
LEX ARTIST

RODO - aktualności

Data publikacji: 17.10.2025

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 Nowe przepisy w sprawie przejrzystości i targetowania reklamy politycznej

02 EROD i Komisja Europejska zatwierdzają wspólne wytyczne dot. DMA i RODO

03 e-Doręczenia w administracji publicznej to fikcja

04 Wzmocnienie bezpieczeństwa Schengen i zapobieganie nieuregulowanej migracji

05 Sąd wymierzył karę 2000 zł za przetwarzanie danych bez uprawnienia

06 Szeroki nakaz przechowywania wszystkich czatów przez OpenAI uchylony

07 ENISA Threat Landscape 2025 – kluczowe wnioski dla bezpieczeństwa cybernetycznego w Europie

08 Jawność pod kontrolą. Ministerstwo chce wiedzieć, kto zagląda do ksiąg wieczystych

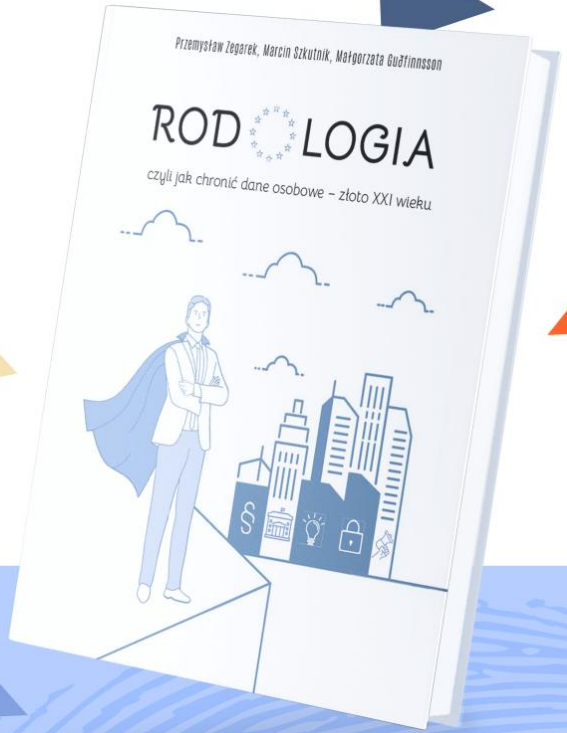
09 NSA podtrzymał decyzje Prezesa UODO dotyczące przetwarzania danych niedoszłych klientów banków

10 Raport ZFODO: Systematycznie rośnie liczba naruszeń powodowanych przez źródła zewnętrzne (w tym hakerów)

11 Cyberatak na F5: Skradziono kod źródłowy. Co to oznacza dla firm w Polsce?

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 Nowe przepisy w sprawie przejrzystości i targetowania reklamy politycznej

- Kontekst: Od 10 października 2025 r. zacznie obowiązywać bezpośrednio w państwach UE rozporządzenie (UE) 2024/900 dotyczące przejrzystości i targetowania reklamy politycznej w przestrzeni cyfrowej.
- Cel regulacji: Zwiększenie przejrzystości reklamy politycznej, ochrona praw podstawowych użytkowników oraz zapobieganie dezinformacji i ingerencji państw trzecich w procesy wyborcze.
- Zakres podmiotowy: Rozporządzenie obejmuje:
  - dostawców usług reklamy politycznej,
  - wydawców reklamy politycznej,
  - sponsorów (zleceniodawców reklam politycznych).
- Nowe obowiązki:
  - obowiązek ujawniania finansowania reklamy politycznej,
  - czytelne oznaczanie reklam, by przekaz był jednoznaczny dla odbiorców,
  - prowadzenie rejestrów i repozytorium reklam politycznych,
  - opisanie metod targetowania w przejrzysty sposób oraz coroczna ocena ryzyka dla praw i wolności osób.
- Ograniczenia w targetowaniu reklam politycznych online:

Źródło: https://uodo.gov.pl/pl/138/3912

01 cd. Nowe przepisy w sprawie przejrzystości i targetowania reklamy politycznej

- zakaz profilowania na podstawie szczególnych kategorii danych osobowych (np. poglądy polityczne, religia, orientacja seksualna),
- zakaz stosowania targetowania na podstawie danych dotyczących osób, które nie osiągną wieku wyborczego przed kolejnymi wyborami,
- możliwość targetowania jedynie po uzyskaniu wyraźnej zgody użytkownika na konkretne cele reklamowe.

- RODO i nadzór: Nowe przepisy uzupełniają RODO i nadają organom ochrony danych osobowych (takim jak Prezes UODO) kompetencje do nadzoru nad przestrzeganiem zasad targetowania reklam politycznych.
- Dalsze działania:
  - Komisja Europejska opublikowała wstępne wytyczne dotyczące stosowania rozporządzenia,
  - Europejska Rada Ochrony Danych (EROD) planuje opracowanie dodatkowych wytycznych do 2025 r.,
  - W Polsce trwają prace nad ustawą wdrażającą rozporządzenie – prowadzone przez Ministerstwo Cyfryzacji, przy wsparciu Prezesa UODO.
- Źródła dodatkowe: Polecane są również:
  - Wytyczne EROD 05/2020 dotyczące zgody (RODO),
  - Wytyczne EROD 03/2022 o zwodniczych wzorcach projektowych na platformach społecznościowych.

Źródło: https://uodo.gov.pl/pl/138/3912

02 EROD i Komisja Europejska zatwierdzają wspólne wytyczne dot. DMA i RODO

- **Kontekst**: Europejska Rada Ochrony Danych (EROD) oraz Komisja Europejska po raz pierwszy wspólnie opracowały wytyczne dotyczące współdziałania aktu o rynkach cyfrowych (DMA) i ogólnego rozporządzenia o ochronie danych (RODO).
- **Cel wytycznych**: Ułatwienie spójnego stosowania DMA i RODO, zwiększenie pewności prawa dla dużych platform cyfrowych (tzw. strażników dostępu), użytkowników biznesowych oraz osób fizycznych.
- **Zakres wytycznych**: Wyjaśnienie, w jaki sposób strażnicy dostępu mogą zgodnie z przepisami łączyć lub wykorzystywać dane osobowe, w szczególności w kontekście:
  - zgody użytkowników na podstawie DMA i RODO,
  - dystrybucji aplikacji i sklepów stron trzecich,
  - przenoszenia danych,
  - dostępu do danych i interoperacyjności komunikatorów.
- **Rola i znaczenie**: DMA i RODO mają wzajemnie uzupełniające się cele – RODO chroni prawa jednostki i prywatność, a DMA wspiera uczciwość i konkurencyjność rynków cyfrowych.
- **Następne kroki**: Rozpoczęto konsultacje publiczne dotyczące treści wytycznych, które potrwają do 4 grudnia 2025 r. Ostateczna wersja zostanie opracowana po analizie zgłoszonych uwag.

Źródło: https://uodo.gov.pl/pl/185/3921

02 cd. EROD i Komisja Europejska zatwierdzają wspólne wytyczne dot. DMA i RODO

- Kolejne obszary współpracy: Trwają wspólne prace EROD i Komisji nad wytycznymi dotyczącymi współdziałania aktu o sztucznej inteligencji z przepisami RODO.
- Wydarzenie EROD nt. anonimizacji i pseudonimizacji: EROD zapowiedziała zorganizowanie spotkania online z interesariuszami jeszcze przed końcem 2024 r., aby zebrać opinie i wspierać prace związane z interpretacją danych osobowych zgodnie z wyrokiem TSUE.

Źródło: https://uodo.gov.pl/pl/185/3921

03 e-Doręczenia w administracji publicznej to fikcja

- **Kontekst**: Od 1 stycznia 2025 r. wszystkie organy administracji publicznej, w tym ZUS, mają obowiązek doręczania pism do profesjonalnych pełnomocników (adwokatów, radców prawnych, doradców podatkowych itp.) za pośrednictwem e-Doręczeń – zgodnie z ustawą z 18 listopada 2020 r. o doręczeniach elektronicznych.
- **Obecna praktyka**: Mimo ustawowego obowiązku, ZUS i inne organy administracji nadal często wysyłają pisma pocztą tradycyjną, ignorując elektroniczne adresy doręczeń pełnomocników.
- **Problem prawny**: Takie działanie jest sprzeczne z przepisami Kodeksu postępowania administracyjnego i ustawą o doręczeniach elektronicznych, co może skutkować nieskutecznym doręczeniem i brakiem ważności decyzji administracyjnych.
- **Argumentacja ZUS**: ZUS powołuje się na tzw. "przesłanki organizacyjne" oraz potrzebę oszczędności środków publicznych, twierdząc, że wysyłka tradycyjna jest tańsza niż e-Doręczenia (3,01 zł vs. 6,52 zł).
- **Reakcje prawników**: Eksperci wskazują, że tłumaczenia ZUS są niezgodne z obowiązującym prawem. Podkreślają, że to urzędy mają obowiązek stosowania e-Doręczeń, skoro nakładają ten obowiązek na profesjonalnych pełnomocników.
- **Potencjalne konsekwencje**: Błędne doręczenia mogą powodować problemy dla przedsiębiorców i pełnomocników – np. brak wiedzy o decyzjach urzędowych, utrata terminów, większe odsetki za zaległości podatkowe.
- **Problemy techniczne i praktyczne**: System e-Doręczeń nie jest w pełni zintegrowany z innymi portalami administracji (np. ePUAP, PUE ZUS, e-US), co powoduje dezorientację wśród pełnomocników posiadających po kilka kont.

Źródło: https://www.prawo.pl/kadry/e-doreczenia-praktyczne-problemy-w-korespondencji-z-administracja,535328.html

03 cd. e-Doręczenia w administracji publicznej to fikcja

- Stanowisko Ministerstwa Finansów: Resort potwierdza, że również organy podatkowe od początku 2025 r. mają obowiązek doręczania korespondencji przez e-Doręczenia, chyba że pełnomocnik wyrazi zgodę na doręczenia przez inne systemy.
- Głos ekspertów: Prawnicy i doradcy podatkowi zgodnie podkreślają, że wybiórcze stosowanie doręczeń elektronicznych przez ZUS narusza zasadę równości i przejrzystości cyfrowego państwa prawa.

Źródło: https://www.prawo.pl/kadry/e-doreczenia-praktyczne-problemy-w-korespondencji-z-administracja,535328.html

04 Wzmocnienie bezpieczeństwa Schengen i zapobieganie nieuregulowanej migracji

- **Kontekst**: Od 12 października 2024 r. w krajach strefy Schengen zostanie uruchomiony System Wjazdu/Wyjazdu (EES), którego celem jest poprawa zarządzania granicami, zwiększenie bezpieczeństwa i zapobieganie nielegalnej migracji.
- EES zastępuje dotychczasowe stemplowanie paszportów poprzez cyfrową rejestrację danych osób przekraczających granice zewnętrzne strefy Schengen.
- System będzie obejmował obywateli państw trzecich podróżujących na podstawie wiz krótkoterminowych lub zwolnionych z obowiązku wizowego.
- Dane rejestrowane przez EES:
  - Imię, nazwisko, data i miejsce urodzenia,
  - Data wjazdu, wyjazdu lub decyzji odmowy wjazdu,
  - Dane biometryczne – wizerunek twarzy i odciski palców.
- System będzie wdrażany stopniowo – początkowo obejmując 10% przejść granicznych, a pełne wdrożenie powinno nastąpić w ciągu 6 miesięcy.
- Ochrona danych osobowych odbywa się na podstawie unijnych przepisów:
  - **RODO** – dla organów granicznych i migracyjnych,
  - **DODO** – dla organów ścigania w kontekście zapobiegania przestępczości i terroryzmowi.
- Osoby, których dane są przetwarzane, mają prawo do:

Źródło: https://uodo.gov.pl/pl/138/3913

04 cd. Wzmocnienie bezpieczeństwa Schengen i zapobieganie nieuregulowanej migracji

  - dostępu do swoich danych,
  - sprostowania, uzupełnienia lub usunięcia danych,
  - ograniczenia przetwarzania danych.
- W Polsce nadzór nad przetwarzaniem danych osobowych w EES sprawuje Prezes Urzędu Ochrony Danych Osobowych (UODO).
- Na poziomie europejskim funkcjonuje mechanizm skoordynowanego nadzoru, obejmujący współpracę między organami krajowymi a Europejskim Inspektorem Ochrony Danych.
- Podstawa prawna działania EES:
  - Rozporządzenie (UE) 2017/2226,
  - Ustawa o udziale Polski w Systemie Wjazdu/Wyjazdu,
  - Rozporządzenie MSWiA ws. jednostek operacyjnych i dostępu do danych EES.
- Dodatkowe informacje można znaleźć na stronach: Urzędu Ochrony Danych Osobowych (UODO), Komendanta Głównego Straży Granicznej oraz Komisji Europejskiej.

Źródło: https://uodo.gov.pl/pl/138/3913

05 Sąd wymierzył karę 2000 zł za przetwarzanie danych bez uprawnienia

- **Kontekst sprawy**: Artykuł omawia wyrok w sprawie karnej dotyczącej niewłaściwego przetwarzania danych osobowych przez kosmetyczkę pracującą wcześniej na etacie, która wykorzystała dane klientów firmy do celów własnej, konkurencyjnej działalności gospodarczej.
- **Opis sytuacji**: Kosmetyczka, będąc zatrudniona w firmie, miała dostęp do danych klientów, w tym ich numerów telefonów i informacji zdrowotnych. Po złożeniu wypowiedzenia i założeniu własnej działalności, skopiowała te dane z firmowego systemu i przesłała je swojemu partnerowi.
- **Podstawa oskarżenia**: Prokurator zarzucił jej ujawnienie informacji stanowiących tajemnicę przedsiębiorstwa oraz nielegalne przetwarzanie danych osobowych, w tym danych wrażliwych (zdrowotnych), bez odpowiednich uprawnień.
- **Wyrok sądu**: W lipcu 2025 r. Sąd uznał ją winną usiłowania przestępstwa związanego z:
  - ujawnieniem informacji poufnych (art. 266 § 1 kk),
  - naruszeniem zasad uczciwej konkurencji (art. 23 ust. 1 ustawy o zwalczaniu nieuczciwej konkurencji),
  - nieuprawnionym przetwarzaniem danych osobowych (art. 107 ust. 2 ustawy o ochronie danych osobowych).
- **Orzeczona kara**: Grzywna w wysokości 100 stawek dziennych po 20 zł każda (łącznie 2000 zł).
- **Ustawowe podstawy odpowiedzialności**:
  - RODO definiuje dane osobowe jako wszelkie informacje pozwalające zidentyfikować osobę fizyczną, bezpośrednio lub pośrednio.
  - Polskie przepisy zabraniają przetwarzania danych osobowych przez osoby nieuprawnione lub w sposób niedozwolony.

Źródło: https://judykatura.pl/sad-wymierzyl-kare-2000-zl-za-przetwarzanie-danych-bez-uprawnienia/

05 cd. Sąd wymierzył karę 2000 zł za przetwarzanie danych bez uprawnienia

- Kontekst sprawy: Artykuł omawia wyrok w sprawie karnej dotyczącej niewłaściwego przetwarzania danych osobowych przez kosmetyczkę pracującą wcześniej na etacie, która wykorzystała dane klientów firmy do celów własnej, konkurencyjnej działalności gospodarczej.
- Ustalenia sądu:
  - Kosmetyczka złamała zobowiązanie do zachowania poufności danych klientów,
  - Przeniosła dane poza firmowy system, naruszając zasady ochrony danych,
  - Celem działania było przygotowanie gruntu pod własną, konkurencyjną działalność gospodarczą,
  - Czyn zakwalifikowano jako usiłowanie przestępstwa, ponieważ działalność jej firmy faktycznie nie została uruchomiona, a szkoda majątkowa nie powstała.

Źródło: https://judykatura.pl/sad-wymierzyl-kare-2000-zl-za-przetwarzanie-danych-bez-uprawnienia/

06 Szeroki nakaz przechowywania wszystkich czatów przez OpenAI uchylony

- **Kontekst**: Artykuł dotyczy uchylenia szerokiego nakazu przechowywania wszystkich czatów użytkowników przez firmę OpenAI — tematu, który wcześniej wywołał kontrowersje i obawy dotyczące prywatności danych.
- Sąd w Nowym Jorku uchylił nakaz przechowywania wszystkich czatów przez OpenAI – dotyczy to użytkowników z Unii Europejskiej, Szwajcarii i Wielkiej Brytanii.
- Decyzja ta jest efektem porozumienia zawartego pomiędzy stronami postępowania.
- OpenAI nadal ma obowiązek przechowywania wcześniej zebranych logów czatów — z wyjątkiem danych użytkowników z wymienionych regionów.
- W przyszłości firma musi przechowywać dane związane z konkretnymi domenami (m.in. agregatorami treści), wskazanymi w załączniku do decyzji sądu.
- Mimo złagodzenia przepisów, zachęca się użytkowników do zachowania ostrożności przy udostępnianiu poufnych informacji za pośrednictwem usług AI, takich jak ChatGPT.
- Zalecanym podejściem dla przetwarzania danych wrażliwych są lokalne rozwiązania AI (LLM on-prem), które działają całkowicie w ramach infrastruktury firmy, jak np. system Bielik.

Źródło: https://www.linkedin.com/posts/jakub-wyczik_nytimes-vs-openai-nowy-nakaz-przechowania-ugcPost-7384125015350231040-mKK8?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL_z0rPX_x8

07 ENISA Threat Landscape 2025 – kluczowe wnioski dla bezpieczeństwa cybernetycznego w Europie

- **Kontekst**: Europejska Agencja ds. Cyberbezpieczeństwa (ENISA) opublikowała raport Threat Landscape 2025, analizując trendy w cyberzagrożeniach między lipcem 2024 a czerwcem 2025 roku – raport oparto na analizie ok. 4 900 incydentów.
- **Phishing to nadal najczęstszy typ ataku** – stanowi 60% zagrożeń. Coraz częściej wykorzystywane są do niego usługi Phishing-as-a-Service oraz sztuczna inteligencja.
- **Ataki ransomware pozostają głównym zagrożeniem** w cyberprzestępczości – przestępcy decentralizują działania i stosują silniejsze techniki wymuszania okupu.
- **Sztuczna inteligencja (AI)** pełni podwójną rolę – jest używana w kampaniach ataków (ponad 80% kampanii phishingowych korzysta z modeli AI do personalizacji) oraz sama staje się celem ataków.
- **Hacktywiści odpowiadają za 80% incydentów** – najczęściej posługują się tanimi i łatwymi w użyciu atakami DDoS, motywowanymi ideologicznie.
- **Sektor publiczny (38%) najczęściej pada ofiarą cyberataków**, zwłaszcza ze strony grup prorosyjskich i proirańskich. Wysokie ryzyko dotyczy także sektorów: transportowego, cyfrowego, finansowego i produkcyjnego.
- **Zacieranie się granic między typami zagrożeń** – działania państwowe, przestępcze i hacktywistyczne stają się coraz trudniejsze do rozróżnienia.
- **Zależności cyfrowe i łańcuch dostaw** coraz częściej wykorzystywane są jako punkt wejścia – atak na jednego dostawcę może sparaliżować wiele organizacji.

Źródło: https://www.linkedin.com/posts/kamil-pszczolkowski_enisa-threat-landscape-2025-ugcPost-7382014238275383297-J062?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLlzLMFC01FENWMw0oL_z0rPX_x8

07 cd. ENISA Threat Landscape 2025 – kluczowe wnioski dla bezpieczeństwa cybernetycznego w Europie

- Główne zalecenia ENISA:
  - Wzmocnienie podstawowej higieny cybernetycznej (np. aktualizacje systemów, kontrola uprawnień, monitoring).
  - Rozwijanie odporności i zdolności reagowania na poziomie sektorów i krajów.
  - Stałe monitorowanie nadużyć związanych z AI i dezinformacją.
- Wniosek ogólny: W dobie automatyzacji i napięć geopolitycznych, cyberbezpieczeństwo staje się kluczowym elementem stabilności gospodarczej i politycznej w Europie.

Źródło: https://www.linkedin.com/posts/kamil-pszczolkowski_enisa-threat-landscape-2025-ugcPost-7382014238275383297-J062?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL_z0rPX_x8

08 Jawność pod kontrolą. Ministerstwo chce wiedzieć, kto zagląda do ksiąg wieczystych

- **Temat**: Ministerstwo Sprawiedliwości planuje zmiany w dostępie do ksiąg wieczystych. Celem jest zwiększenie ochrony danych osobowych i ograniczenie nieuprawnionego dostępu do rejestrów.
- **Koniec anonimowego przeglądania**: Wszyscy użytkownicy będą musieli potwierdzać swoją tożsamość, by przeglądać księgi wieczyste – zarówno stacjonarnie (okazując dowód osobisty), jak i online (logując się m.in. przez profil zaufany).
- **Rejestrowanie aktywności**: System będzie zapisywać, kto, kiedy i jaką księgę przeglądał. Dane te (w tym numer IP, PESEL, numer księgi, data i godzina) będą przechowywane przez 5 lat.
- **Cel zmian**: Resort wskazuje na konieczność ochrony danych wrażliwych, takich jak dane osobowe właścicieli nieruchomości oraz informacje o zadłużeniu czy adresie.
- **Walka z nielegalnymi portalami**: Projekt ma ograniczyć działalność portali kopiujących dane z ksiąg wieczystych i oferujących do nich płatny dostęp, często działających z zagranicy bez podstaw prawnych.
- **Ochrona przed masowym dostępem**: System ma uniemożliwiać automatyczne, masowe pobieranie danych przez boty, jednocześnie zachowując dostęp dla służb i uprawnionych użytkowników (np. sądów).
- **Dostęp organów państwowych**: Przechowywane dane mają być udostępniane m.in. sądom, prokuraturze, policji, ABW, CBA oraz innym służbom w związku z prowadzonymi postępowaniami.
- **Zastrzeżenia ekspertów**:

Źródło: https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/10494331,jawnosc-pod-kontrola-ministerstwo-chce-wiedziec-kto-zaglada-do-ksiag.html

08 cd. Jawność pod kontrolą. Ministerstwo chce wiedzieć, kto zagląda do ksiąg wieczystych

- Brak szczegółowych zapisów w ustawie – część kluczowych informacji ujawniono tylko w uzasadnieniu.
- Niejasne zasady blokowania dostępu i brak informacji o procedurze odwoławczej dla użytkownika.
- Wątpliwości co do zgodności z zasadą jawności ksiąg wieczystych i możliwością sprawdzenia, kto przeglądał konkretną księgę.

- Podsumowanie: Ministerstwo argumentuje, że nowe regulacje zwiększą bezpieczeństwo i zgodność z RODO. Krytycy obawiają się jednak ograniczenia jawności rejestrów oraz niedostatecznego doprecyzowania zasad w dokumentach legislacyjnych.

Źródło: https://serwisy.gazetaprawna.pl/orzeczenia/artykuly/10494331,jawnosc-pod-kontrola-ministerstwo-chce-wiedziec-kto-zaglada-do-ksiag.html

09 NSA podtrzymał decyzje Prezesa UODO dotyczące przetwarzania danych niedoszłych klientów banków

- Kontekst: Artykuł dotyczy zasad przetwarzania danych osobowych przez banki oraz Biuro Informacji Kredytowej (BIK) w sytuacji, gdy osoba złożyła wniosek kredytowy, ale nie podpisała umowy kredytowej.
- Orzeczenie NSA: Naczelny Sąd Administracyjny (sprawy III OSK 1552/22 i III OSK 1877/22) podtrzymał decyzje Prezesa Urzędu Ochrony Danych Osobowych (UODO), uznając, że dalsze przetwarzanie danych takich osób jest niezgodne z prawem.
- Kluczowy wniosek: Jeżeli nie doszło do zawarcia umowy kredytowej, instytucje finansowe nie mają podstaw prawnych do dalszego przechowywania ani przetwarzania danych wnioskodawcy.
- Argumenty banków i BIK: SKOK Stefczyka, Alior Bank i BIK powoływały się na przepisy Prawa bankowego i RODO twierdząc, że mają prawnie uzasadniony interes w zachowaniu danych w celach takich jak obrona przed ewentualnymi roszczeniami czy tworzenie modeli analitycznych.
- Stanowisko UODO i NSA:
  - Dane osobowe mogą być przetwarzane tylko na podstawie wyraźnego przepisu prawa.
  - Przy braku zawartej umowy kredytowej nie ma przesłanek do legalnego dalszego przetwarzania danych.
  - Przesłanka prawnie uzasadnionego interesu z art. 6 ust. 1 lit. f RODO nie może być stosowana „na zapas", bez konkretnego istniejącego celu.
- Znaczenie orzeczenia: NSA wyraźnie ograniczył możliwość wykorzystywania danych osobowych kandydatów na klientów banku, którzy ostatecznie nie podpisali umowy. Przetwarzanie danych w takich przypadkach – np. w celach analitycznych lub tworzenia modeli ryzyka kredytowego – nie jest dozwolone.

Źródło: https://uodo.gov.pl/pl/138/3926

09 cd. NSA podtrzymał decyzje Prezesa UODO dotyczące przetwarzania danych niedoszłych klientów banków

- Konsekwencje dla sektora finansowego: Instytucje finansowe muszą dostosować swoje procedury do wykładni prawa przyjętej przez NSA – dane niedoszłych klientów powinny być usuwane, jeżeli nie doszło do podpisania umowy.

Źródło: https://uodo.gov.pl/pl/138/3926

10 Raport ZFODO: Systematycznie rośnie liczba naruszeń powodowanych przez źródła zewnętrzne (w tym hakerów)

- Kontekst: Raport ZFODO analizuje incydenty związane z naruszeniem ochrony danych osobowych w 325 organizacjach z sektora publicznego i prywatnego w 2024 roku.
- Najważniejsze fakty i wnioski:
- W 2024 roku odnotowano 449 incydentów – to najwyższa średnia od początku raportów (1,38 incydentu na organizację).
- Tylko 37% incydentów zgłoszono do UODO, a 67% niezgłoszonych uznano za niskiego ryzyka.
- W 33% przypadków poinformowano osoby, których dane dotyczyły – w 67% zaniechano takiej informacji.
- Najbardziej narażone branże:
    - Handel i e-commerce – 25%
    - Finanse, ubezpieczenia, windykacja, nieruchomości – łącznie 23%
    - Przemysł i produkcja – 11%
    - Zdrowie i opieka społeczna – 5%
    - Transport – 4%
- Sektor prywatny odpowiada za większość incydentów ze względu na większą liczbę obsługiwanych podmiotów.

Źródło: https://www.zfodo.org.pl/typ/raporty/

10 cd. Raport ZFODO: Systematycznie rośnie liczba naruszeń powodowanych przez źródła zewnętrzne (w tym hakerów)

- Źródła naruszeń:
  - 60% – źródła wewnętrzne (głównie pracownicy)
  - 29% – źródła zewnętrzne (rosnący udział hakerów i byłych pracowników)
  - 11% – podmioty przetwarzające dane (spadek w porównaniu z 2023)
- 84% incydentów miało charakter nieumyślny – ludzkie błędy dominują.
- 82% przyczyn incydentów miało charakter osobowy, 18% – techniczny.
- Naruszane dane:
  - Dane podstawowe – 83%
  - Dane finansowe – 26%
  - Numery PESEL – 25%
  - Dane szczególnych kategorii – 12%
- Najwięcej incydentów występuje w II kwartale roku (kwiecień–czerwiec), ze wzmożoną aktywnością cyberprzestępców latem.
- 25% incydentów zgłoszono organom ścigania – to stosunkowo wysoki odsetek w kontekście potencjalnych przestępstw.

Źródło: https://www.zfodo.org.pl/typ/raporty/

10 cd. Raport ZFODO: Systematycznie rośnie liczba naruszeń powodowanych przez źródła zewnętrzne (w tym hakerów)

- Wnioski końcowe:
- Wzrost liczby incydentów wynika z rosnącej świadomości i nowych wytycznych, a nie z pogorszenia poziomu bezpieczeństwa.
- Czynnikiem o największym ryzyku pozostaje człowiek – błędy i zaniedbania pracowników.
- Rosną zagrożenia zewnętrzne, w szczególności cyberataki i phishing.
- Kluczowe są działania prewencyjne oraz szybka reakcja na incydenty – maksymalnie w ciągu 72 godzin.
- Coraz więcej organizacji decyduje się na outsourcing Inspektora Ochrony Danych (IOD), zamiast rozwijać własne kompetencje wewnętrzne.

Źródło: https://www.zfodo.org.pl/typ/raporty/

11 Cyberatak na F5: Skradziono kod źródłowy. Co to oznacza dla firm w Polsce?

- **Kontekst**: Firma F5, globalny dostawca technologii sieciowych i zabezpieczeń, padła ofiarą poważnego cyberataku, uznanego za zagrożenie dla bezpieczeństwa narodowego USA i potencjalnie tysięcy firm na świecie, w tym w Polsce.
- **Źródło ataku**: Atak przypisywany jest zaawansowanej grupie hakerskiej powiązanej z rządem Chin, określanej przez ekspertów jako UNC5221. Wykorzystano złośliwe oprogramowanie Brickstorm.
- **Skala ataku**: Hakerzy mieli dostęp do systemów F5 przez co najmniej rok (do sierpnia 2025 r.), co pozwoliło im na kradzież krytycznych danych, w tym kodu źródłowego produktu BIG-IP oraz informacji o lukach w zabezpieczeniach.
- **Wykradzione dane**:
  - Kod źródłowy systemu BIG-IP – używanego przez 85% firm z listy Fortune 500 i instytucje rządowe.
  - Informacje o nieujawnionych lukach w zabezpieczeniach.
  - Pliki zawierające dane konfiguracyjne części klientów.
- **Reakcja F5**:
  - Wdrożono pomoc zewnętrzną od firm Mandiant i CrowdStrike.
  - Wydano aktualizacje bezpieczeństwa i przewodnik dla klientów do wykrywania zagrożeń związanych z Brickstorm.
  - Rotacja kluczy kryptograficznych i certyfikatów podpisywania.

Źródło: https://www.securityweek.com/f5-hack-attack-linked-to-china-big-ip-flaws-patched-governments-issue-alerts/
https://itreseller.pl/cyberatak-na-f5-skradziono-kod-zrodlowy-co-to-oznacza-dla-firm-w-polsce/

11 cd. Cyberatak na F5: Skradziono kod źródłowy. Co to oznacza dla firm w Polsce?

- Zalecenia dla klientów:
  - Natychmiastowe zainstalowanie udostępnionych aktualizacji bezpieczeństwa.
  - Weryfikacja konfiguracji urządzeń BIG-IP.
  - Dla starszych urządzeń – odłączenie, jeśli nie są już wspierane.
- Zagrożenia wynikające z incydentu:
  - Możliwość opracowania nowych exploitów z wykorzystaniem przejętego kodu i wiedzy o lukach.
  - Ryzyko przejęcia pełnej kontroli nad systemami używanymi m.in. przez instytucje rządowe, infrastrukturę krytyczną i sektor finansowy na całym świecie, również w Polsce.
  - Możliwość eksfiltracji danych, poruszania się po sieci organizacji i przejmowania kont oraz danych uwierzytelniających.
- Ostrzeżenia agencji:
  - Amerykańska CISA wydała dyrektywę zobowiązującą rządowe organizacje do aktualizacji systemów do 31 października 2025 r.
  - Podobne ostrzeżenie wydało brytyjskie Narodowe Centrum Bezpieczeństwa Cybernetycznego (NCSC).
- Wnioski: Atak na F5 to jedno z najpoważniejszych naruszeń w sektorze technologii sieciowych. Skalę zagrożenia potęguje strategiczne znaczenie produktów F5 w infrastrukturze globalnej. Organizacje korzystające z rozwiązań F5 muszą podjąć natychmiastowe działania zabezpieczające.

Źródło: https://www.securityweek.com/f5-hack-attack-linked-to-china-big-ip-flaws-patched-governments-issue-alerts/
https://itreseller.pl/cyberatak-na-f5-skradziono-kod-zrodlowy-co-to-oznacza-dla-firm-w-polsce/