





# RODO - aktualności

Data publikacji: 04.07.2025

# 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

UODO nakłada karę w wysokości 66 500 PLN na Uniwersytecki Dziecięcy Szpital Kliniczny

02

Przełomowe orzeczenie NSA co do odpowiedzialności administratora za procesora

03

WSA: administrator może przetwarzać dane do prawomocnego zakończenia postępowania

04

NSA rozstrzygając kilka skarg kasacyjnych Prezesa UODO dokonał przełomowej interpretacji przepisów

05

Zasady przetwarzania danych w CEIDG wymagają doprecyzowania

06

Norwegia: kara upomnienia dla operatora strony internetowej korzystającego z Meta Pixel

07

Sejm przyjął projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa

08

Czy Afryka stworzy własne RODO?

09

Dania: każdy obywatel otrzyma prawo autorskie do własnego wizerunku, rysów twarzy i głosu

# 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



Razem z książką otrzymasz dostęp do aplikacji SODO z Modelowym RCP

# 01 UODO nakłada karę w wysokości 66 500 PLN na Uniwersytecki Dziecięcy Szpital Kliniczny

- Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył karę w wysokości 66 500 PLN na Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku. Decyzja ta była wynikiem incydentu naruszenia bezpieczeństwa systemów informatycznych placówki, który spowodował poważne zagrożenie dla danych osobowych pracowników.
- Powodem nałożenia kary był brak wdrożenia odpowiednich środków technicznych i organizacyjnych chroniących dane osobowe, co stanowi naruszenie przepisów RODO.
- Atak typu ransomware doprowadził do zablokowania systemów informatycznych szpitala i zagroził danym ok. 2000 pracowników – nieuprawnione osoby mogły mieć dostęp do ich danych.
- Dane pacjentów nie zostały naruszone – atak nie objął systemów przetwarzających te informacje.
- Szpital nieprawidłowo przeprowadził analizę ryzyka – skupił się na zagrożeniach dla instytucji, a nie na ochronie praw osób, których dane dotyczą.
- Brak wskazania konkretnych procesów przetwarzania danych i ich powiązania z zagrożeniami oraz oceną ryzyka.
- Dokumentacja dotycząca analizy ryzyka była niespójna, niejasna i nie zawierała konkretnych rozwiązań.
- Szpital powoływał się na audyt zgodny z ustawą o krajowym systemie cyberbezpieczeństwa, co nie spełnia wymogów ochrony danych osobowych według RODO.
- Nie wdrożono odpowiednich procedur dotyczących testów odtworzeniowych danych oraz zabezpieczeń kopii zapasowych, co utrudniło odzyskanie utraconych danych po incydencie.

Źródło: <https://uodo.gov.pl/pl/138/3803>

# 01 cd. UODO nakłada karę w wysokości 66 500 PLN na Uniwersytecki Dziecięcy Szpital Kliniczny

- Szpital nie prowadził regularnych testów skuteczności środków bezpieczeństwa, ich oceny ani udokumentowanej kontroli, co narusza obowiązek rozliczalności przewidziany w RODO.
- **Wniosek końcowy:** Kara finansowa wynika z systemowych zaniedbań w zakresie ochrony danych osobowych, w tym braku właściwej analizy ryzyka, nieskutecznego wdrażania środków bezpieczeństwa oraz niewypełnienia podstawowych obowiązków rozliczalności i przejrzystości wynikających z RODO.

Źródło: <https://uodo.gov.pl/pl/138/3803>

## 02 Przełomowe orzeczenie NSA co do odpowiedzialności administratora za procesora

- Naczelny Sąd Administracyjny (NSA) opublikował uzasadnienia wyroków związanych ze sprawami naruszeń przepisów RODO przez administratorów danych. Chodzi o przypadki, w których dane osobowe zostały pobrane z niezabezpieczonego serwera przez osoby nieuprawnione. Serwer obsługiwał podmiot przetwarzający, a odpowiedzialność próbowano przypisać administratorowi danych.
- **Odpowiedzialność administratora danych:** NSA uznał, że administrator danych osobowych ponosi pełną odpowiedzialność za działania podmiotu przetwarzającego, szczególnie gdy dochodzi do przetwarzania danych poza jurysdykcją państw UE – jak to miało miejsce w przypadku administratora współpracującego z podmiotem z Białorusi.
- **Charakter umowy o przetwarzanie danych:** Aby odpowiedzialność administratora mogła być ograniczona, umowa z podmiotem przetwarzającym musi być zawarta zgodnie z przepisami prawa UE lub prawa państwa członkowskiego oraz wiązać strony podlegające tym przepisom.
- **Obiektywna odpowiedzialność administratora:** Jeżeli podmiot przetwarzający nie podlega jurysdykcji UE, administrator danych ponosi odpowiedzialność obiektywną za wszelkie naruszenia przepisów RODO dokonane przez ten podmiot.
- **Wykładnia przepisów RODO:** NSA powołał się na art. 5 ust. 2 RODO, zgodnie z którym administrator odpowiada za przestrzeganie przepisów dotyczących ochrony danych – odpowiedzialność ta nie może być przerzucana na inny podmiot bez zapewnienia możliwości skutecznego jej wyegzekwowania.
- **Znaczenie dla orzeczeń sądów cywilnych:** NSA wypowiedział się również na temat skutków decyzji Prezesa UODO dla postępowań przed sądami cywilnymi – decyzje te mają charakter wiążący.
- **Postępowania przed UODO:** NSA wskazuje, że w sprawach naruszenia ochrony danych osobowych powinno być prowadzone jedno postępowanie obejmujące zarówno badanie naruszenia, jak i rozpatrzenie skarg od osób, których dane dotyczą.

Źródło: <https://judykatura.pl/przelomowe-orzeczenie-nsa-co-do-odpowiedzialnosci-ado-za-procesora/>

## 02 cd. Przełomowe orzeczenie NSA co do odpowiedzialności administratora za procesora

- **Status stron:** Osoby, których dane dotyczą, powinny mieć status strony w postępowaniach dotyczących kar pieniężnych dla administratorów danych.
- **Wniosek końcowy:** Administrator danych osobowych musi dochować szczególnej staranności przy powierzaniu przetwarzania danych osobowych, zwłaszcza jeśli współpracuje z podmiotami spoza UE. W przeciwnym razie ponosi pełną odpowiedzialność administracyjną za działania tych podmiotów, w tym za udostępnienie danych osobowych bez podstawy prawnej.

Źródło: <https://judykatura.pl/przelomowe-orzeczenie-nsa-co-do-odpowiedzialosci-ado-za-procesora/>

## 03 WSA: administrator może przetwarzać dane do prawomocnego zakończenia postępowania

- Sprawa dotyczyła przetwarzania danych osobowych w związku z wierzytelnością na kwotę 24,46 zł – jej cesję przeprowadziła spółka, z którą osoba fizyczna miała wcześniej umowę abonamentową.
- Prezes UODO w decyzji z lipca 2024 r. nakazał spółce usunięcie danych osobowych (imię, nazwisko, adres, PESEL, dowód osobisty, numer telefonu), uznając, że dalsze ich przechowywanie nie ma podstawy prawnej.
- Spółka twierdziła, że może nadal przetwarzać te dane na podstawie art. 74 ustawy o rachunkowości. Sąd uznał jednak, że termin przechowywania danych zgodnie z tą ustawą już upłynął – z dniem 1 stycznia 2022 r.
- WSA w Warszawie wyjaśnił ważną kwestię proceduralną: decyzja organu nadzorczego (UODO) musi zostać wykonana dopiero po jej uprawomocnieniu, a nie w trakcie trwania postępowania sądowego.
- Oznacza to, że administrator danych osobowych może nadal je przetwarzać do czasu, aż decyzja nakazująca ich usunięcie stanie się prawomocna.
- W praktyce podważa to częsty argument administratorów danych, którzy we wnioskach o wstrzymanie wykonania decyzji powołują się na art. 61 § 2 i § 3 ustawy ppsa (Prawo o postępowaniu przed sądami administracyjnymi).
- **Podsumowanie:**
- Sąd wyraźnie wskazał, że do momentu prawomocności decyzji UODO, administrator ma prawo przetwarzać dane.
- Podstawy przetwarzania danych muszą rzeczywiście istnieć – przepisy rachunkowe nie mogą być powoływane po upływie ich okresu stosowania.
- Orzeczenie to może mieć wpływ na sposób, w jaki administratorzy danych argumentują wnioski o wstrzymanie wykonania decyzji organu nadzorczego.

Źródło: <https://judykatura.pl/wsa-administrator-moze-przetwarzac-dane-do-prawomocnego-zakonczenia-postepowania/>

## 04 NSA rozstrzygając kilka skarg kasacyjnych Prezesa UODO dokonał przełomowej interpretacji przepisów

- Artykuł dotyczy sprawy naruszenia ochrony danych osobowych przez administratora danych i podmiot przetwarzający. Podmiot ten nieprawidłowo zabezpieczył serwery, co umożliwiło dostęp osób nieuprawnionych do tysięcy danych osobowych klientów. UODO nałożył na administratora karę ponad 1 mln zł. W odpowiedzi osoby, których dane zostały naruszone, złożyły setki indywidualnych skarg. W orzecznictwie pojawiły się rozbieżności, które zostały rozstrzygnięte przez Naczelną Sąd Administracyjny (NSA).
- NSA uznał, że w przypadku gdy jedna sytuacja doprowadziła do naruszenia danych wielu osób, należy traktować to jako jedną sprawę administracyjną.
- Wskazano, że PUODO powinien przeprowadzić jedno połączone postępowanie administracyjne, dotyczące zarówno naruszenia przepisów RODO, jak i indywidualnych skarg.
- Prowadzenie wielu odrębnych postępowań w sprawie jednego incydentu jest nieefektywne i może wypaczać ocenę skali oraz istotności naruszenia.
- NSA podkreślił, że osoby, których dane zostały naruszone, muszą uzyskać status stron postępowania i mieć zapewnione prawa procesowe.
- Wyjaśnienie obowiązków administratora danych (z art. 5 ust. 1 i art. 32 RODO) jest kluczowe dla oceny naruszeń przepisów wobec konkretnych osób.
- Wydanie jednej decyzji administracyjnej powinno obejmować zarówno ocenę naruszenia, jak i ustalenie odpowiedzialności oraz kary.
- NSA zaznaczył, że każda osoba, która nie brała udziału w postępowaniu głównym, a jej dane zostały naruszone, powinna mieć możliwość odwołania się od decyzji, zgodnie z art. 47 Karty Praw Podstawowych UE.
- Stwierdzono, że pomijanie poszkodowanych w głównym postępowaniu narusza europejskie standardy proceduralne.
- NSA nakazał ponowne rozpoznanie sprawy, połączenie wszystkich postępowań i wydanie jednej wspólnej decyzji administracyjnej.

Źródło: <https://judykatura.pl/nsa-konieczne-jest-wszczecie-i-przeprowadzenie-jednego-postepowania-w-sprawie-naruszenia-ochrony-danych-osobowych-oraz-indywidualnych-skarg/>

# 05 Zasady przetwarzania danych w CEIDG wymagają doprecyzowania

- Prezes UODO popiera upraszczanie przepisów dla przedsiębiorców, ale podkreśla konieczność doprecyzowania zasad dostępu do systemów teleinformatycznych.
- Wątpliwości budzi ogólne opisanie w projekcie ustawy zasad dostępu do danych w systemie PIP i ich publikacji.
- Brakuje jasności w kwestii przekazywania informacji między systemami PIP i Krajowej Administracji Skarbowej (KAS), zwłaszcza danych z wykazu podatników VAT.
- Projekt powinien precyzyjnie wskazywać role podmiotów, tryb przekazywania danych oraz odpowiedzialność za publikację danych.
- Niejasne jest, który administrator będzie sprawował kontrolę nad systemem oraz jak będzie kształtowana odpowiedzialność za przetwarzanie danych.
- Konieczne jest dokładne określenie celu i sposobu przetwarzania danych w rejestrze CEIDG.
- Zapisy w projekcie nie gwarantują faktycznego rozdzielenia baz danych, co budzi zastrzeżenia ze względu na przepisy RODO (motyw 31).
- Prezes UODO wskazuje na potrzebę przeprowadzenia testu prywatności i oceny skutków dla ochrony danych osobowych w procesie legislacyjnym.
- Nowe ryzyka związane z dostępnością danych w CEIDG to m.in. profilowanie, nadużycia wobec danych osób, które zawiesiły lub zakończyły działalność, oraz upublicznienie prywatnych adresów.
- Podkreślono znaczenie ochrony prywatności i wysokich standardów bezpieczeństwa przy wdrażaniu zmian w systemach IT..

Źródło: <https://uodo.gov.pl/pl/138/3797>

## 06 Norwegia: kara upomnienia dla operatora strony internetowej korzystającego z Meta Pixel

- Artykuł dotyczy decyzji norweskiego organu ochrony danych (Datatilsynet), który udzielił upomnienia firmie Norsk Helseinformatikk AS (NHI) – operatorowi największego norweskiego portalu z informacjami medycznymi – za niezgodne z przepisami RODO przetwarzanie danych wrażliwych za pośrednictwem narzędzia śledzącego Meta Pixel.
- NHI wykorzystywało piksel Meta (narzędzie Facebooka/Instagrama) na swojej stronie głównej i wielu podstronach, umożliwiając nielegalne gromadzenie danych o zachowaniach użytkowników.
- Zbierane dane obejmowały m.in. odwiedzane podstrony dotyczące konkretnych chorób, adresy IP, identyfikatory plików cookie oraz tzw. odciski palców urządzeń.
- Norweski organ uznał, że nawet pośrednia możliwość wywnioskowania stanu zdrowia danej osoby (np. poprzez odwiedzenie strony o depresji czy epilepsji) sprawia, że mamy do czynienia z danymi wrażliwymi zgodnie z art. 9 RODO.
- Argumenty NHI, że samo odwiedzenie strony nie oznacza ujawnienia stanu zdrowia, zostały odrzucone – powołano się na orzecznictwo Trybunału Sprawiedliwości UE, wskazujące na niski próg uznania danych za wrażliwe.
- Organ podkreślił również, że nie tylko bezpośrednie zbieranie danych, ale także możliwość ich połączenia z innymi informacjami w ekosystemie reklamowym (jak to robi Meta), rodzi obowiązki w zakresie ochrony danych.
- Analiza banera zgód na pliki cookie wykazała stosowanie praktyki typu "dark pattern" – design nakłaniał użytkowników do akceptowania zbędnych plików cookie.

Źródło: [https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121\\_darkpattern-gdpr-privacy-activity-7341354623607156736-ZPQz?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121_darkpattern-gdpr-privacy-activity-7341354623607156736-ZPQz?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL_z0rPX_x8); [https://www.edpb.europa.eu/news/national-news/2025/norwegian-sa-issues-one-administrative-fine-and-five-reprimands-unlawful\\_en](https://www.edpb.europa.eu/news/national-news/2025/norwegian-sa-issues-one-administrative-fine-and-five-reprimands-unlawful_en)

## 06 cd. Norwegia: kara upomnienia dla operatora strony internetowej korzystającego z Meta Pixel

- Polityka prywatności NHI zawierała fałszywe informacje, że żadne dane wrażliwe nie są przetwarzane, co oznacza, że użytkownicy nie byli w stanie wyrazić świadomej zgody.
- Decyzja Datatilsynet tworzy ważny precedens: już samo śledzenie aktywności użytkownika na stronach dotyczących zdrowia jest przetwarzaniem danych wrażliwych w rozumieniu RODO.

Źródło: [https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121\\_darkpattern-gdpr-privacy-activity-7341354623607156736-ZPQz?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLizLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/mateusz-kupiec-fip-cipp-e-cipm-289700121_darkpattern-gdpr-privacy-activity-7341354623607156736-ZPQz?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLizLMFC01FENWMw0oL_z0rPX_x8); [https://www.edpb.europa.eu/news/national-news/2025/norwegian-sa-issues-one-administrative-fine-and-five-reprimands-unlawful\\_en](https://www.edpb.europa.eu/news/national-news/2025/norwegian-sa-issues-one-administrative-fine-and-five-reprimands-unlawful_en)

# 07 Sejm przyjął projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa

- W zeszłym tygodniu Sejm przyjął projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa, opracowany przez Ministerstwo Cyfryzacji. Nowe przepisy mają na celu uporządkowanie zasad funkcjonowania systemu certyfikacji bezpieczeństwa cyfrowego w Polsce oraz dostosowanie ich do standardów unijnych.
- Celem ustawy jest organizacja krajowego systemu certyfikacji cyberbezpieczeństwa, w tym ustalenie procedur certyfikacji i nadzoru nad ich stosowaniem.
- Ministerstwo Cyfryzacji będzie sprawowało nadzór nad funkcjonowaniem rynku certyfikacji.
- Ustawa przewiduje automatyczne uznawanie certyfikatów cyberbezpieczeństwa w całej Unii Europejskiej – jeden certyfikat będzie działać we wszystkich krajach członkowskich UE.
- Certyfikacja pozostaje w pełni dobrowolna – firmy mogą, ale nie muszą się certyfikować.
- Poza unijnymi certyfikatami wprowadzone zostaną również Nowe Schematy Krajowe, m.in. dotyczące zarządzania cyberbezpieczeństwem i kwalifikacji specjalistów.
- Krajowe certyfikaty będą wydawane na okres od 2 do 5 lat.

Źródło: [https://www.linkedin.com/posts/maciej-kaczmarek\\_projekt-ustawy-o-cyberbezpiecze%C5%84stwie-ugcPost-7345350325542817792-TEgh?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/maciej-kaczmarek_projekt-ustawy-o-cyberbezpiecze%C5%84stwie-ugcPost-7345350325542817792-TEgh?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLzLMFC01FENWMw0oL_z0rPX_x8)

# 08 Czy Afryka stworzy własne RODO?

- Wraz z rozwojem cyfrowym, afrykańskie kraje zmierzają ku lepszemu ochronie danych osobowych. Mimo że większość z 54 państw Afryki posiada przepisy o ochronie danych, brakuje spójnych regulacji i wspólnych standardów, co utrudnia ochronę obywateli i działalność międzynarodowych firm.
- Obecnie 46 krajów afrykańskich ma przepisy o ochronie danych, z czego 39 posiada odrębne ustawy, a w 34 działają niezależne organy nadzorcze.
- Główne problemy to brak jednolitych zasad, niespójność przepisów oraz trudności w egzekwowaniu prawa, zwłaszcza w kontekście transgranicznym.
- Konwencja z Malabo miała stanowić podstawę harmonizacji regulacji, jednak została ratyfikowana tylko przez 15 państw i ma liczne luki (m.in. brak definicji podstawowych pojęć oraz zasad dotyczących naruszeń danych i transferów zagranicznych).
- Wzorem dla wielu reform stało się europejskie RODO – oferujące jasne zasady, obowiązki i silne mechanizmy egzekwowania prawa.
- Wdrożenie rozwiązań inspirowanych RODO w Afryce utrudniają jednak ograniczone zasoby instytucjonalne, brak stabilnego finansowania oraz niska edukacja cyfrowa.
- Dodatkowym wyzwaniem jest duża różnorodność kulturowa i inne – często kolektywne – podejście do pojęcia prywatności.
- Eksperci sugerują potrzebę aktualizacji Konwencji z Malabo, utworzenia instytucji dążącej do harmonizacji prawa, zwiększenia edukacji cyfrowej oraz finansowania nadzoru z kar nałożonych za naruszenia.
- Stworzenie wspólnego kontynentalnego systemu ochrony danych może zwiększyć bezpieczeństwo obywateli, przyciągnąć inwestycje i umocnić pozycję Afryki w globalnej gospodarce danych.

Źródło: [https://www.linkedin.com/posts/adam-szkur%C5%82at\\_rodoochronadanych-rodoo-activity-7345368306222034946-rmTD?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/adam-szkur%C5%82at_rodoochronadanych-rodoo-activity-7345368306222034946-rmTD?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL_z0rPX_x8)

## 08 cd. Czy Afryka stworzy własne RODO?

- **Wniosek:** Afryka stoi przed kluczową decyzją – czy i jak stworzyć spójny system ochrony danych inspirowany RODO, który uwzględni lokalne realia i potrzeby. Harmonizacja tych przepisów może być impulsem do rozwoju nie tylko prawa, ale i całej gospodarki cyfrowej kontynentu.

Źródło: [https://www.linkedin.com/posts/adam-szkur%C5%82at\\_rododochronadanych-rodod-activity-7345368306222034946-rmTD?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLizLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/adam-szkur%C5%82at_rododochronadanych-rodod-activity-7345368306222034946-rmTD?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLizLMFC01FENWMw0oL_z0rPX_x8)

# 09 Dania: każdy obywatel otrzyma prawo autorskie do własnego wizerunku, rysów twarzy i głosu

- W dobie rosnącej popularności technologii deepfake i wykorzystania sztucznej inteligencji do tworzenia realistycznych, fałszywych reprezentacji wyglądu lub głosu konkretnych osób, rządy zaczynają podejmować próby uregulowania tej przestrzeni. Duński rząd zapowiedział pierwszą w Europie nowelizację prawa autorskiego, która ma nadać obywatelom prawa autorskie do ich własnego wizerunku, głosu i rysów twarzy.
- **Nowe prawo autorskie w Danii:** Każdy obywatel będzie miał prawo autorskie do swojego wizerunku, rysów twarzy i głosu.
- **Definicja deepfake'a:** Treści generowane przez sztuczną inteligencję, realistycznie imitujące wygląd lub głos osoby, będą kwalifikowane jako deepfake.
- **Mechanizmy ochronne:** Obywatele zyskają prawo żądania usunięcia materiałów udostępnionych bez ich zgody na platformach internetowych.
- **Sankcje dla platform:** Firmy technologiczne, które nie usuwają zgłoszonych treści, będą podlegały odszkodowaniom i wysokim grzywnom.
- **Nowatorskie podejście:** Twarz i głos zostaną uznane nie tylko za dobra osobiste, ale jako elementy praw autorskich, podobne do dzieł twórczych.
- **Porównanie z Polską:** W Polsce wizerunek jest obecnie chroniony głównie przez prawo cywilne i dobra osobiste; nowelizacja duńska znacznie rozszerza tę ochronę.
- **Wątpliwości co do skuteczności:** Egzekwowanie przepisów ma opierać się na reakcji platform internetowych, co może być trudne, zwłaszcza w przypadku firm spoza UE.
- **Wartość inicjatywy:** Mimo ograniczeń, jest to pierwsza tego typu próba systemowego podejścia do złożonego i rosnącego problemu deepfake'ów.
- **Podsumowanie:** Duński projekt nowelizacji prawa autorskiego to przełomowy krok w kierunku ochrony tożsamości osobistej w erze cyfrowej. Chociaż skuteczność tych rozwiązań może być ograniczona praktycznym wykonaniem przez platformy internetowe, to inicjatywa ta stanowi początek ważnej dyskusji i działania na rzecz ochrony praw jednostki w obliczu nowych zagrożeń technologicznych.

Źródło: <https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence> ; [https://www.linkedin.com/posts/paula-skrzypecka\\_czy-ka%C5%BCdy-z-nas-ma-prawa-autorskie-do-swojego-activity-7345333396203569154-YOOD?utm\\_source=share&utm\\_medium=member\\_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL\\_z0rPX\\_x8](https://www.linkedin.com/posts/paula-skrzypecka_czy-ka%C5%BCdy-z-nas-ma-prawa-autorskie-do-swojego-activity-7345333396203569154-YOOD?utm_source=share&utm_medium=member_desktop&rcm=ACoAAETcUUUBLIzLMFC01FENWMw0oL_z0rPX_x8)

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,  
w szczególności rozpowszechniany i kopiowany.*