
LEX ARTIST

RODO - aktualności

Data publikacji: 31.01.2025

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 WSA uchyla decyzję organu nadzorczego ze względu na niejasność decyzji

02 Kara dla Toyota Bank za niewłaściwe usytuowanie IOD i nieuwzględnienie profilowania w dokumentacji

03 TSUE: organ nadzorczy musi wykazać zamiar nadużycia prawa do żądania

04 Atak ransomware na EuroCert

05 Pracodawcy będą mierzyć, ważyć i pytać o wiek pracowników

06 PUODO: W 2024 r. dziesięciokrotnie wzrosła suma kwot nałożonych kar

07 Różne podejścia do ryzyka w ochronie danych osobowych - podsumowanie konferencji UODO

08 NIE ma obowiązku usuwania skrzynki mailowej byłego pracownika po ustaniu zatrudnienia

09 Czarne chmury nad transferami danych do USA

10 Pracownik zgubił pendrive'a z danymi osobowymi. Sąd uchylił karę dla firmy

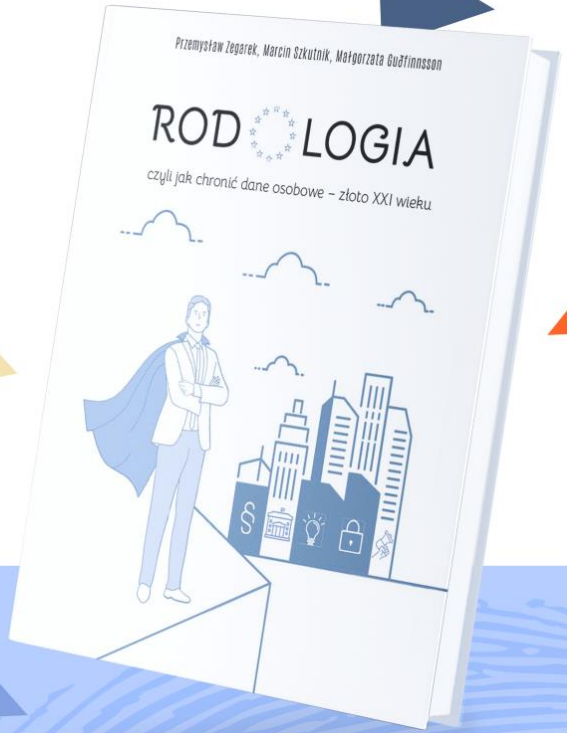
11 NSA przesądził, że numer księgi wieczystej to dane osobowe

12 UODO chce, by zgłaszać mu incydenty. Nawet gdy ryzyko jest niewielkie

13 WSA uchyla karę 103 000 zł za przesłanie maila do błędnego adresata

O naszej książce: poznaj RODOLOGIĘ

- Autorska koncepcja pięciu filarów
- Gotowe sprawdzone rozwiązania
- Automatyzacja rozwiązań
- Prosty język, przykłady i schematy
- Myślenie procesowe by default
- Ponad 500 stron w pięknej, premium formie



SODO

Razem z książką otrzymasz dostęp do aplikacji SODO z Modelowym RCP

01 WSA uchyla decyzję organu nadzorczego ze względu na niejasność decyzji.

- **Kontekst sprawy**: Prezes UODO stwierdził naruszenie przepisów RODO przez skarżonych, które miało miejsce w latach 2021-2022. Naruszenie polegało na przetwarzaniu danych osobowych za pomocą monitoringu wizyjnego, który obejmował obszary publiczne oraz na braku realizacji obowiązku informacyjnego wobec skarżących.
- **Monitoring wizyjny**:
  - W 2021 r. skarżeni zainstalowali 4 kamery na swojej nieruchomości.
  - Monitoring przez pewien czas obejmował obszary publiczne, takie jak fragment jeziora i drogi publicznej oraz prywatną łąkę należącą do osoby trzeciej.
  - Rejestracji podlegał jedynie obraz, a nagrania były przechowywane maksymalnie przez 3 tygodnie.
- **Decyzja Prezesa UODO**:
  - Skarżonym udzielono upomnienia za brak podstawy prawnej w przetwarzaniu danych oraz niewypełnienie obowiązku informacyjnego wobec skarżących.
  - Prezes UODO wskazał, że monitoring obejmował dane osób korzystających z przylegającej drogi publicznej, co było podstawą do uznania, że dochodziło do przetwarzania danych osobowych bez odpowiedniej podstawy prawnej.
- **Obowiązek informacyjny**:
  - Skarżeni nie oznakowali terenu objętego monitoringiem, co stanowiło naruszenie art. 13 ust. 1 i 2 RODO.

Źródło: https://judykatura.pl/wsa-uchyla-decyzje-organu-nadzorczego-ze-wzgledu-na-niejasnosc-decyzji/

01 cd. WSA uchyla decyzję organu nadzorczego ze względu na niejasność decyzji.

- Obowiązek ten powinien być spełniony przez administratora danych, nawet jeśli skarżący znają administratora.

- Postępowanie sądowe:
  - Skarżeni złożyli skargę na decyzję Prezesa UODO do Wojewódzkiego Sądu Administracyjnego w Warszawie (WSA).
  - WSA uchylił decyzję Prezesa UODO, wskazując na brak precyzyjnego uzasadnienia i niespełnienie wymogu jednoznaczności decyzji.
  - Zdaniem WSA, organ nie odwołał się do konkretnych dowodów, takich jak ujęcia z kamer, co powoduje problemy interpretacyjne decyzji.
- Wnioski:
  - Prezes UODO nie przedstawił wystarczających dowodów potwierdzających naruszenie przepisów RODO przez skarżonych.
  - Wymaga się, aby decyzje administracyjne były precyzyjne i nie pozostawiały miejsca na różne interpretacje.

Źródło: https://judykatura.pl/wsa-uchyla-decyzje-organu-nadzorczego-ze-wzgledu-na-niejasnosc-decyzji/

02 Kara dla Toyota Bank za niewłaściwe usytuowanie IOD i nieuwzględnienie profilowania w dokumentacji.

- **Kontekst sprawy**: Postępowanie dotyczyło naruszeń przepisów o ochronie danych osobowych przez Toyota Bank Polska S.A., w szczególności braku niezależności inspektora ochrony danych oraz nieprawidłowości związanych z profilowaniem danych klientów.
- **Profilowanie klientów**: Bank profilował dane klientów i potencjalnych klientów, przetwarzał wyniki oceny punktowej ryzyka kredytowego (tzw. scoring) oraz nadawał kategorie ryzyka kredytowego. Te działania nie były ujęte w rejestrze czynności przetwarzania danych, co stanowiło naruszenie.
- **Brak oceny skutków dla ochrony danych**: Bank nie przeprowadził wymaganej przepisami oceny skutków przetwarzania danych osobowych, mimo że zakres i cel profilowania wskazują na istotne ryzyko dla danych klientów.
- **Problemy z niezależnością inspektora ochrony danych**: Inspektor ochrony danych nie podlegał bezpośrednio najwyższemu kierownictwu banku (zarządowi), lecz znajdował się pod nadzorem dyrektora departamentu bezpieczeństwa. Prezes UODO uznał, że taka struktura ograniczała jego niezależność.
- **Kary finansowe**: Prezes UODO nałożył na Toyota Bank Polski S.A. dwie kary:
  - 261 918 zł za brak niezależności inspektora ochrony danych osobowych.
  - 314 302 zł za niewłaściwe uwzględnienie profilowania w dokumentacji i brak odpowiedniej analizy ryzyka.
- Łączna kwota kary wyniosła 576 220 zł.
- **Argumentacja Prezesa UODO**: Decyzja o nałożeniu kar była podyktowana koniecznością skutecznego, proporcjonalnego i odstraszającego działania wobec naruszeń RODO.

Źródło: https://uodo.gov.pl/pl/138/3519

02 cd. Kara dla Toyota Bank za niewłaściwe usytuowanie IOD i nieuwzględnienie profilowania w dokumentacji.

- **Reakcja banku**: Toyota Bank Polska S.A. wyjaśniała, że działania inspektora ochrony danych były niezależne, a jego umiejscowienie w strukturze organizacyjnej miało jedynie charakter administracyjny. Ponadto, bank zaktualizował rejestr czynności przetwarzania danych jeszcze przed kontrolą UODO.
- **Podsumowanie**: Sprawa ta podkreśla konieczność przestrzegania przepisów RODO dotyczących niezależności inspektora ochrony danych oraz właściwego udokumentowania działań związanych z profilowaniem i oceną ryzyka. Wysokość nałożonych kar ma działać odstraszająco, aby zapobiec podobnym naruszeniom w przyszłości.

Źródło: https://uodo.gov.pl/pl/138/3519

03 TSUE: organ nadzorczy musi wykazać zamiar nadużycia prawa do żądania.

- **Kontekst sprawy**: RODO daje administratorom danych oraz organom nadzorczym możliwość odmowy realizacji nadmiernych lub ewidentnie nieuzasadnionych żądań. W Austrii obywatel wniósł 77 skarg o naruszenie prawa dostępu do danych osobowych w okresie około 20 miesięcy, co doprowadziło do odmowy rozpatrzenia spraw przez organ nadzorczy.
- **Decyzja austriackiego organu nadzorczego (DSB)**: Organ odmówił rozpatrzenia skarg, powołując się na art. 57 ust. 4 RODO, uznając liczbę skarg za „nadmierną". Federalny sąd administracyjny unieważnił tę decyzję, uznając, że brak było wykazania złej wiary lub zamiaru nadużycia po stronie składającego skargę.
- **Wątpliwości prawne**: Trybunał administracyjny Austrii zwrócił się do TSUE z pytaniami prejudycjalnymi dotyczącymi:
  - Pojęcia „żądania" w art. 57 ust. 4 RODO i jego odniesienia do skarg składanych zgodnie z art. 77 ust. 1 RODO,
  - Konieczności wykazania zamiaru nadużycia oprócz samej liczby skarg jako elementu przesądzającego o ich nadmiernym charakterze,
  - Obowiązku stosowania łagodniejszych środków, takich jak pobranie opłaty, zanim odmówi się rozpatrzenia skarg.
- **Orzeczenie TSUE**:
  - Skargi składane na podstawie art. 77 ust. 1 RODO wchodzą w zakres pojęcia „żądania" w art. 57 ust. 4 RODO.
  - Liczba skarg nie może sama w sobie uzasadniać uznania ich za nadmierne. Konieczne jest wykazanie złej wiary lub zamiaru nadużycia ze strony osoby składającej skargi.

Źródło: https://judykatura.pl/tsue-organ-nadzorczy-musi-wykazac-zamiar-naduzycia-prawa-do-zadania/

03 cd. TSUE: organ nadzorczy musi wykazać zamiar nadużycia prawa do żądania.

- Organ nadzorczy ma wybór między pobraniem rozsądnej opłaty wynikającej z kosztów administracyjnych a odmową podjęcia działań. Wyboru należy dokonać, kierując się zasadą proporcjonalności oraz uwzględniając wszystkie istotne okoliczności.

- Rekomendacja TSUE: Zanim organ zdecyduje się na odmowę rozpoznania skargi z powodu jej nadmiernego charakteru, w pierwszej kolejności powinien rozważyć pobranie rozsądnej opłaty, o ile takie rozwiązanie jest adekwatne i wystarczające w danych okolicznościach.

- Wnioski: Orzeczenie TSUE określa, że nadmierne lub ewidentnie nieuzasadnione żądania muszą być precyzyjnie udowodnione przez organ nadzorczy, a zamiar nadużycia ma kluczowe znaczenie. Pobieranie opłat za rozpatrywanie skarg powinno być preferowanym środkiem przed odmową realizacji praw, aby zminimalizować ingerencję w prawa wynikające z RODO.

Źródło: https://judykatura.pl/tsue-organ-nadzorczy-musi-wykazac-zamiar-naduzycia-prawa-do-zadania/

04 Atak ransomware na EuroCert.

- Kontekst zdarzenia: EuroCert, znany dostawca podpisów kwalifikowanych, padł ofiarą ataku ransomware 12 stycznia br. w godzinach nocnych, co doprowadziło do wycieku danych osobowych klientów, kontrahentów i pracowników spółki. Próbka danych została już opublikowana, a reszta może trafić do darknetu.
- Wpływ incydentu: Dane, które mogły wyciec, obejmują:
    - Serię i numer dowodu osobistego,
    - PESEL, imię, nazwisko, datę urodzenia, wizerunek,
    - Hasła i nazwy użytkowników,
    - Dane kontaktowe (adres e-mail, numer telefonu).
- Łącznie przestępcy mogą mieć dostęp do ok. 65 GB danych.
- Podjęte działania:
    - Incydent zgłoszono na Policję, do CERT Polska oraz Prezesa Urzędu Ochrony Danych Osobowych (PUODO).
    - Rozpoczęto analizę ataku we współpracy z CSIRT NASK, CBZC i Ministerstwem Cyfryzacji.
- Skutki i rekomendacje dla klientów:
    - Zaleca się zastrzec numer PESEL w serwisie gov.pl oraz rozważyć zastrzeżenie dowodu osobistego w banku.

Źródła: https://niebezpiecznik.pl/post/atak-ransomware-na-eurocert-wyciekly-nawet-wizerunki-klientow/

https://www.msn.com/pl-pl/wiadomosci/other/gawkowski-po-ataku-na-eurocert-nale%C5%BCy-przejrze%C4%87-infrastruktur%C4%99-i-zmieni%C4%87-dane-logowania/ar-AA1xnoOh?ocid=BingNewsSerp

04 cd. Atak ransomware na EuroCert.

- Zmienić hasła do systemów, w których korzystano z takich samych danych logowania, oraz włączyć dwuskładnikowe uwierzytelnianie.
- Sprawdzić swoje dane w Biurach Informacji Gospodarczej oraz pobrać raport z BIK.
- Monitorować korespondencję e-mail i rozmowy telefoniczne w celu wykrycia potencjalnych prób phishingu lub podszywania się pod instytucje.

- Zalecenia dla firm i instytucji:
  - Przegląd infrastruktury IT w związku z danymi przetwarzanymi za pośrednictwem usług EuroCert.
  - Zablokowanie zdalnego dostępu i odcięcie powiązań infrastruktury z EuroCert.
  - Zmiana poświadczeń do kont oraz wdrożenie dwuskładnikowego uwierzytelniania.
  - Analiza logów systemowych od 1 listopada 2024 r. w celu wykrycia nieautoryzowanych działań.
  - Zgłaszanie podejrzanych incydentów do odpowiednich instytucji, takich jak CSIRT.
- Długofalowe skutki: Wykradzione dane mogą być publikowane, sprzedawane i wykorzystywane w przyszłości, co naraża klientów i firmy na ryzyko podszywania się, oszustw i innych incydentów jeszcze przez wiele lat.
- Informacje o firmie: EuroCert działa od 2012 roku i oferuje m.in. podpisy elektroniczne oraz pieczęcie. Obsługuje klientów korporacyjnych oraz publicznych, takich jak Miasto Stołeczne Warszawa, PKP, czy Poczta Polska.

Źródła: https://niebezpiecznik.pl/post/atak-ransomware-na-eurocert-wyciekly-nawet-wizerunki-klientow/

https://www.msn.com/pl-pl/wiadomosci/other/gawkowski-po-ataku-na-eurocert-nale%C5%BCy-przejrze%C4%87-infrastruktur%C4%99-i-zmieni%C4%87-dane-logowania/ar-AA1xnoOh?ocid=BingNewsSerp

05 Pracodawcy będą mierzyć, ważyć i pytać o wiek pracowników.

- **Kontekst**: Ministerstwo Rodziny, Pracy i Polityki Społecznej opracowało projekt rozporządzenia wprowadzającego maksymalne limity temperatury dla pracy w pomieszczeniach i na otwartej przestrzeni, co spotkało się z falą krytyki ze strony przedsiębiorców.
- **Wymóg ustalania tempa metabolizmu**: Projekt zakłada konieczność ustalania tempa metabolizmu pracowników na podstawie ich wzrostu, wagi i wieku zgodnie z Polskimi Normami, co budzi wątpliwości dotyczące ochrony danych osobowych i prawa pracy.
- **Koszty dla pracodawców**: Ustalanie tempa metabolizmu oraz dostosowanie stanowisk pracy do nowych norm może generować znaczne koszty (np. zakup Polskich Norm, wynajem ekspertów, dostosowanie infrastruktury, aktualizacja ocen ryzyka zawodowego).
- **Krytyka regulacji**: Eksperci ds. prawa pracy i organizacji pracodawców wskazują, że przepisy są nieprecyzyjne i nieprzemyślane, a istniejące pojęcia w przepisach BHP mogłyby wystarczyć bez wprowadzania nowych definicji.
- **Maksymalne temperatury**: Projekt wprowadza konkretne limity temperatur dla różnych rodzajów pracy (np. 28°C dla pracy biurowej, 22°C dla pracy o bardzo wysokim tempie metabolizmu) oraz obowiązek wdrożenia rozwiązań technicznych i organizacyjnych w przypadku ich przekroczenia.
- **Zakaz pracy w ekstremalnych warunkach**: W pomieszczeniach przekraczających 35°C oraz na otwartej przestrzeni powyżej 32°C (dla pracy o wysokim tempie metabolizmu) zakazuje się wykonywania pracy.
- **Proponowane środki organizacyjne**: Ministerstwo zaproponowało narzędzia takie jak praca zdalna, dodatkowe przerwy, skrócony czas pracy czy korzystanie z klimatyzowanych pomieszczeń.
- **Kontrowersje związane z ochroną danych**: Wymóg gromadzenia danych o wzroście, wadze i wieku pracowników może naruszać przepisy o ochronie danych osobowych, co podkreślają eksperci prawni.

Źródło: https://www.prawo.pl/kadry/jak-pracodawca-ma-ustalic-tempo-metabolizmu-by-wiedziec-jaka-jest-maksymalna-temperatura-na-stanowisku-pracy,531070.html

05 cd. Pracodawcy będą mierzyć, ważyć i pytać o wiek pracowników.

- Problematyczna implementacja: Przedsiębiorcy obawiają się trudności w jednolitym ustalaniu tempa metabolizmu i dostosowywaniu warunków w miejscu pracy do specyficznych potrzeb pracowników.
- Podsumowanie:
- Proponowane zmiany w przepisach dotyczących BHP, mające na celu regulowanie maksymalnych temperatur w miejscu pracy, budzą liczne kontrowersje. Pracodawcy wskazują na wysokie koszty implementacji oraz komplikacje związane z ustalaniem tempa metabolizmu pracowników. Eksperci podkreślają, że nowe obowiązki mogą naruszać ochronę danych osobowych i są trudne do realizacji technicznej oraz organizacyjnej dla firm, zwłaszcza małych przedsiębiorstw. Według krytyków, ministerstwo powinno skupić się na bardziej przejrzystych i efektywnych rozwiązaniach zgodnych z realiami gospodarczymi.

Źródło: https://www.prawo.pl/kadry/jak-pracodawca-ma-ustalic-tempo-metabolizmu-by-wiedziec-jaka-jest-maksymalna-temperatura-na-stanowisku-pracy,531070.html

06 PUODO: W 2024 r. dziesięciokrotnie wzrosła suma kwot nałożonych kar.

- **Wzrost kar za naruszenia RODO**: Suma nałożonych kar w 2024 roku wyniosła 13,3 mln zł, co stanowi aż 44% wszystkich kar od początku stosowania RODO w Polsce. Znacząca kara dotknęła mBank za niezawiadamianie klientów o wyciekach danych.
- **Egzekwowanie przepisów**: UODO podejmuje intensywniejsze działania m.in. wobec gigantów cyfrowych, takich jak Meta, w sprawie fałszywych reklam wykorzystujących wizerunki publiczne.
- **Edukacja i świadomość**:
  - UODO prowadzi działania edukacyjne, organizując seminaria i konferencje, w tym dotyczące praw dzieci, młodzieży i seniorów.
  - Wzmocniono współpracę z uniwersytetami trzeciego wieku oraz organizacjami branżowymi i publicznymi.
  - Program „UODO rusza w kraj" umożliwia działania regionalne mimo braku oddziałów w województwach.
- **Sztuczna inteligencja jako priorytet**:
  - Planowane powołanie grupy roboczej ds. AI.
  - Trwają postępowania dotyczące ochrony danych w narzędziach takich jak ChatGPT i wprowadzanych regulacjach.
- **Ochrona danych medycznych**: Jednostki medyczne objęto w 2024 roku priorytetowymi kontrolami w związku z licznymi skargami na przetwarzanie danych osobowych.
- **Działania wobec Meta**:
  - Wydano precedensowe decyzje w sprawie fałszywych reklam (deep-fake) wykorzystujących wizerunki.

Źródło: https://www.rp.pl/dane-osobowe/art41729641-miroslaw-wroblewski-prezes-uodo-wyzsze-kary-maja-efekt-prewencyjny

06 cd. PUODO: W 2024 r. dziesięciokrotnie wzrosła suma kwot nałożonych kar.

- Meta podejmuje działania eliminujące tego typu treści, ale skuteczność pozostaje niepewna.

- Polityczne postępowania:
  - Trwają sprawy dotyczące wyborów kopertowych oraz pozyskiwania numerów PESEL przez partie polityczne.
  - W obu przypadkach UODO dąży do skutecznego wyjaśnienia i zakończenia spraw w zgodzie z prawem.
- Priorytety na resztę kadencji:
  - Kontynuacja działań edukacyjnych, zwłaszcza dla młodzieży i seniorów, oraz intensyfikacja transgranicznej współpracy w kwestiach danych osobowych.
  - Rozwój nowych technologii – regulacje ochrony danych w zakresie AI oraz transfer danych poza Unię Europejską.
- Podsumowanie: UODO skutecznie łączy egzekwowanie przepisów o ochronie danych osobowych z intensywnymi działaniami edukacyjnymi i uświadamiającymi. Priorytetem na przyszłość jest ochrona danych w kontekście nowych technologii, w tym sztucznej inteligencji, oraz rozwiązywanie wielowątkowych spraw związanych z transgranicznym przetwarzaniem danych.

Źródło: https://www.rp.pl/dane-osobowe/art41729641-miroslaw-wroblewski-prezes-uodo-wyzsze-kary-maja-efekt-prewencyjny

07 Różne podejścia do ryzyka w ochronie danych osobowych - podsumowanie konferencji UODO.

- Temat konferencji: Konferencja „Ocena ryzyka a ochrona danych osobowych" dotyczyła zagadnień związanych z ryzykiem na gruncie RODO, w tym jego definicji, interpretacji oraz praktycznych konsekwencji.
- Różnorodność podejść do definicji ryzyka:
    - Negatywne podejście: ryzyko jako prawdopodobieństwo wystąpienia straty lub szkody.
    - Neutralne podejście: ryzyko jako każde zdarzenie odbiegające od stanu oczekiwanego (potencjalnie także zysk).
- Kluczowe pytanie: Na gruncie RODO brak jednoznacznej definicji ryzyka, co wpływa na realizację oceny skutków dla ochrony danych osobowych.
- Ocena skutków z różnych perspektyw:
    - Skupienie wyłącznie na zdarzeniu (np. wyciek danych).
    - Uwzględnienie dalszych konsekwencji, takich jak naruszenie praw i wolności.
- Brak spójności w normach: W regulacjach dotyczących bezpieczeństwa, takich jak normy ISO czy prawo ochrony środowiska, podejścia do ryzyka różnią się i niedopasowanie tych norm komplikuje praktykę.
- Problematyka ryzyka systemowego: Ryzyko systemowe (dotyczące całego państwa lub społeczeństwa) nie jest wprost poruszone w RODO, ale zyskuje na znaczeniu, szczególnie w kontekście regulacji sektorowych.
- Regulacja oparta na ryzyku (RBR):
    - RBR traktuje ryzyko nie tylko jako przedmiot regulacji, ale także jako metodę zarządzania regulacjami.

Źródło: https://www.prawo.pl/biznes/ocena-ryzyka-a-ochrona-danych-osobowych-konferencja-uodo,531132.html

07 cd. Różne podejścia do ryzyka w ochronie danych osobowych - podsumowanie konferencji UODO.

- Koncepcja ta coraz częściej staje się przedmiotem krytyki, np. z powodu nadmiernego upolitycznienia decyzji regulacyjnych.

- Znaczenie polityki i decyzji legislacyjnych: Potencjalne zmiany w podejściu do regulacji opartej na ryzyku mogą być wynikiem decyzji politycznych.
- Podsumowanie: Konferencja zorganizowana przez UODO i Uniwersytet Warszawski podkreśliła złożoność interpretacji ryzyka w kontekście RODO. Wagę mają zarówno spójne metody oceny skutków, jak i potrzeba dopasowania siatki pojęciowej z innych dziedzin. Pojęcie ryzyka systemowego oraz regulacji opartej na ryzyku (RBR) wskazują na konieczność dostosowywania przepisów ochrony danych do zmieniających się realiów regulacyjnych i politycznych.

Źródło: https://www.prawo.pl/biznes/ocena-ryzyka-a-ochrona-danych-osobowych-konferencja-uodo,531132.html

08 NIE ma obowiązku usuwania skrzynki mailowej byłego pracownika po ustaniu zatrudnienia.

- Kontekst: Sprawa dotyczy zarządzania adresami mailowymi pracowników po ustaniu ich zatrudnienia, co ma kluczowe znaczenie z punktu widzenia ochrony danych osobowych i komunikacji firmowej.
- Wnioski z wyroku i decyzji:
    - Pod żadnym pozorem nie wolno odpowiadać na wiadomości przychodzące na adres mailowy byłego pracownika po zakończeniu jego zatrudnienia.
    - Zaleca się niezwłoczne wprowadzenie autorespondera, który poinformuje nadawcę wiadomości, że dany adres nie jest już aktywny.
    - Przykładowa treść autorespondera:

    „Dziękujemy za wiadomość. Adres, na który została skierowana, nie jest już aktualny do prowadzenia korespondencji ze Spółką X. W celu uzyskania informacji prosimy o kontakt z XVZ @(...) (Wiadomość została wygenerowana automatycznie. Prosimy na nią nie odpowiadać.)”
- Kluczowe działania do wdrożenia:
- Opracowanie zasad zarządzania adresami mailowymi byłych pracowników, w tym:
    - Ustalenie okresu, przez jaki ma być wysyłany autoresponder.
    - Określenie momentu, w którym skrzynka e-mailowa zostanie dezaktywowana (wiadomości zaczynają się "odbijać").
    - Ustalenie procedury dostępu do zawartości skrzynki w uzasadnionych przypadkach.

Źródło: https://www.linkedin.com/posts/dominika-dorre-kolasa_nie-ma-obowi%C4%85zku-usuwania-skrzynki-mailowej-activity-7288091336941953025-a6pz?utm_source=share&utm_medium=member_desktop

08 cd. NIE ma obowiązku usuwania skrzynki mailowej byłego pracownika po ustaniu zatrudnienia.

- Rozważenie możliwości przekierowania wiadomości w okresie wypowiedzenia ze zwolnieniem z obowiązku świadczenia pracy – wskazanie jasnych okoliczności dla takiego rozwiązania.

- Komunikacja zasad wobec pracowników:
  - Poinformowanie pracowników o zasadach korzystania z adresów e-mail i zarządzania nimi po zakończeniu zatrudnienia.
  - Szkolenie pracowników w zakresie zasad prowadzenia korespondencji mailowej w firmie.
  - Regularne przypominanie, że sprzęt, oprogramowanie, adresy e-mail i inne zasoby służbowe pozostają własnością pracodawcy i służą wyłącznie celom zawodowym.

Źródło: https://www.linkedin.com/posts/dominika-dorre-kolasa_nie-ma-obowi%C4%85zku-usuwania-skrzynki-mailowej-activity-7288091336941953025-a6pz?utm_source=share&utm_medium=member_desktop

09 Czarne chmury nad transferami danych do USA.

- Konflikt dotyczy: porozumienia między Unią Europejską a Stanami Zjednoczonymi w sprawie przesyłania danych osobowych – tzw. Data Privacy Framework (DPF).
- Podstawa prawna: Umowa DPF została zatwierdzona przez Komisję Europejską w lipcu 2023 r. jako zapewniająca poziom ochrony danych porównywalny z RODO.
- Zagrożenia wynikające z działań Donalda Trumpa:
    - Nowa administracja USA może podważyć zasady ochrony danych wprowadzone przez poprzedniego prezydenta Joego Bidena.
    - Sparaliżowano działanie Rady ds. Prywatności i Swobód Obywatelskich (PCLOB), odpowiedzialnej za kontrolowanie ochrony danych w Stanach Zjednoczonych.
    - Donald Trump zapowiedział rewizję rozporządzeń swojego poprzednika dotyczących nadzoru i bezpieczeństwa, które stanowią podstawę obecnych amerykańskich gwarancji ochrony danych.
- Uwagi prawne Maxa Schremsa:
    - Max Schrems, prawnik i aktywista, zauważa, że umowa DPF od początku opierała się na niestabilnych podstawach prawnych.
    - Schrems już wcześniej doprowadził do unieważnienia poprzednich porozumień o wymianie danych między UE a USA, znanych jako „Bezpieczna przystań" i „Tarcza prywatności".

Źródło: https://www.gazetaprawna.pl/firma-i-prawo/artykuly/9719253,rodo-czarne-chmury-nad-transferami-danych-do-usa.html

09 cd. Czarne chmury nad transferami danych do USA.

- **Wpływ na firmy**: W przypadku unieważnienia umowy DPF wiele firm z UE, które korzystają z amerykańskich usług chmurowych lub platform internetowych, może znaleźć się w sytuacji prawnej niepewności.
- **Rekomendacja**: Eksperci, w tym Max Schrems, sugerują firmom przygotowanie planów awaryjnych na wypadek dalszych zmian w amerykańskim prawie.
- **Dodatkowe działania**: Umowa DPF została także zaskarżona w Trybunale Sprawiedliwości UE przez francuskiego deputowanego Philippe'a Latombe, co oznacza dodatkowe ryzyko dla jej trwałości.
- **Wniosek**: Stabilność i przyszłość DPF są zagrożone, co szczególnie odbije się na firmach i organizacjach korzystających z transferu danych do USA. Kontrowersje polityczne w Stanach Zjednoczonych mogą skutkować poważnymi konsekwencjami prawnymi dla współpracy transatlantyckiej w zakresie ochrony danych osobowych.

Źródło: https://www.gazetaprawna.pl/firma-i-prawo/artykuly/9719253,rodo-czarne-chmury-nad-transferami-danych-do-usa.html

10 Pracownik zgubił pendrive'a z danymi osobowymi. Sąd uchylił karę dla firmy.

- **Kontekst sprawy**: Wojewódzki Sąd Administracyjny (WSA) w Warszawie orzekł w sprawie nałożenia kary na restaurację z Podkarpacia przez Prezesa Urzędu Ochrony Danych Osobowych (UODO). Powodem był incydent związany z utratą niezaszyfrowanych danych pracownika na pendrivie.
- **Stanowisko Prezesa UODO**: UODO oskarżył administratora danych o przerzucenie obowiązku zabezpieczania danych na pracowników, co miało doprowadzić do incydentu.
- **Argumenty administratora**:
  - Administrator wdrożył procedury dotyczące korzystania z nośników danych, w tym obowiązek szyfrowania pendrive'ów.
  - Pracownik został poinstruowany, jak stosować oprogramowanie szyfrujące, m.in. poprzez krótkie filmy instruktażowe.
  - Przeprowadzono wewnętrzne audyty procesu zarządzania danymi.
- **Orzeczenie sądu**:
  - WSA uchylił decyzję UODO, uznając, że administrator danych wypełnił swoje obowiązki prawne na poziomie organizacyjnym i technicznym.
  - Sąd stwierdził, że incydent był wynikiem ludzkiego błędu pracownika, a nie zaniedbania administratora.
  - Stwierdzono, że administrator nie może być odpowiedzialny za naruszenie ochrony danych, jeśli pracownik nie przestrzegał wdrożonych procedur.
- **Znaczenie wyroku**:
  - Wyrok precyzuje granice obowiązków i odpowiedzialności między administratorem a pracownikami w zakresie ochrony danych osobowych.

Źródło: https://pro.rp.pl/abc-firmy/art41721351-pracownik-zgubil-pendrive-a-z-danymi-osobowymi-sad-uchylil-kare-dla-firmy

10 cd. Pracownik zgubił pendrive'a z danymi osobowymi. Sąd uchylił karę dla firmy.

  - Wskazuje, że wypełnienie wymogów przewidzianych w art. 32 RODO zdejmuje bezpośrednią odpowiedzialność administratora za incydenty wynikające z błędów pracowników.

- Eksperci o sprawie:
  - Zdaniem ekspertów, odpowiedzialność administratora powinna być oceniana w kontekście analizy ryzyk, wdrożonych środków ochrony oraz przestrzegania procedur przez pracowników.
  - Nie można wymagać od administratora całkowitego wyeliminowania ryzyka wycieków danych, lecz tylko odpowiedniego dostosowania środków ochrony do specyfiki przetwarzania danych.
- Perspektywa UODO: Urząd Ochrony Danych Osobowych zapowiedział dalszą analizę pisemnego uzasadnienia wyroku przed podjęciem kolejnych działań.

Źródło: https://pro.rp.pl/abc-firmy/art41721351-pracownik-zgubil-pendrive-a-z-danymi-osobowymi-sad-uchylil-kare-dla-firmy

11 NSA przesądził, że numer księgi wieczystej to dane osobowe.

- Kontekst: Naczelny Sąd Administracyjny (NSA) w wyroku z 28 stycznia 2025 roku orzekł, że numery ksiąg wieczystych są danymi osobowymi, zgodnie z definicją danymi osobowymi w art. 4 RODO. Wyrok kończy trwający spór między Prezesem UODO a byłym Głównym Geodetą Kraju (GGK).
- Kluczowe fakty:
  - NSA podtrzymał decyzję Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie z 2021 roku, oddalając skargę kasacyjną GGK.
  - Zgodnie z wyrokiem, publikowanie numerów ksiąg wieczystych bez podstawy prawnej narusza przepisy o ochronie danych osobowych.
  - Numery ksiąg wieczystych umożliwiają identyfikację właścicieli nieruchomości, co naraża ich na ryzyko kradzieży tożsamości.
- Decyzja NSA oznacza:
  - Potwierdzenie zasadności administracyjnej kary pieniężnej w wysokości 100 tys. zł, nałożonej w 2020 roku przez Prezesa UODO na GGK za publikację tych numerów w serwisie Geoportal2.
  - Ugruntowanie stanowiska, że numery ksiąg wieczystych są danymi osobowymi zgodnie z RODO.
- Dlaczego to ważne?
  - Opublikowanie numerów ksiąg wieczystych pozwalało na uzyskanie dostępu do szerokiego zakresu danych osobowych, takich jak imiona, nazwiska, numery PESEL, adresy nieruchomości i informacje o hipotece.
  - Działanie GGK ułatwiało użytkownikom serwisu Geoportal2 bezpośredni dostęp do zawartości ksiąg wieczystych, co naruszało przepisy o ochronie danych osobowych.

Źródło: https://uodo.gov.pl/pl/138/3533

11 cd. NSA przesądził, że numer księgi wieczystej to dane osobowe.

- Wypowiedź Prezesa UODO: Prezes UODO, Mirosław Wróblewski, podkreślił, że wyrok NSA kończy dyskusję na temat numery ksiąg wieczystych jako danych osobowych. „Wszystkie argumenty przedstawione przez Prezesa UODO zostały potwierdzone" – zaznaczył.

Źródło: https://uodo.gov.pl/pl/138/3533

12 UODO chce, by zgłaszać mu incydenty. Nawet gdy ryzyko jest niewielkie.

- Urząd Ochrony Danych Osobowych (UODO) przedstawił stanowisko, zgodnie z którym nawet niskie ryzyko naruszenia ochrony danych osobowych może wymagać zgłoszenia go do UODO.
- Na konferencji „Ocena ryzyka a ochrona danych osobowych" zapowiedziano publikację zaktualizowanego poradnika o trzystopniowym modelu postępowania w przypadku naruszeń danych osobowych:
    - Stopień 1: Brak ryzyka – należy jedynie udokumentować incydent.
    - Stopień 2: Ryzyko zwykłe – konieczne jest zgłoszenie do UODO i udokumentowanie.
    - Stopień 3: Wysokie ryzyko – wymaga dokumentacji, zgłoszenia do UODO oraz powiadomienia osób, których dane dotyczą.
- Zgłoszenie incydentu do UODO nie jest równoznaczne z naruszeniem przepisów RODO – jest to zawiadomienie o zaistniałej sytuacji, a nie przesądzenie o winie organizacji.
- Podczas konferencji zwrócono uwagę na ryzyko związane z brakiem zgłoszenia – może to skutkować wyższymi karami, jeśli UODO dowie się o zdarzeniu z innych źródeł, np. mediów.
- Pojęcie „zaufanego odbiorcy" zostało omówione szczegółowo – aby dana organizacja mogła być tak zakwalifikowana, konieczna jest znajomość i ocena jej procedur bezpieczeństwa. Przyjęto, że nie każdy podmiot z sektora publicznego automatycznie spełnia te kryteria.
- Eksperci sugerują, że nowe podejście UODO może wymagać przeglądu i aktualizacji procedur dotyczących naruszeń ochrony danych w organizacjach.
- Podsumowanie: Zmiany w interpretacji przepisów przez UODO oznaczają bardziej rygorystyczne podejście do kwestii zgłaszania naruszeń ochrony danych osobowych. Organizacje muszą przygotować się na dokładniejsze analizy ryzyka oraz dostosowanie swoich procedur do nowych wytycznych.

Źródło: https://www.prawo.pl/biznes/czy-trzeba-zglosic-naruszenie-danych-osobowych-do-uodo,531221.htm

13 WSA uchyla karę 103 000 zł za przesłanie maila do błędnego adresata.

- Kontekst sprawy: Wyrok Wojewódzkiego Sądu Administracyjnego (WSA) w Warszawie uchyla decyzję Prezesa Urzędu Ochrony Danych Osobowych (UODO) z października 2023 r., dotyczącą nałożenia kary pieniężnej na Towarzystwo Ubezpieczeniowe za brak zgłoszenia naruszenia danych osobowych.
- Stan faktyczny: Prezes UODO ukarał Towarzystwo Ubezpieczeniowe kwotą ponad 103 000 zł za niezawiadomienie organu o naruszeniu, gdzie w wyniku błędu w komunikacji e-mail ujawniono dane osobowe osoby trzeciej, w tym imię, nazwisko, adres, informacje o szkodzie, model i numer rejestracyjny samochodu.
- Stanowisko Towarzystwa: Towarzystwo przeprowadziło wewnętrzną analizę ryzyka i uznało, że naruszenie nie prowadzi do ryzyka większego niż niskie, dlatego odnotowało problem w swoim rejestrze, ale nie zgłosiło go Prezesowi UODO.
- Decyzja Prezesa UODO:
  - Stwierdzono naruszenie art. 33 ust. 1 RODO, mówiącego o obowiązku zgłoszenia naruszenia ochrony danych w przypadku ryzyka dla praw i wolności osób fizycznych.
  - Prezes UODO uznał, że ujawnione dane mogły skutkować konsekwencjami dla osoby, której dotyczą, co nakładało obowiązek zgłoszenia naruszenia.
- Ocena WSA w Warszawie:
  - WSA stwierdził, że Prezes UODO nie uzasadnił wystarczająco, dlaczego okoliczności sprawy wskazywały na wysokie ryzyko naruszenia praw i wolności osoby poszkodowanej.

Źródło: https://judykatura.pl/wsa-uchyla-kare-103-000-zl-za-przeslanie-maila-do-blednego-adresata/

13 cd. WSA uchyla karę 103 000 zł za przesłanie maila do błędnego adresata.

- Sąd wskazał brak analizy ryzyka dokonanej przez UODO, uwzględniającej np. zachowanie nieuprawnionego odbiorcy danych.
- Prezes UODO bez podstaw przywołał argument ujawnienia numeru PESEL, choć w sprawie nie było dowodów na takie naruszenie.

- Orzeczenie WSA:
  - Sąd uchylił decyzję Prezesa UODO, uznając ją za przedwczesną i niewystarczająco uzasadnioną.
- WSA podkreślił, że organ administracyjny powinien bardziej szczegółowo wyjaśnić podstawy swojego stanowiska i nie może wymagać od sądu czy strony skarżącej domyślania się intencji organu.

Źródło: https://judykatura.pl/wsa-uchyla-kare-103-000-zl-za-przeslanie-maila-do-blednego-adresata/