AURACO

NEWSLETTER

OCHRONA DANYCH • CYBERBEZPIECZEŃSTWO • REGULACJE

Kwiecień 2026 – Anonimizacja nagrań wideo – jak udostępniać monitoring bez naruszania praw osób trzecich

SPIS TREŚCI

01 Artykuł autorski
02 Przegląd newsów
03 Orzeczenia i decyzje
04 NIS2
05 AI Act
06 Kalendarz

ARTYKUŁ AUTORSKI

Tekst: **Łukasz Onysyk**

Anonimizacja nagrań wideo – jak udostępniać monitoring bez naruszania praw osób trzecich

Wyobraźmy sobie sytuację: pracownik składa wniosek o udostępnienie nagrania z kamery w magazynie. Twierdzi, że doszło do incydentu i potrzebuje dowodu. Na nagraniu – oprócz niego – widać dwanaście innych osób. Administrator ma miesiąc na odpowiedź. Co powinien zrobić?

To nie jest pytanie akademickie. W mojej praktyce IOD wnioski o udostępnienie nagrań z monitoringu wizyjnego pojawiają się coraz częściej – i coraz częściej dotyczą sytuacji, w których proste „tak" lub „nie" nie wystarczy. Prawo dostępu do danych gwarantuje wnioskodawcy kopię jego informacji. Jednocześnie na tym samym nagraniu znajdują się dane osobowe osób trzecich, których prawa administrator musi chronić z równą starannością.

Rozwiązaniem jest anonimizacja. Ale diabeł – jak zwykle – tkwi w szczegółach.

Prawo dostępu a nagrania z CCTV

Art. 15 RODO daje każdej osobie prawo do uzyskania kopii przetwarzanych danych osobowych. Wizerunek zarejestrowany przez kamerę monitoringu jest daną osobową – to potwierdziły zarówno wytyczne EDPB 3/2019 dotyczące przetwarzania danych przez urządzenia wideo, jak i konsekwentna linia orzecznicza polskich sądów administracyjnych.

Gdy ktoś żąda nagrania, na którym jest widoczny, administrator co do zasady musi je udostępnić. Odmowa jest dopuszczalna, ale wymaga solidnego uzasadnienia – samo powołanie się na „względy bezpieczeństwa" nie wystarczy.

Tu pojawia się art. 15 ust. 4 RODO: prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych osób. Na nagraniu z kamery w hali produkcyjnej, na parkingu czy w korytarzu biurowca zwykle widać więcej niż jedną osobę. Udostępnienie pełnego materiału bez żadnej obróbki oznaczałoby przekazanie wnioskodawcy danych osobowych (wizerunków, a niekiedy zachowań) osób, które o tym nie wiedzą i na to się nie godziły.

Anonimizacja jako jedyne wyjście

EDPB w wytycznych 3/2019 (pkt 94) wprost wskazuje, że jeżeli na nagraniu widoczne są osoby trzecie, administrator powinien zastosować środki techniczne – w szczególności maskowanie lub zamazywanie – zanim udostępni materiał wnioskodawcy. To nie jest rekomendacja. W sytuacji, gdy udostępnienie bez anonimizacji naruszyłoby prawa osób trzecich, jest to obowiązek wynikający z art. 15 ust. 4.

Warto zwrócić uwagę na pewien niuans: anonimizacja osób trzecich nie jest anonimizacją w rozumieniu motywu 26 RODO (czyli trwałym pozbawieniem danych charakteru osobowego). To raczej selektywne maskowanie – dane wnioskodawcy pozostają rozpoznawalne, a dane pozostałych osób stają się nieidentyfikowalne. Efekt: nagranie nadal stanowi dane osobowe wnioskodawcy, ale nie zawiera już danych osób postronnych.

Jak to się robi technicznie

Metod jest kilka i każda ma swoje ograniczenia.

Rozmycie twarzy (face blur) to najpopularniejsze podejście. Algorytm wykrywa twarze w kadrze i nakłada na nie filtr rozmywający. Działa dobrze przy nagraniach o przyzwoitej rozdzielczości, z frontalnym ujęciem i stabilnym oświetleniem. Problem pojawia się, gdy kamera jest daleko, osoba jest odwrócona tyłem albo nosi maseczkę – paradoksalnie, częściowe zakrycie twarzy utrudnia jej automatyczne wykrycie.

Maskowanie sylwetek (body masking) idzie dalej – zakrywa całą postać, nie tylko twarz. To bezpieczniejsze rozwiązanie, bo eliminuje ryzyko identyfikacji po ubiorze, postawie czy kontekście. Wymaga jednak bardziej zaawansowanych modeli detekcji i jest kosztowniejsze obliczeniowo.

Pixelizacja – technicznie prostsza od rozmycia, ale łatwiejsza do odwrócenia przy niskim poziomie mozaikowania. Badania opublikowane w ostatnich latach pokazują, że sieci neuronowe potrafią w pewnych warunkach odtworzyć twarz z pixelizowanego obrazu. Rozmycie gaussowskie jest w tym kontekście bezpieczniejsze.

Narzędzia AI nowej generacji oferują śledzenie obiektów w czasie rzeczywistym (object tracking) – raz oznaczona osoba jest maskowana na wszystkich klatkach, nawet gdy zmienia pozycję, wchodzi za przeszkodę i wraca. Ręczna obróbka minutowego nagrania z kilkoma osobami może zająć godzinę; automatyzacja skraca to do sekund. Nie oznacza to, że wynik nie wymaga kontroli – w ocenie naszego zespołu każde nagranie po automatycznej anonimizacji powinno przejść przegląd przez człowieka.

Kiedy anonimizacja nie wystarczy

Są sytuacje, w których nawet zaanonimizowane nagranie nie powinno zostać udostępnione.

Gdy kontekst pozwala na identyfikację – na przykład na nagraniu widać jedyną osobę w uniformie ochroniarza, a wnioskodawca wie, kto tego dnia pełnił dyżur. Zamazanie twarzy nic tu nie da. Podobnie z dźwiękiem: jeśli kamera rejestruje audio, sam głos może wystarczyć do rozpoznania osoby.

Gdy nagranie zawiera dane szczególnych kategorii osób trzecich – np. ujawnia stan zdrowia (ktoś upada, ma atak padaczki) albo przynależność do związku zawodowego (spotkanie w sali konferencyjnej z widocznym logo). Tu administrator powinien rozważyć, czy nawet częściowe udostępnienie jest proporcjonalne.

Odmowa udostępnienia musi być jednak wyjątkiem, nie regułą. PUODO konsekwentnie podkreśla, że ochrona praw osób trzecich nie może służyć jako pretekst do blokowania realizacji prawa dostępu. Jeśli da się zaanonimizować – trzeba to zrobić i udostępnić.

Monitoring w placówkach medycznych – sygnał od UODO

Plan kontroli sektorowych UODO na 2026 rok wymienia monitoring wizyjny w placówkach medycznych jako jeden z pięciu priorytetów. Szczególna uwaga ma dotyczyć przetwarzania danych dzieci – oddziały pediatryczne, poradnie. To kontekst, w którym anonimizacja nabiera dodatkowego wymiaru: nagranie z kamery na korytarzu szpitala dziecięcego to potencjalnie dane wrażliwe osób najbardziej bezbronnych.

Drugi priorytet z tego samego planu – anonimizacja nagrań z sesji rad gmin publikowanych w Biuletynie Informacji Publicznej. Samorządy muszą udostępniać nagrania, ale muszą też chronić dane osób na widowni czy petentów zabierających głos. To ten sam problem, tylko w innej skali.

Co zrobić, gdy wpłynie wniosek

Na szczególną uwagę zasługuje fakt, że większość problemów z udostępnianiem nagrań wynika nie z braku narzędzi technicznych, lecz z braku procedury. Administrator dostaje wniosek i nie wie, od czego zacząć.

Pierwszy krok to weryfikacja, czy nagranie w ogóle istnieje. Kamery mają typowo 14–30 dni retencji. Jeśli wniosek dotyczy zdarzenia sprzed dwóch miesięcy, odpowiedź jest prosta – danych już nie ma. Ale uwaga: art. 12 ust. 3 RODO daje miesiąc na odpowiedź, więc zwlekanie z obsługą wniosku może oznaczać, że nagranie zostanie nadpisane zanim ktokolwiek je obejrzy. W mojej ocenie – wniosek o nagranie powinien od razu uruchamiać zabezpieczenie materiału.

Dalej: identyfikacja wnioskodawcy na nagraniu. Trzeba ustalić, w jakim przedziale czasowym i na której kamerze wnioskodawca jest widoczny. Potem – ocena, czy na nagraniu są osoby trzecie i czy ich zamazanie jest technicznie wykonalne bez utraty sensu materiału.

Jeśli anonimizacja jest możliwa – wykonujemy ją i udostępniamy. Jeśli nie – odmawiamy z pisemnym uzasadnieniem, wskazując konkretnie, które prawa osób trzecich byłyby zagrożone (art. 15 ust. 4). Ogólnikowe „ze względu na prywatność innych osób" to za mało.

Całość dokumentujemy. PUODO przy kontroli zapyta nie tylko o wynik, ale o proces decyzyjny.

Dla organizacji, które nie dysponują własnym zapleczem technicznym do obróbki wideo, AURACO oferuje usługę anonimizacji nagrań CCTV – opartą na rozwiązaniu AI działającym w całości on-premises, bez przekazywania materiału poza infrastrukturę klienta.

Źródła

- EDPB, Wytyczne 3/2019 dotyczące przetwarzania danych osobowych przez urządzenia wideo, wersja 2.0 przyjęta 29.01.2020
- Plan kontroli sektorowych UODO na 2026 rok – uodo.gov.pl
- Wyrok NSA z 6.02.2026 r., sygn. III OSK 2014/24 – monitoring wizyjny dopuszczalny wyłącznie jako ostateczność (omówienie w wydaniu #2)
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO), art. 15, art. 12

PRZEGLĄD NEWSÓW

Przegląd najważniejszych wiadomości

Prezes UODO zawiadamia prokuraturę w sprawie deepfake'u nauczycielki (27.03.2026)

Prezes UODO Mirosław Wróblewski złożył zawiadomienie do prokuratury po tym, jak pod postem nauczycielki w mediach społecznościowych opublikowano jej zdjęcie przerobione za pomocą AI – przedstawiające ją nago. Prezes UODO uznał, że doszło do przetwarzania danych osobowych przez osobę nieuprawnioną, co może stanowić przestępstwo z art. 107 ust. 1 ustawy o ochronie danych osobowych (grzywna, ograniczenie wolności lub pozbawienie wolności do 2 lat). UODO podkreślił, że generowanie wizerunku ofiary w takim kontekście jest społecznie szkodliwe i wymaga reakcji organów ścigania. To pierwszy publicznie opisany przypadek, w którym PUODO bezpośrednio interweniuje w sprawie deepfake'u. Warto zwrócić uwagę, że zjawisko „rozbierania" zdjęć za pomocą AI narasta – i dotyczy nie tylko osób publicznych. Organizacje powinny uwzględnić ten rodzaj zagrożenia w szkoleniach z ochrony danych osobowych oraz w procedurach reagowania na incydenty.

Źródło: UODO

CEF 2026: EDPB uruchamia skoordynowaną akcję egzekucyjną ws. przejrzystości (19.03.2026)

Europejska Rada Ochrony Danych oficjalnie rozpoczęła tegoroczną skoordynowaną akcję egzekucyjną (Coordinated Enforcement Framework – CEF). Tematem przewodnim jest przejrzystość i realizacja obowiązków informacyjnych wynikających z art. 12, 13 i 14 RODO. W akcji uczestniczy 25 organów nadzorczych z całej Europy. Organy skontaktują się z wybranymi administratorami z różnych sektorów – część z nich może spodziewać się kontroli, część postępowań wyjaśniających. Wyniki zostaną przeanalizowane zbiorczo, a EDPB opublikuje raport – analogicznie do ubiegłorocznego raportu CEF dotyczącego prawa do usunięcia danych. W ocenie zespołu AURACO to dobry moment na przegląd własnych klauzul informacyjnych: na stronie internetowej, w formularzach rekrutacyjnych, w komunikacji marketingowej. Sprawdźcie, czy odzwierciedlają aktualny stan przetwarzania, a nie wersję sprzed trzech lat.

Źródło: EDPB

EDPB: prawnie uzasadniony interes w praktyce – 62 decyzje pod lupą (26.03.2026)

EDPB opublikował obszerny case digest poświęcony stosowaniu art. 6 ust. 1 lit. f RODO – przetwarzaniu opartemu na prawnie uzasadnionym interesie administratora. Opracowanie liczy 29 stron i analizuje 62 decyzje wydane w mechanizmie one-stop-shop oraz 5 wiążących decyzji samej Rady. Dokument systematyzuje test trzystopniowy: (1) czy interes jest wyraźny i zgodny z prawem, (2) czy przetwarzanie jest niezbędne do jego realizacji – a nie jedynie użyteczne, (3) czy zachowano proporcjonalną równowagę z prawami i wolnościami osób, których dane dotyczą. Organy nadzorcze akceptują szeroki zakres interesów – od antyfraudowych przez komercyjne po scoringowe – ale regularnie stwierdzają naruszenia tam, gdzie administrator nie przeprowadził uprzedniej oceny (Legitimate Interest Assessment), sformułował cel zbyt ogólnikowo albo nie rozważył mniej inwazyjnych alternatyw. Kluczowy wniosek: sam fakt posiadania uzasadnionego interesu nie zwalnia z przeprowadzenia pełnego testu – co bezpośrednio koresponduje z linią orzeczniczą NSA w sprawach monitoringu wizyjnego.

Źródło: EDPB

EDPB i EDPS: ostrożne poparcie dla europejskiego prawa biotechnologicznego (12.03.2026)

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych wydali wspólną opinię 3/2026 w sprawie projektu European Biotech Act. Oba organy poparły harmonizację zasad prowadzenia badań klinicznych na poziomie unijnym, lecz zgłosiły zastrzeżenia dotyczące ochrony danych zdrowotnych i genetycznych – czyli danych szczególnych kategorii w rozumieniu art. 9 RODO. Kluczowe rekomendacje: precyzyjne określenie ról administratorów i podmiotów przetwarzających w kontekście wieloośrodkowych badań klinicznych, ograniczenie proponowanego obowiązkowego 25-letniego okresu retencji wyłącznie do dokumentacji badania (a nie wszystkich zebranych danych osobowych) oraz jasne zdefiniowanie celów dalszego przetwarzania danych po zakończeniu badania. Opinia jest istotna dla sektora farmaceutycznego i medycznego, ale również dla IOD w szpitalach i ośrodkach badawczych, które uczestniczą w badaniach klinicznych.

Źródło: EDPB

ORZECZENIA I DECYZJE

Orzeczenia i decyzje – marzec 2026

Glovo (Restaurant Partner Polska) – 5,9 mln zł za wymaganie skanów dowodów tożsamości (16.03.2026)

- **Organ**: Prezes UODO
- **Podmiot**: Restaurant Partner Polska sp. z o.o. (operator platformy Glovo)
- **Sygnatura**: DKN.5112.33.2022
- **Kara/nakaz**: 5 898 064 zł + nakaz zaprzestania zbierania skanów dokumentów tożsamości i usunięcia zebranych danych w ciągu 30 dni
- **Istota**: Platforma Glovo wymagała od użytkowników przesyłania skanów lub zdjęć dowodów osobistych w ramach procedury weryfikacji tożsamości przy podejrzeniu oszustwa na koncie. Prezes UODO Mirosław Wróblewski uznał, że zakres zbieranych danych – pełny skan dokumentu zawierający numer PESEL, zdjęcie, datę urodzenia, adres zameldowania – był rażąco nadmiarowy w stosunku do deklarowanego celu. Weryfikacja tożsamości mogła zostać przeprowadzona mniej inwazyjnymi metodami, np. przez porównanie danych podanych przy rejestracji. Naruszono zasadę minimalizacji danych (art. 5 ust. 1 lit. c RODO).
- **Znaczenie dla praktyki**: Decyzja potwierdza, że zbieranie kopii dokumentów tożsamości „na wszelki wypadek" – nawet przy uzasadnionym celu antyfraudowym – jest nadmiarowe w rozumieniu art. 5 ust. 1 lit. c RODO. Warto na tej podstawie przejrzeć własne procedury weryfikacji tożsamości i ocenić, czy zakres zbieranych danych rzeczywiście odpowiada celowi przetwarzania. Jeżeli weryfikację da się przeprowadzić bez pełnego skanu dokumentu, należy wybrać mniej inwazyjną metodę. Decyzja jest nieprawomocna.

Źródło: UODO

WSA uchyla karę 27 mln zł dla Poczty Polskiej za wybory kopertowe (5.03.2026)

- **Organ**: Wojewódzki Sąd Administracyjny w Warszawie
- **Sygnatura**: II SA/Wa 837/25
- **Istota**: WSA uchylił najwyższą w historii karę nałożoną przez PUODO – 27 mln zł za przetwarzanie danych ok. 30 mln obywateli w związku z przygotowaniami do wyborów korespondencyjnych w maju 2020 r. Poczta Polska pozyskała dane z rejestru PESEL na podstawie decyzji Prezesa Rady Ministrów, bez odrębnej podstawy ustawowej w ówcześnie obowiązujących przepisach. PUODO uznał to za naruszenie art. 6 RODO – brak legalnej podstawy przetwarzania. Sąd przyjął jednak inną linię argumentacji: decyzja administracyjna premiera korzystała z domniemania legalności, a Poczta Polska jako adresat tej decyzji nie mogła samodzielnie oceniać jej zgodności z prawem.
- **Znaczenie dla praktyki**: Wyrok nie oznacza, że przetwarzanie było legalne – sąd orzekł jedynie, że Poczta Polska nie ponosi odpowiedzialności za wykonanie wiążącej decyzji organu władzy publicznej. Rozstrzygnięcie jest nieprawomocne; PUODO może złożyć skargę kasacyjną do NSA. Niezależnie od wyniku, sprawa ilustruje fundamentalny problem: co ma zrobić administrator, gdy polecenie organu publicznego budzi wątpliwości co do zgodności z RODO? Zdaniem sądu administrator powinien polecenie wykonać, a odpowiedzialność za jego legalność spoczywa na autorze decyzji.

Źródło: UODO

TSUE C-526/24 Brillen Rottler – nawet pierwsze żądanie dostępu może być nadużyciem prawa (19.03.2026)

- **Organ**: Trybunał Sprawiedliwości Unii Europejskiej
- **Sygnatura**: C-526/24 (Brillen Rottler)
- **Istota**: Trybunał orzekł, że administrator może odmówić realizacji żądania dostępu do danych (art. 15 RODO) nawet wówczas, gdy jest to pierwsze żądanie osoby, której dane dotyczą – jeśli wykaże, że celem żądania nie było uzyskanie informacji o przetwarzaniu, lecz nadużycie prawa. Sprawa dotyczyła zjawiska określanego jako „GDPR hopping": osoby celowo rejestrują się w usłudze, natychmiast składają wniosek o dostęp do danych, a następnie żądają odszkodowania za rzekome uchybienia w odpowiedzi administratora. TSUE potwierdził, że art. 12 ust. 5 RODO pozwala na odmowę realizacji żądań „ewidentnie nieuzasadnionych", ale ciężar dowodu spoczywa na administratorze. Jednocześnie Trybunał wskazał, że art. 82 ust. 1 RODO przyznaje prawo do odszkodowania za naruszenie prawa dostępu, nawet jeśli samo naruszenie nie stanowi „przetwarzania" w ścisłym znaczeniu.
- **Znaczenie dla praktyki**: Wyrok daje administratorom narzędzie obrony przed nadużyciami, ale wymaga ostrożności. Odmowa realizacji żądania DSAR zawsze wiąże się z ryzykiem – w razie sporu to administrator musi udowodnić, że żądanie było abuzywne. Warto zatem traktować możliwość odmowy jako wyjątek od zasady, nie jako nową regułę. Zespół AURACO zwraca uwagę, że wyrok nie powinien służyć jako pretekst do rutynowego kwestionowania żądań dostępu.

Źródło: TSUE, C-526/24

NSA podtrzymał karę 545 tys. zł dla Santander Bank Polska (6.03.2026)

- **Organ**: Naczelny Sąd Administracyjny (wyrok oddalający skargę kasacyjną); decyzja Prezesa UODO
- **Podmiot**: Santander Bank Polska S.A.
- **Sygnatura decyzji UODO**: DKN.5131.33.2021
- **Kara/nakaz**: 545 748 zł + nakaz niezwłocznego powiadomienia poszkodowanych pracowników
- **Istota**: Byłemu pracownikowi banku nie odebrano dostępu do Platformy Usług Elektronicznych ZUS. Przez osiem miesięcy po rozwiązaniu umowy o pracę logował się do systemu pięciokrotnie, uzyskując dostęp do danych osobowych innych pracowników – w tym numerów PESEL i informacji zdrowotnych. Bank zamieścił na wewnętrznej platformie jedynie ogólny komunikat przypominający o zasadach ochrony danych, nie informując poszkodowanych pracowników o faktycznym incydencie. Prezes UODO uznał, że naruszono art. 34 ust. 1 RODO – obowiązek powiadomienia osób, których dane dotyczą, o naruszeniu mogącym powodować wysokie ryzyko dla ich praw i wolności. NSA podkreślił, że dla zastosowania art. 34 RODO istotne jest samo wystąpienie ryzyka naruszenia praw osób, a nie to, czy nieuprawniona osoba faktycznie skorzystała z uzyskanych danych.
- **Znaczenie dla praktyki**: Warto na tej podstawie zweryfikować procedury offboardingu pracowników. Odbieranie dostępów do platform zewnętrznych (ZUS, systemy księgowe, usługi chmurowe) powinno następować w dniu rozwiązania umowy, a nie „przy najbliższej okazji". Wyrok potwierdza też, że ogólnikowy komunikat wewnętrzny nie zastąpi indywidualnego powiadomienia o naruszeniu wymaganego przez art. 34 RODO.

Źródło: UODO

Podsumowanie trendów

- **Minimalizacja danych to nie slogan.** Kara Glovo potwierdza, że zbieranie dokumentów tożsamości w formie skanów „na wszelki wypadek" jest nadmiarowe, nawet gdy administrator tłumaczy to ochroną przed oszustwami.
- **Domniemanie legalności decyzji administracyjnych.** Wyrok WSA w sprawie Poczty Polskiej tworzy precedens: wykonawca polecenia organu władzy publicznej może nie ponosić odpowiedzialności za jego niezgodność z RODO. Sprawa trafi zapewne do NSA.
- **Prawo dostępu nie jest bezwarunkowe.** Wyrok TSUE Brillen Rottler daje administratorom narzędzie wobec nadużyć, ale ciężar dowodu pozostaje po ich stronie. Odmowa realizacji żądania DSAR powinna być traktowana jako ostateczność, nie jako punkt wyjścia.
- **Offboarding to nie formalność.** NSA potwierdził karę dla Santander za niedostateczne powiadomienie o naruszeniu. Brak odebrania dostępu do ZUS po odejściu pracownika to błąd organizacyjny, ale ogólnikowy komunikat zamiast indywidualnego powiadomienia – to już naruszenie art. 34 RODO.

NIS2

NIS2 – co nowego

Ustawa o KSC wchodzi w życie – 2 kwietnia 2026

2 kwietnia 2026 r. weszła w życie znowelizowana ustawa o krajowym systemie cyberbezpieczeństwa. Opublikowana w Dzienniku Ustaw 2 marca, po miesięcznym vacatio legis stała się częścią polskiego porządku prawnego. Polska – z ponad rocznym opóźnieniem – dołącza do grupy państw, które transponowały dyrektywę NIS2.

Co to oznacza w praktyce? Obowiązki nie spadają na organizacje z dnia na dzień. Ustawa przewiduje **12 miesięcy na pełne dostosowanie** (do 2 kwietnia 2027 r.), ale pierwsze 6 miesięcy to okres samoidentyfikacji i rejestracji. Każda organizacja spełniająca kryteria – sektor z załączników I lub II dyrektywy, powyżej 50 pracowników lub obrót/suma bilansowa ponad 10 mln EUR – powinna do **2 października 2026 r.** ustalić, czy jest podmiotem kluczowym czy ważnym, i zgłosić się do właściwego CSIRT.

Trzy priorytety na najbliższe tygodnie:

Klasyfikacja. Pierwszym krokiem jest ustalenie, czy organizacja jest podmiotem kluczowym czy ważnym. Od tego zależy zakres obowiązków, wysokość potencjalnych kar i intensywność nadzoru. Podmioty kluczowe podlegają nadzorowi proaktywnemu (kontrole planowe), a podmioty ważne – reaktywnemu (po incydencie). Warto pamiętać, że dostawcy DNS, rejestry TLD i usługi zaufania podlegają przepisom niezależnie od wielkości.

Analiza luk. Art. 21 NIS2 wymienia konkretne obszary, które organizacja musi zabezpieczyć: polityki bezpieczeństwa, obsługę incydentów, ciągłość działania, bezpieczeństwo łańcucha dostaw, szkolenia, kryptografię, kontrolę dostępu, zarządzanie aktywami i uwierzytelnianie wieloskładnikowe. Organizacje z wdrożonym ISO 27001 mają solidną bazę, ale NIS2 w kilku miejscach idzie dalej – szczególnie w zakresie łańcucha dostaw i odpowiedzialności zarządu.

Procedury zgłaszania incydentów. Ustawa przewiduje 24 godziny na wczesne ostrzeżenie, 72 godziny na zgłoszenie formalne i miesiąc na raport końcowy. Warto sprawdzić, czy procedury organizacji zadziałają również poza godzinami pracy.

Wniosek Prezydenta do Trybunału Konstytucyjnego (kontrola następcza) nadal jest w toku – termin rozprawy nieznany. Przepisy obowiązują do momentu ewentualnego uchylenia.

EDPB i EDPS wspierają reformę cyberbezpieczeństwa – z zastrzeżeniami (18.03.2026)

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych wydali wspólną opinię dotyczącą dwóch powiązanych inicjatyw: Cybersecurity Act 2 (CSA2) oraz proponowanych zmian w dyrektywie NIS2. Oba organy poparły trzy kluczowe elementy: wzmocnienie operacyjnej roli ENISA, ułatwienie wzajemnego uznawania certyfikatów cyberbezpieczeństwa między państwami członkowskimi oraz – co najistotniejsze dla organizacji podlegających wielu reżimom – ustanowienie jednego punktu zgłaszania incydentów (single-entry point).

Ten ostatni postulat ma realne znaczenie. Dziś organizacja, która doświadczy incydentu naruszającego jednocześnie przepisy NIS2, RODO i DORA, musi zgłaszać go do kilku organów w różnych terminach i formatach. Jeden punkt wejścia i harmonizacja wymogów raportowania to krok w dobrym kierunku – choć od opinii do prawa droga jeszcze daleka.

Źródło: EDPB

Atak na Narodowe Centrum Badań Jądrowych w Świerku (12.03.2026)

NCBJ potwierdziło wykrycie i zablokowanie próby włamania do infrastruktury IT ośrodka w Świerku. Dyrektor prof. Jakub Kupecki zapewnił, że reaktor badawczy MARIA nie został narażony i działał normalnie. Wstępne ślady wskazywały na Iran, ale Minister Cyfryzacji Krzysztof Gawkowski poinformował 18 marca, że trop irański został wykluczony – dowody wskazują na rosyjskich hakerów. Początkowe wskaźniki mogły stanowić celową dezinformację.

Incydent ilustruje, dlaczego NIS2 obejmuje sektor badawczy. Infrastruktura naukowa – szczególnie jądrowa – jest celem ataków o motywacji geopolitycznej. Nawet skuteczne odparte próby włamania powinny być traktowane jako sygnał do weryfikacji procedur: segmentacji sieci, monitoringu anomalii i gotowości zespołów SOC do reagowania na zaawansowane zagrożenia (APT).

Źródło: BleepingComputer

AI ACT

AI Act – aktualności

Rada Ministrów przyjęła projekt ustawy o systemach sztucznej inteligencji (31.03.2026)

Dzień przed wejściem w życie ustawy o KSC Rada Ministrów przyjęła kolejny akt regulacyjny o dużym ciężarze gatunkowym – projekt ustawy o systemach sztucznej inteligencji (nr UC71). Wnioskodawcą jest Minister Cyfryzacji Krzysztof Gawkowski. Projekt trafia teraz do Sejmu.

Ustawa wdraża w polskim prawie rozporządzenie 2024/1689 (AI Act) i tworzy krajowe ramy nadzoru, sankcji oraz wsparcia dla innowacji. Trzy elementy wymagają bliższego omówienia.

KRiBSI – nowy organ nadzoru AI

Polska zdecydowała się na utworzenie jednego centralnego organu nadzoru rynku AI: **Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji** (KRiBSI). To wybór rzadki w skali Unii – jedynie Litwa przyjęła podobny model z jednym regulatorem. Polska jest przy tym jedynym krajem tworzącym w tym celu całkowicie nową instytucję.

Skład Komisji: - Przewodniczący – powoływany przez Sejm za zgodą Senatu, kadencja 5 lat, wyłaniany w drodze otwartego konkursu ogłoszonego przez Prezesa Rady Ministrów - Dwóch zastępców przewodniczącego - Przedstawiciele: UOKiK, UKE, KNF, KRRiT

Prezes UODO nie wchodzi w skład Komisji, ale projekt przyznaje mu rozszerzone kompetencje nadzorcze nad systemami AI stosowanymi w ściganiu przestępstw, kontroli granic, wymiarze sprawiedliwości i procesach demokratycznych (pkt 6, 7 i 8 załącznika III rozporządzenia 2024/1689). UODO pełni rolę organu współpracującego z KRiBSI w tym zakresie.

Kompetencje KRiBSI obejmują: nadzór rynku AI, prowadzenie postępowań administracyjnych, nakładanie sankcji, wycofywanie z rynku systemów niezgodnych z przepisami, prowadzenie piaskownic regulacyjnych oraz – co interesujące – wydawanie wiążących opinii indywidualnych. Ta ostatnia instytucja ma dawać firmom pewność prawną co do zgodności ich systemu AI z regulacjami, zanim wdrożą go na rynek.

Przy KRiBSI powstanie również **Społeczna Rada ds. Sztucznej Inteligencji** – organ doradczy liczący 9–15 członków wyłonionych spośród kandydatów zgłoszonych przez RPO, izby gospodarcze, związki zawodowe, środowisko akademickie i organizacje pozarządowe. Opinie Rady będą niewiążące, ale publicznie dostępne.

Spór o niezależność – i kompromis

Droga do obecnego kształtu KRiBSI nie była prosta. We wrześniu 2025 r. Ministerstwo Cyfryzacji proponowało w pełni niezależną agencję z odrębną osobowością prawną i budżetem rzędu 105 mln EUR na dekadę. W grudniu 2025 r. resort opublikował dwie konkurujące wersje legislacyjne. Kompromis zatwierdzony przez Komitet Stały Rady Ministrów w lutym 2026 r. zakłada, że KRiBSI działa jako niezależna jednostka, ale jej obsługa operacyjna jest osadzona w strukturze Ministerstwa Cyfryzacji.

Eksperci (m.in. Interface EU, Oxford Blavatnik School) zwracają uwagę, że takie rozwiązanie rodzi pytania o faktyczną niezależność – ten sam resort, który kształtuje politykę AI, zapewnia zaplecze organizacyjne dla organu nadzorującego jej wdrożenie. Wiceminister Dariusz Standerski odpowiada, że to model pragmatyczny, pozwalający zaoszczędzić ok. 23 mln zł rocznie na kosztach administracyjnych.

Kadry: start z ok. 30 pracownikami w 2026 r., docelowo ok. 70–80 ekspertów. Budżet operacyjny ma być niższy niż pierwotna propozycja z września 2025 r. (która zakładała ok. 105 mln EUR na dekadę i 100 etatów) – kompromis z lutego 2026 r. ograniczył koszty dzięki osadzeniu obsługi operacyjnej w MC.

Sankcje

System kar jest odzwierciedleniem unijnych progów: - Naruszenia zakazanych praktyk AI (manipulacja zachowaniem, social scoring, eksploatacja podatności grup wrażliwych): do **35 mln EUR** lub **7% globalnego rocznego obrotu** – obowiązują od 2 sierpnia 2025 r. - Pozostałe naruszenia: do **15 mln EUR** lub **3% obrotu** – od 2 sierpnia 2026 r. - Utrudnianie kontroli: grzywna do **500 tys. zł**, ograniczenie wolności lub pozbawienie wolności do 2 lat - Odwołania: do Sądu Okręgowego w Warszawie (Wydział Ochrony Konkurencji i Konsumentów)

Ustawa przewiduje też „ulgową politykę" – firmy, które szybko usuną stwierdzone naruszenia, mogą liczyć na obniżoną karę. Szczegóły mechanizmu zostaną doprecyzowane w toku prac parlamentarnych.

Piaskownica regulacyjna AI

Projekt zobowiązuje do uruchomienia piaskownic regulacyjnych (AI regulatory sandbox) do **2 sierpnia 2026 r.** To kontrolowane środowisko, w którym firmy – szczególnie startupy i MŚP – będą mogły testować innowacyjne systemy AI pod nadzorem KRiBSI, zanim wprowadzą je na rynek. Prowadzeniem piaskownic zajmie się Komisja.

Wytyczne do art. 6 AI Act – Komisja wciąż się spóźnia

2 lutego 2026 r. upłynął termin publikacji wytycznych Komisji Europejskiej dotyczących klasyfikacji systemów AI jako systemów wysokiego ryzyka (art. 6). Na początku kwietnia finalna wersja nadal nie jest dostępna. Komisja „integruje feedback" z konsultacji publicznych. To nie jedyne opóźnienie – organizacje standaryzacyjne CEN i CENELEC przesunęły termin opracowania norm technicznych na koniec 2026 r.

Brak wytycznych nie zwalnia z przygotowań. Rozporządzenie stosuje się bezpośrednio, a art. 6 jest wystarczająco precyzyjny, by przeprowadzić wewnętrzną ocenę – czy system AI wykorzystywany w organizacji mieści się w jednej z kategorii załącznika III. Nasz zespół zaleca przeprowadzenie tej inwentaryzacji teraz, nie czekając na wytyczne.

Digital Omnibus – Komisja proponuje przesunięcie terminów

Wspólna opinia EDPB/EDPS 1/2026 potwierdziła, że Komisja rozważa przesunięcie kluczowych terminów stosowania AI Act: systemy Annex III (biometria, infrastruktura krytyczna, edukacja, zatrudnienie, egzekwowanie prawa) z **2 sierpnia 2026** na najwcześniej **2 grudnia 2027**, systemy Annex I z 2 sierpnia 2027 na 2 sierpnia 2028. EDPB i EDPS nie sprzeciwiają się odroczeniu, ale ostrzegają przed usunięciem obowiązku rejestracji systemów, których dostawcy samodzielnie uznali za niebędące systemami wysokiego ryzyka.

Przesunięcie – jeśli zostanie uchwalone – daje organizacjom więcej czasu, ale nie zmienia kierunku. Każdy miesiąc przygotowań, który zostanie „zaoszczędzony" na odwlekaniu, będzie trzeba nadrobić pod większą presją.

Egzekwowanie GPAI – 2 sierpnia 2026

Kodeks praktyk dla dostawców modeli GPAI (opublikowany 10 lipca 2025 r.) to domyślna ścieżka wykazywania zgodności z AI Act. Od **2 sierpnia 2026 r.** Komisja Europejska zyskuje pełne uprawnienia egzekucyjne wobec dostawców modeli ogólnego przeznaczenia – audyty, dochodzenia, kary do 15 mln EUR lub 3% globalnego obrotu. Organizacje korzystające z modeli GPAI (GPT, Claude, Gemini i inne) powinny sprawdzić, czy ich dostawca jest sygnatariuszem Kodeksu – i jakie wynikają z tego zobowiązania umowne.

Źródło: gov.pl – Ministerstwo Cyfryzacji | CyberDefence24 | EDPB – opinia 1/2026

KALENDARZ

Kalendarz

Data	Wydarzenie	Kategoria
2026-04-02	Wejście w życie znowelizowanej ustawy o KSC (transpozycja NIS2)	NIS2
2026-04-09	Security Masters Summit 2026	Cyberbezpieczeństwo
2026-04-12	Zamknięcie naboru wystąpień na IAPP Europe Congress 2026 (Bruksela, 18–19.11.2026)	RODO / AI
2026-04-21/23	CYBERUK 2026 – Glasgow	Cyberbezpieczeństwo
kwiecień 2026	IN.SE.CON 2026 – International Cybersecurity Congress	Cyberbezpieczeństwo
kwiecień 2026	Planowana publikacja wytycznych KE do art. 6 AI Act (przesuwana z lutego)	AI Act
2026-05-20	CyberGov Conference 2026 – Warszawa	Cyberbezpieczeństwo / sektor publiczny
2026-05-25/26	CONFidence 2026 – Kraków	Cyberbezpieczeństwo
2026-05-26/29	CyCon 2026 „Securing Tomorrow" – Tallinn, Estonia	Cyberbezpieczeństwo
2026-06-01/04	IAPP AI Governance Global Europe 2026 – Dublin	AI / RODO
2026-06-02/04	Infosecurity Europe 2026 – Londyn	Cyberbezpieczeństwo
2026-08-02	Pełne stosowanie AI Act – systemy high-risk Annex III (chyba że Digital Omnibus przesunie na XII 2027)	AI Act
2026-08-02	Pełne uprawnienia egzekucyjne KE wobec dostawców modeli GPAI	AI Act
do 2026-10-02	Koniec 6-miesięcznego okresu samoidentyfikacji podmiotów kluczowych/ważnych (KSC/NIS2)	NIS2

Na co zwrócić uwagę w tym wydaniu

1. **Ustawa o KSC obowiązuje od 2 kwietnia 2026 r.** Okres vacatio legis d