, co narusza zasady bezpieczeństwa.
- **Jak doszło do ujawnienia problemu**: W marcu 2019 r. Meta ogłosiła, że podczas przeglądu bezpieczeństwa odkryto usterkę – hasła setek milionów użytkowników Facebooka Lite, dziesiątek milionów użytkowników Facebooka oraz milionów użytkowników Instagrama były przechowywane bez odpowiedniego zabezpieczenia.
- **Oświadczenie firmy Meta**: Spółka zapewniała, że usterka została naprawiona, a hasła nie były widoczne dla nikogo poza pracownikami Facebooka. Nie znaleziono też dowodów na nadużycia wewnętrzne związane z ujawnieniem tych haseł.
- **Działania organów nadzorczych**: W kwietniu 2019 r. DPC rozpoczęło dochodzenie, aby zbadać, czy Meta zastosowała odpowiednie środki bezpieczeństwa chroniące dane osobowe użytkowników.
- **Wynik dochodzenia**: Ustalono, że Meta popełniła cztery naruszenia RODO, m.in. niezgłoszenie naruszenia bez zbędnej zwłoki oraz brak odpowiednich zabezpieczeń technicznych.
- **Decyzja DPC**: W piątek organ ogłosił nałożenie kary w wysokości 91 mln euro, zwracając uwagę, iż Meta nie spełniła wymogów dotyczących zasad integralności i poufności RODO.

Źródło: https://www.gazetaprawna.pl/firma-i-prawo/artykuly/9622153,meta-naruszyla-rodo-zaplaci-wielka-kare.html

12 NSA: To administrator, a nie pracownik, ustala sposób zabezpieczenia danych

- Naczelny Sąd Administracyjny (NSA) oddalił skargę kasacyjną prezesa Sądu Rejonowego w Zgierzu dotyczącą nałożonej kary za nieodpowiednie zabezpieczenie danych osobowych.
- Sprawa dotyczyła zgubienia niezaszyfrowanego pendrive'a przez kuratora sądowego w Zgierzu w lutym 2020 r., na którym znajdowały się dane osobowe 400 osób.
- Dane te obejmowały imiona i nazwiska, adresy, numery PESEL, informacje o majątku i zarobkach, a także dane medyczne oraz informacje na temat wyroków skazujących.
- Prezes Sądu Rejonowego zgłosił incydent do Prezesa Urzędu Ochrony Danych Osobowych (UODO), jednak nie spełnił w pełni obowiązków: nie poinformował odpowiednio osób poszkodowanych o konsekwencjach zdarzenia ani o działaniach, które podjął w celu zminimalizowania skutków naruszenia.
- Prezes UODO stwierdził, że zabezpieczenia techniczne i organizacyjne wdrożone przez administratora danych w sądzie w Zgierzu były niewystarczające – pracownicy mieli samodzielnie zabezpieczać nośniki, a szyfrowanie zostało wprowadzone dopiero po incydencie.
- Jednorazowe szkolenie pracowników z zakresu ochrony danych nie było wystarczające do zapobieżenia utracie danych.
- UODO nałożył na administratora danych karę w wysokości 10 tys. zł, uznając, że nie podjęto odpowiednich działań zabezpieczających na poziomie technicznym, mimo że ryzyko zagubienia nośników danych zostało wcześniej zidentyfikowane.
- Sąd pierwszej instancji (WSA) oraz NSA podtrzymały decyzję UODO, wskazując, że administrator powinien był wdrożyć środki zabezpieczenia technicznego (np. szyfrowane nośniki), co znacznie zmniejszyłoby ryzyko nieuprawnionego dostępu w przypadku zgubienia danych.

Źródło: https://www.prawo.pl/biznes/pendrivea-zdanymi-osobowymi-jaka-kara-grozi-za-zgubienie,529273.html