RODO Aktualności

Data publikacji: 20.10.2026

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.

Spis treści

1. Istota testu prywatności. Eksperci UODO na Warsztatach Legislacyjnych
2. Czy DSA może pomóc zapobiegać atakom w szkołach?
3. Fiński Organ Ochrony Danych uznał, że szkolne dane służą tylko nauczaniu
4. Hiszpański Sąd Krajowy zawiesił ogólny nakaz naprawczy
5. Austriacki organ ochrony danych zakwestionował ujawnienie nazwiska
6. Recepta na cyberbezpieczeństwo. Szkolenie z ochrony danych dla dyrektorów placówek medycznych
7. Włoski organ ochrony danych nałożył 10 000 euro kary na instytut badawczy
8. Sąd Pracy w Weiden zasądził 8 tys. euro od właściciela baru za tajne nagrania
9. Duży cyberatak na lodówki i zamrażarki sklepowe we Francji
10. Dostęp Policji do monitoringu prowadzonego przez gminy – uwagi Prezesa UODO dla MSWiA

Istota testu prywatności. Eksperci UODO na Warsztatach Legislacyjnych

- **Kontekst:** Artykuł podkreśla, że im lepsze prawo, tym lepsze państwo. Jasne i sprawiedliwe przepisy służą wszystkim, a państwo oparte na dobrym prawie wzmacnia zaufanie obywateli.
- **O czym są Warsztaty Legislacyjne:** To wydarzenie poświęcone tworzeniu prawa, technice prawodawczej i praktyce legislacyjnej, będące miejscem dyskusji prawników-legislatorów pracujących w rządowych i parlamentarnych służbach prawnych.
- **Kto bierze udział:** Oprócz legislatorów uczestniczą zaproszeni przedstawiciele nauk prawnych i praktycy procesu prawotwórczego, którzy dzielą się wiedzą i doświadczeniem.
- **Udział UODO:** Podczas XV edycji nie zabrakło przedstawicieli Urzędu Ochrony Danych Osobowych, co podkreśla znaczenie ochrony danych w nowoczesnym prawodawstwie.
- **Główny punkt programu (1 października):** Wykład pt. „Ocena stopnia wdrażania przepisów o ochronie danych osobowych w procesie legislacyjnym - przegląd praktyk", prowadzony przez Weronikę Kowalik i Tomasza Głuszczyka z Departamentu Prawa i Nowych Technologii UODO.
- **Najważniejsze przesłanie wykładu UODO:** W procesie stanowienia prawa kluczowe jest realne sprawdzanie, jak przepisy o ochronie danych są wdrażane oraz rzetelna ocena skutków regulacji (czyli przewidywanie konsekwencji nowych przepisów).
- **Wskazane wyzwania praktyczne:**
  - przetwarzanie danych na dużą skalę w warunkach coraz powszechniejszej automatyzacji,
  - dobór adekwatnych rozwiązań technicznych przy szybkim rozwoju technologii,
  - ryzyko wdrażania nowych rozwiązań IT bez wystarczających podstaw prawnych.

- **Szersze otoczenie regulacyjne:** Zwrócono uwagę, że przy projektowaniu przepisów trzeba uwzględniać nie tylko RODO, ale także inne regulacje dotyczące danych i technologii (m.in. DGA, DSA, AI Act) oraz dbać o gwarancje ochrony praw i wolności osób, których dane dotyczą.
- **Dobre i złe praktyki:** Prelegenci przedstawili przykłady rozwiązań godnych stosowania oraz negatywnych podejść spotykanych w projektach przepisów regulujących przetwarzanie danych osobowych.
- **Rola organu nadzorczego i „test prywatności":** Celem wystąpienia było pokazanie roli UODO, dzielenie się doświadczeniami oraz promowanie dobrych praktyk, w tym podkreślenie znaczenia testu prywatności (czyli sprawdzania wpływu projektowanych rozwiązań na prywatność).
- **Organizacja wydarzenia:** XV Warsztaty Legislacyjne odbyły się w Juracie w dniach 30 września – 2 października.
- **Otwarcie warsztatów:** Uczestników powitali m.in. przedstawiciele Ministerstwa Sprawiedliwości, samorządu oraz instytucji publicznych; wykład inauguracyjny wygłosił dr hab. Piotr Zientarski („O stałej potrzebie szacunku do Prawa i Legislatora").
- **Inne poruszane tematy:** W programie znalazły się m.in. zagadnienia deregulacji, zarządzania interesariuszami w procesie legislacyjnym oraz konstytucyjne aspekty ogłaszania aktów prawnych.
- **Zakończenie:** Warsztaty zamknęło podsumowanie i dyskusja 2 października, moderowana przez Michała Zonia (Dyrektora Biura Prawnego CZSW).

Źródło: https://uodo.gov.pl/pl/138/4600

Czy DSA może pomóc zapobiegać atakom w szkołach?

- **Kontekst:** 8 października Sejm przyjął ustawę wdrażającą unijny Akt o usługach cyfrowych (DSA) do polskiego prawa. Projekt **nagle trafił do bloku głosowań** po serii ataków nożowników w polskich szkołach. Rząd widzi w nowych przepisach narzędzie do ograniczania przemocy promowanej w internecie, ale eksperci podkreślają, że **to może nie wystarczyć**.
- **Co się wydarzyło w szkołach:** w krótkim czasie doszło do kilku niebezpiecznych zdarzeń. W Leszczydole-Nowinach 15-letni były uczeń zaatakował dyrektora, nauczycielkę i woźną; **37-letnia kobieta zmarła**. Premier wskazał, że sprawca miał kask z kamerą, bo **chciał nagrać atak**.
- **Dlaczego rząd łączy to z internetem:** według premiera internet może nie tylko relacjonować, ale też **promować przemoc** (np. przez „wyzwania", materiały sprawców, treści z gier/streamów), co może wpływać na zachowania osób nieletnich.
- **Co dokładnie wdraża Polska:** chodzi o nowelizację ustawy o świadczeniu usług drogą elektroniczną, która ma wprowadzić rozwiązania DSA. Wcześniejsza wersja została **zawetowana przez prezydenta**, potem przygotowano **dwa osobne projekty**.
- **Co już weszło / jest przesądzone:** prezydent podpisał ustawę, która ustanawia **Prezesa UKE** koordynatorem ds. usług cyfrowych.
- **Co ma wejść w życie teraz:** drugi projekt (przyjęty przez Sejm 8 października) ma dać organowi państwa możliwość **blokowania i usuwania nielegalnych treści** w internecie. Ustawa trafia do Senatu i równolegle jest **notyfikowana w Komisji Europejskiej**.
- **Dlaczego prace przyspieszono:** rząd powołał się na wyjątek w procedurze notyfikacji KE – „**gwałtowna konieczność zabezpieczenia życia, zdrowia i porządku publicznego**".
- **Cel operacyjny zmian (wg MC):** stworzenie systemu, który wymusi na platformach **szybkie ścieżki reagowania** oraz może ograniczać „masowe" publikowanie nielegalnych treści przez **boty**.
- **Jakie treści UKE będzie mógł blokować (przykłady z ustawy):**
  - treści dotyczące przemocy lub groźby bezprawnej motywowanej m.in. rasą, pochodzeniem, wyznaniem/bezwyznaniowością, przynależnością polityczną,
  - groźby i nękanie w mediach społecznościowych,
  - treści dotyczące zlecania zabójstwa „za korzyść",
  - namawianie lub pomoc w doprowadzeniu do samobójstwa,
  - cyberbullying (wskazany jako jedna z kategorii),
  - nakłanianie do spowodowania ciężkiego uszczerbku na zdrowiu,
  - utrwalanie wizerunku nagiej osoby lub podczas czynności seksualnej przy użyciu przemocy/groźby/podstępu.

- **Odwołanie:** od decyzji o blokadzie będzie można **odwołać się do sądu powszechnego**.
- **Blokowanie natychmiastowe:** w części spraw treści mają być blokowane od razu, m.in.:
  - prezentowanie pornografii dzieciom poniżej 15 lat oraz składanie im propozycji seksualnych,
  - propagowanie pedofilii,
  - (po poprawce) rozpowszechnianie/prezentowanie pornografii z udziałem małoletnich.

- **Argumenty zwolenników w Sejmie:** według Moniki Rosy radykalizacja młodych w dużej mierze odbywa się w sieci (platformy, streaming, gry, komunikatory), a państwo powinno mieć narzędzia do blokowania treści przestępczych (np. namawiania do samobójstwa, gróźb, treści pedofilskich).
- **Główna wątpliwość ekspertów:** samo DSA **nie zapobiegnie** atakom w szkołach; regulacje mogą pomóc w moderacji treści, ale nie rozwiązują źródeł przemocy.
- **Ocena Panoptykonu:** Katarzyna Szymielewicz wskazuje, że katalog przestępstw w ustawie nie odpowiada wprost mechanizmom stojącym za atakami nożowników; jej zdaniem problem leży też w tym, że polskie przepisy **nie uderzają w model biznesowy i algorytmy platform**, które promują szkodliwe treści.
- **Ocena Kids Alert:** DSA powinno obowiązywać w Polsce od miesięcy, bo ułatwiłoby usuwanie przemocy w sieci i ograniczało „efekt naśladownictwa", ale **nie rozwiąże wszystkich problemów**; część treści „na granicy legalności" i tak pozostanie.
- **Ocena Fundacji Dajemy Dzieciom Siłę:** popiera szybkie usuwanie treści wzywających do przemocy/nienawiści, ale podkreśla, że nie należy upraszczać związku DSA z atakami w szkołach. Potrzebne są też działania pozaprawne: wsparcie nauczycieli, edukacja i profilaktyka przemocy rówieśniczej, rozwijanie kompetencji społecznych i empatii, pomoc rodzicom w zasadach korzystania z ekranów oraz uważność i rozmowa z dzieckiem.
- **Wniosek z artykułu:** nowe przepisy mogą **usprawnić blokowanie nielegalnych treści** i dać państwu dodatkowe narzędzia ochrony (zwłaszcza dzieci), ale eksperci ostrzegają, że **nie są „lekiem" na przemoc w szkołach** i nie zastąpią szerszych działań społecznych oraz zmian po stronie platform internetowych.

Źródło: https://edgp.gazetaprawna.pl/prawo/prawo-internetu-i-ochrony-danych/artykuly/11328205,czy-dsa-moze-pomoc-zapobiegac-atakom-w-szkolach.html

Fiński Organ Ochrony Danych uznał, że szkolne dane służą tylko nauczaniu

- **Kontekst:** 4 września 2026 r. fiński organ ochrony danych wydał decyzję o tym, kiedy szkoły i gminy mogą legalnie przetwarzać dane uczniów przy cyfrowym nauczaniu na podstawie **art. 6 ust. 1 lit. c RODO** (wykonanie obowiązku prawnego). Decyzja pokazuje, że jest to możliwe, ale tylko w **ściśle ograniczonym zakresie** – takim, jaki jest realnie potrzebny do nauczania.

- **Sprawa dotyczyła** miasta Espoo i korzystania w szkołach z programów edukacyjnych Google. Skarga wskazywała na brak zgody opiekuna, ale miasto argumentowało, że podstawą nie jest zgoda, tylko **ustawowy obowiązek organizacji edukacji**.
- **Wątek procesowy:** wcześniejsze stanowisko organu, które całkowicie wykluczało stosowanie art. 6 ust. 1 lit. c RODO, zostało zakwestionowane przez fiński Najwyższy Sąd Administracyjny i sprawa wróciła do ponownego rozpoznania. Sąd nie przesądził szczegółów, ale podważył „automatyczne" odrzucenie tej podstawy prawnej.

- **Najważniejszy wniosek:** obowiązek organizacji kształcenia może być co do zasady **podstawą prawną** przetwarzania danych uczniów przy użyciu narzędzi **centralnie związanych z nauczaniem** (np. edytor tekstu, e-mail, kalendarz, prezentacje, aplikacje do nauki przedmiotów).
- **To nie jest „blankietowa zgoda" na wszystko:** samo użycie platformy edukacyjnej nie oznacza, że wolno przetwarzać **wszystkie** dane, jakie powstają podczas jej działania.
- **Kluczowe wymagania:** trzeba badać łącznie:
  - **niezbędność** przetwarzania do realizacji obowiązku edukacyjnego, oraz
  - **minimalizację danych** (zbieranie tylko tego, co konieczne).

- **Granica dotycząca dostawcy usługi (najbardziej praktyczna część decyzji):** szkoła/gmina nie może powołując się na art. 6 ust. 1 lit. c RODO:
  - przekazywać danych ucznia dostawcy, ani
  - zapewniać dostawcy dostępu do danych w taki sposób, aby mógł je wykorzystywać **do własnych celów**,

  np. do **rozwoju usługi** lub innych programów/usług.
- **Wniosek praktyczny:** dane zebrane w ramach realizacji obowiązku edukacyjnego nie mogą „przy okazji" zasilać celów biznesowych dostawcy.

- **Co oznacza wymóg „niezbędności":** trzeba sprawdzić, czy cel edukacyjny da się osiągnąć **równie skutecznie** metodą mniej ingerującą w prywatność. Jeśli tak, to co do zasady nie spełnia się warunku niezbędności dla art. 6 ust. 1 lit. c RODO.
- **Szczególna wrażliwość sytuacji dzieci:** decyzja podkreśla ryzyko szerokiego i długotrwałego zbierania danych uczniów przez podmioty zewnętrzne, w tym ryzyko **profilowania**. Wybór narzędzi i ich konfiguracja wymagają więc podwyższonej staranności.

- **Znaczenie dla podmiotów publicznych (szkół, gmin):** można korzystać z e-programów na podstawie obowiązku prawnego, ale pod warunkiem że:
  - **cel jest wyłącznie edukacyjny**,
  - **zakres danych jest konieczny** (minimalizacja),
  - **dostawca nie ma możliwości** używania danych do własnych, odrębnych celów.

- **Co należy weryfikować w praktyce:** nie tylko funkcje programu, ale też **umowy** i to, jakie dane są rzeczywiście zbierane (zwłaszcza dane **diagnostyczne i telemetryczne**).
- **Status decyzji:** decyzja **nie jest prawomocna**.

Źródło: https://judykatura.pl/finski-organ-ochrony-danych-uznal-ze-szkolne-dane-sluza-tylko-nauczaniu/

Hiszpański Sąd Krajowy zawiesił ogólny nakaz naprawczy

- **Kontekst:** Sprawa dotyczy tego, jak precyzyjnie organ ochrony danych (hiszpańska AEPD) musi formułować **nakaz naprawczy** przy naruszeniach RODO. Hiszpański Sąd Krajowy uznał, że nie wystarczy ogólne polecenie „dostosowania przetwarzania do RODO" – organ powinien wskazać **konkretny sposób** wykonania nakazu.
- **Najważniejszy wniosek (teza sądu):** Uprawnienie z art. 58 ust. 2 lit. d RODO pozwala wydać nakaz dostosowania przetwarzania, ale musi on zawierać łącznie:
  - **określony sposób wykonania** (co konkretnie trzeba zrobić), oraz
  - **określony termin** realizacji.

  Sam termin bez wskazania „jak" jest niewystarczający.
- **Co było w decyzji AEPD:** Organ stwierdził naruszenia **art. 13 RODO** (obowiązek informacyjny) oraz **art. 6 ust. 1 RODO** (podstawa prawna przetwarzania). Poza karami nakazał spółce w ciągu **6 miesięcy** „dostosować przetwarzanie" do przepisów, wskazując ogólnie, że spółka ma:
  - zapewnić właściwą **podstawę prawną** dla operacji przetwarzania,
  - przekazać osobom wymagane informacje zgodnie z **art. 13 RODO**,
  - ale pozostawił spółce wybór konkretnych procedur i mechanizmów.

- **Stanowisko sądu:** Ogólne odesłanie do przepisów (np. „stosuj art. 6 i art. 13 RODO") **nie zastępuje** obowiązku wskazania przez organ konkretnego sposobu wykonania nakazu. Sąd podkreślił, że brzmienie art. 58 ust. 2 lit. d RODO wymaga działania „w określony sposób i w określonym terminie".
- **Dlaczego to ważne dla firm:** Zbyt ogólny nakaz może wymuszać poważne zmiany organizacyjne („działania strukturalne") wpływające na funkcjonowanie przedsiębiorstwa, a jednocześnie pozostawiać niejasność, co dokładnie jest wymagane.
- **Ryzyko prawne przy nieprecyzyjnym nakazie:** Sąd wskazał, że brak precyzji może powodować:
  - **niepewność prawną** (firma nie wie, co dokładnie ma wdrożyć),
  - potencjalne naruszenie **prawa do obrony**,
  - przerzucanie na administratora konieczności „domyślania się" treści obowiązku pod groźbą kolejnych sankcji.

- **Co zrobił sąd w tej sprawie:** Postanowieniem z **13 lipca 2026 r.** Audiencia Nacional **zawiesił wykonanie** nakazu wdrożenia środków naprawczych **do czasu**, aż AEPD go doprecyzuje (czyli wskaże konkretne środki/oczekiwane działania).
- **Czego zawieszenie nie dotyczyło:** Sąd **nie wstrzymał** dwóch administracyjnych kar pieniężnych:
  - **20 000 euro**,
  - **200 000 euro** – spółka je zapłaciła.

- **Co pozostaje otwarte:** To rozstrzygnięcie ma charakter zabezpieczający – sąd:
  - nie przesądził, jakie dokładnie środki powinny zostać wdrożone,
  - nie rozstrzygnął ostatecznie, czy doszło do naruszeń wskazanych przez organ,
  - nie uchylił kar pieniężnych w tym trybie.

- **Praktyczna puenta:** Organ nadzorczy nie może ograniczyć się do ogólnego celu („dostosuj się do RODO"). Powinien jasno opisać **konkretny obowiązek** do wykonania, a dopiero w ramach tak wyznaczonych granic administrator dobiera adekwatne rozwiązania wdrożeniowe.

Źródło: https://judykatura.pl/hiszpanski-sad-krajowy-zawiesil-ogolny-nakaz-naprawczy/

Austriacki organ ochrony danych zakwestionował ujawnienie nazwiska

- **Kontekst:** Austriacki organ ochrony danych (DPA) ocenił publikację fragmentów orzeczenia karnego na publicznych profilach w mediach społecznościowych. Mimo „przywileju medialnego" (ułatwień dla działalności dziennikarskiej) organ uznał, że trzeba każdorazowo sprawdzać, czy ujawnienie konkretnych danych jest **niezbędne** do celu publikacji, a nie tylko „związane z dziennikarstwem".
- **O co chodziło w sprawie:** autor (redaktor naczelny) opublikował na trzech publicznych platformach wybrane fragmenty rozstrzygnięcia, dodał własny tytuł i komentarz oraz próbował anonimizacji. Jednak nazwisko i informacja o roli osoby jako oskarżonego pozostały miejscami czytelne. Wpisy były dostępne co najmniej od 15 czerwca do 1 lipca 2026 r.; jeden z nich zebrał 1302 reakcje i 36 udostępnień.
- **Najważniejszy wniosek:** nawet jeśli publikacja ma cel dziennikarski i korzysta z przywileju medialnego, **nie zwalnia to z zasady minimalizacji danych** (ujawniać tylko to, co konieczne) oraz z obowiązku wykazania, że tę zasadę spełniono.
- **Teza 1 – dane oskarżonego są chronione:** imię i nazwisko wraz z informacją, że dana osoba jest oskarżonym, to dane osobowe. Dodatkowo informacja o byciu oskarżonym stanowi też **dane dotyczące przestępstw** (art. 10 RODO) – nawet jeśli nie doszło do stwierdzenia winy lub sprawa zakończyła się korzystnie dla tej osoby.
- **Teza 2 – odpowiedzialność ponosi publikujący:** osoba prowadząca własne publiczne profile i samodzielnie decydująca o treści, czasie i miejscu publikacji jest **administratorem danych** w rozumieniu RODO. To dotyczy także sytuacji, gdy zawodowo jest redaktorem naczelnym, ale firma medialna nie kierowała tą publikacją.
- **Teza 3 – przywilej medialny nie wymaga zgody, ale ma granice:** przywilej medialny może być samodzielną podstawą prawną przetwarzania do celów dziennikarskich (bez dodatkowej podstawy z art. 6 RODO i bez uprzedniej zgody). Jednak **nie wyłącza** zasad: minimalizacji danych i rozliczalności.
- **Teza 4 – anonimizacja może być konieczna:** trzeba ocenić, czy cel dziennikarski da się osiągnąć poprzez anonimizację lub mniej ingerującą prezentację o porównywalnej wartości informacyjnej. W tej sprawie organ uznał, że **tożsamość oskarżonego nie była potrzebna** do zrozumienia wyniku sprawy ani do krytycznego komentarza autora (dotyczącego m.in. postępowań określanych jako SLAPP).
- **Znaczenie częściowej anonimizacji:** fakt, że autor w jednym miejscu zaczął usuwać nazwisko, był dodatkowym sygnałem, że ujawnienie tożsamości nie było „celowym elementem" przekazu. Organ podkreślił jednak, że kluczowe jest obiektywne pytanie: czy identyfikacja była potrzebna do celu publikacji.
- **Teza 5 – późniejsza zgoda nie „cofa" naruszenia:** zgoda uzyskana po publikacji nie legalizuje wcześniejszego ujawnienia i nie usuwa naruszenia w okresie, gdy wpisy były dostępne. Może natomiast wpłynąć na dobór środka (np. łagodniej), bo zmniejsza ocenę realnych negatywnych skutków dla osoby, której dane ujawniono.
- **Teza 6 – ostrzeżenie nie wymaga winy:** organ może wydać **ostrzeżenie** już przy samym obiektywnym stwierdzeniu naruszenia RODO; nie trzeba wykazywać umyślności czy niedbalstwa. Wina ma znaczenie przede wszystkim przy **karze pieniężnej**.
- **Dlaczego skończyło się na ostrzeżeniu, a nie karze:** organ nie uznał sprawy za błahą (publiczny zasięg, udostępnienia, ryzyko stygmatyzacji związane z informacją o oskarżeniu). Jednocześnie wziął pod uwagę: usunięcie wpisów, późniejszą zgodę osoby oraz brak wcześniejszych naruszeń – i dlatego odstąpił od kary pieniężnej, poprzestając na ostrzeżeniu.
- **Status decyzji:** decyzja nie była prawomocna; w chwili opisu sprawy otwarty był termin na złożenie skargi do austriackiego Federalnego Sądu Administracyjnego.

Źródło: https://judykatura.pl/austriacki-organ-ochrony-danych-zakwestionowal-ujawnienie-nazwiska/

Recepta na cyberbezpieczeństwo. Szkolenie z ochrony danych dla dyrektorów placówek medycznych

- **Kontekst:** Urząd Ochrony Danych Osobowych (UODO) wraz z Naczelną Izbą Lekarską zorganizował szkolenie dla dyrektorów placówek medycznych pt. „Praktyczne zagadnienia związane z ochroną oraz udostępnianiem danych osobowych w podmiotach leczniczych". Tematem przewodnim była ochrona danych pacjentów w realiach rosnących zagrożeń (ataki hakerskie i szybki rozwój AI), które szczególnie niebezpiecznie wpływają na dane dotyczące zdrowia.
- **Skala problemu:** Wyciek danych medycznych staje się coraz częstszy — niemal co tydzień media informują o kolejnych incydentach obejmujących dane milionów pacjentów. W takich sytuacjach wyciek numeru PESEL może być mniej dotkliwy niż ujawnienie informacji o stanie zdrowia.
- **Dane o incydentach:** CSIRT CeZ (zespół reagowania na incydenty powołany przez Ministerstwo Zdrowia) podał, że tylko do końca września wykryto **1379 incydentów cyberbezpieczeństwa** w sektorze ochrony zdrowia.
- **Głośne wycieki i reakcja UODO:** W ostatnich tygodniach doszło do dużych wycieków danych m.in. z **MyDr** i **Medyc**. Prezes UODO zdecydował o przeprowadzeniu kontroli w firmach przetwarzających dane w tych przypadkach.
- **Zapowiedziane kontrole w całym sektorze:** Prezes UODO Mirosław Wróblewski zapowiedział również **dodatkowe kontrole dotyczące przetwarzania danych w ochronie zdrowia**, które mają zostać przeprowadzone **do końca 2026 roku**.
- **„Miesiąc miodowy z RODO się skończył":** Prezes UODO podkreślił, że podejście „na przeczekanie" się kończy — instytucje muszą traktować ochronę danych poważnie, bo inaczej pacjenci mogą tracić zaufanie do cyfryzacji i do systemu ochrony zdrowia.
- **UODO nie tylko kontroluje:** Obok kontroli i kar urząd prowadzi też działania edukacyjne. Szkolenie z 2 października było skierowane do kadry zarządzającej placówkami (dyrektorów), z założeniem, że uczestnicy mają pełnić rolę „ambasadorów" ochrony danych.
- **Ochrona danych jako element zarządzania placówką:** Monika Krasińska (UODO) zwróciła uwagę, że dobrze wdrożony system ochrony danych wpływa na sposób zarządzania placówką, cyberbezpieczeństwo oraz jakość usług. Podkreślono też tezę: **nie ma cyberbezpieczeństwa bez ochrony danych osobowych**.
- **Kluczowe elementy bezpieczeństwa:** Wskazano na znaczenie:
  - **analizy ryzyka** (rozpoznania realnych zagrożeń i słabych punktów),
  - **roli inspektora ochrony danych (IOD)**,
  - **zaangażowania kadry zarządzającej** w proces ochrony danych (to nie jest tylko zadanie IT).

- **Najczęstsze problemy i źródła naruszeń:** Piotr Popielewicz (UODO) omówił zgłoszenia z placówek medycznych i wskazywał m.in. na przypadki:
  - nieuprawnionego ujawnienia danych,
  - naruszenia integralności danych,
  - pozostawienia dokumentacji w niezabezpieczonych miejscach,
  - nieuprawnionego wykorzystania danych osobowych.

- **Braki organizacyjne:** Zwrócono uwagę na **niedostateczną świadomość zagrożeń** i brak szkoleń dopasowanych do konkretnych ryzyk w placówkach.
- **Typowe cyberzagrożenia:** Wskazano m.in. na **phishing** oraz ataki **ransomware**. Podawano przykłady zabezpieczeń i rozwiązań, które mogą ograniczać ryzyko takich incydentów.
- **Ryzyko przestarzałego oprogramowania:** Jednym z powodów podatności na ransomware bywa korzystanie z systemów i aplikacji, dla których producent zakończył wsparcie techniczne — co często oznacza obecność **krytycznych luk bezpieczeństwa**.
- **Skargi do UODO – dwa główne typy:** Maciej Tracz (UODO) omówił skargi dotyczące ochrony zdrowia, dzieląc je na:
  - skargi na **naruszenie zasad ochrony danych** (RODO, rozdział II),
  - skargi na **naruszenie praw osób, których dane dotyczą** (RODO, rozdział III).

- **Kto składa skargi:** Skargi pochodzą nie tylko od pacjentów, ale również od **obecnych i byłych pracowników** placówek.
- **Praktyczny wymiar:** W szkoleniu omawiano konkretne sprawy i decyzje wydawane przez Prezesa UODO, co miało pomóc placówkom zrozumieć, jakie sytuacje w praktyce prowadzą do naruszeń i konsekwencji.

Źródło: https://uodo.gov.pl/pl/138/4604

Włoski organ ochrony danych nałożył 10 000 euro kary na instytut badawczy

- **Kontekst:** faza testowa monitoringu wizyjnego w miejscu pracy **podlega RODO**. Włoski organ ochrony danych uznał, że **samo wyświetlanie obrazu z kamer (na żywo), nawet bez nagrywania**, jest przetwarzaniem danych osobowych.

- **Teza 1 — test kamer wymaga podstawy prawnej:** uruchomienie kamer w pracy, także „tylko testowo" i bez rejestracji, to przetwarzanie danych pracowników i innych osób na terenie zakładu. Jeśli instalacja różni się od uzgodnień (np. ze związkami), przetwarzanie może być **bez podstawy prawnej** i naruszać zasady legalności, rzetelności i przejrzystości.
- **Teza 2 — informacja musi być przed uruchomieniem:** pracodawca powinien przekazać pracownikom informacje o przetwarzaniu **zanim kamery zostaną włączone**. Nie ma znaczenia, że chodzi wyłącznie o testy techniczne.
- **Teza 3 — sama tabliczka nie wystarcza:** trzeba zapewnić:
  - **informację „pierwszego poziomu"** (oznaczenie przy obszarze monitorowanym), oraz
  - **informację „drugiego poziomu"** (pełna klauzula z elementami z art. 13 RODO, łatwo dostępna).

  Oznaczenie powinno jasno wskazywać m.in. **rzeczywisty cel**, **administratora**, **prawa osób**, **okres przechowywania** oraz **odesłanie do pełnej informacji**.
- **Teza 4 — ocena skutków (DPIA) przed monitoringiem:** monitoring pracowników często wymaga **uprzedniej oceny skutków dla ochrony danych**, bo wiąże się z podwyższonym ryzykiem (relacja zależności pracownik–pracodawca i systematyczne monitorowanie). Brak nagrań **nie znosi** obowiązków: podstawy prawnej, informacji i (gdy wymagane) DPIA.

- **Co się wydarzyło (sprawa we Włoszech):** po skargach dwóch pracowników organ (Garante) zbadał działania instytutu badawczego z Turynu. Było porozumienie ze związkami na **10 kamer** monitorujących zasadniczo obrzeża (mury/ogrodzenie), z ograniczonymi korektami technicznymi.
- **Co zakwestionowano:** zainstalowano **8 dodatkowych kamer** (łącznie 18) oraz zmieniono ich rozmieszczenie i pola widzenia. System włączono w trybie testowym: w wybrane dni robocze obraz był **wyświetlany na żywo przez kilka godzin**, bez zapisu.
- **Stanowisko organu:** to nadal jest **przetwarzanie danych**, bo obraz osób był dostępny w systemie. Ponieważ testy odbywały się w konfiguracji **innej niż uzgodniona**, doszło do naruszeń legalności i przejrzystości (brak właściwej podstawy prawnej w tym zakresie).
- **Obowiązek informacyjny:** instytut nie przekazał pracownikom szczególnej informacji **przed testowym uruchomieniem**; organ uznał to za naruszenie. Kluczowa zasada: granicą jest **start przetwarzania**, a nie „formalny odbiór" czy rozpoczęcie regularnej eksploatacji.
- **Dlaczego oznaczenia były niewystarczające:** pojawiły się dopiero po testach, a ich treść była zbyt ogólna (np. sam skrót nazwy instytutu, ogólny cel „bezpieczeństwo", brak praw osób, brak okresu przechowywania, brak jasnego wskazania, że kod/odnośnik prowadzi do pełnej informacji). Dodatkowo nie zapewniono pełnej informacji „drugiego poziomu".
- **DPIA:** instytut chciał odłożyć ocenę skutków do czasu doprecyzowania systemu, ale organ wskazał, że przy monitoringu pracowników DPIA powinna powstać **przed rozpoczęciem przetwarzania**.

- **Sankcja:** organ potraktował naruszenia jako jedno powiązane zachowanie i nałożył **10 000 euro kary** oraz nakazał publikację części decyzji. Przy wymiarze kary uwzględniono m.in. krótki czas testów (4 dni robocze), nieumyślność, brak danych szczególnych kategorii, dobrą współpracę i brak istotnych wcześniejszych naruszeń.
- **Najważniejszy wniosek praktyczny:** „test monitoringu" nie jest wyjątkiem od RODO. Jeśli obraz osób jest dostępny (nawet bez nagrywania), to już na etapie testów trzeba zadbać o **legalność (w tym zgodność z uzgodnieniami), przejrzystą informację oraz – gdy wymagane – ocenę skutków**.

Źródło: https://judykatura.pl/wloski-organ-ochrony-danych-nalozyl-10-000-euro-kary-na-instytut-badawczy/

Sąd Pracy w Weiden zasądził 8 tys. euro od właściciela baru za tajne nagrania

- **Kontekst sprawy:** wyrok dotyczy wykorzystania monitoringu do **potajemnego nagrywania pracownicy** w damskiej toalecie (nagrania intymne). Sąd wyjaśnił, że **sam fakt nagrywania** jest ciężkim naruszeniem, nawet jeśli nagrania nie zostały później opublikowane.
- **Co się wydarzyło:** właściciel muzycznego baru zainstalował **ukrytą kamerę** skierowaną na sedes. Nagrania zapisywały się w urządzeniu, były widoczne w aplikacji w telefonie oraz przechowywane na innych nośnikach i w chmurze.
- **Zakres naruszenia:** przez wiele miesięcy rejestrowano bez wiedzy pracownicy nagrania pokazujące jej **nagie pośladki i genitalia** podczas korzystania z toalety.
- **Ocena sądu – ciężar naruszenia:** sąd uznał, że już samo **potajemne, długotrwałe utrwalanie intymnych nagrań** stanowi bardzo poważne naruszenie dóbr osobistych (bez potrzeby wykazywania, że nagrania gdziekolwiek „wyszły").
- **Relacja pracodawca–pracownik pogarsza sytuację sprawcy:** dodatkowym obciążeniem było to, że pracodawca działał wbrew obowiązkowi poszanowania interesów pracownicy i **wykorzystał relację zatrudnienia** do ingerencji w najbardziej wrażliwą sferę prywatności.
- **Brak rozpowszechnienia nie zwalnia z odpowiedzialności:** argument pozwanego, że materiał pozostał „w jego prywatnej sferze", został odrzucony. Sąd podkreślił, że waga naruszenia nie znika tylko dlatego, że nagrań nie opublikowano.
- **Dodatkowe konsekwencje dla pokrzywdzonej:** sąd uwzględnił, że w toku postępowania karnego i sądowego pokrzywdzona musiała wielokrotnie konfrontować się z upokarzającymi okolicznościami sprawy (materiał był analizowany i omawiany przez różne osoby).
- **Dlaczego zasądzono pieniądze (a nie tylko zakaz dalszych działań):** sąd uznał, że samo żądanie zaniechania nie rekompensuje naruszenia, które już się zakończyło (powódka nie pracowała już u pozwanego i ryzyko powtórzenia wobec niej nie było aktualne).
- **Jak sąd ustalał wysokość świadczenia:** wziął pod uwagę trzy elementy:
  - **zadośćuczynienie** dla pokrzywdzonej,
  - **funkcję prewencyjną** (żeby zniechęcać do podobnych działań),
  - **intensywność naruszenia**.

  Jednocześnie sąd wskazał, że **nie trzeba udowadniać konkretnych następstw psychicznych**, aby przyznać takie świadczenie.
- **Co przesądzało o „szczególnej wadze" naruszenia:** m.in. cel seksualny, zaplanowane przygotowanie techniczne, ukryty montaż kamery, wielomiesięczne działanie oraz przechowywanie nagrań na kilku nośnikach (a także próba usunięcia materiału po wykryciu).
- **Rozstrzygnięcie (kwoty):** wyrokiem z 16 kwietnia 2026 r. Sąd Pracy w Weiden zasądził na rzecz byłej pracownicy **8 000 euro** świadczenia pieniężnego.
- **Wątek karny i „obowiązek probacyjny":** w sprawie karnej nałożono na pozwanego obowiązek zapłaty **1 600 euro** tytułem naprawienia szkody (według ustaleń sądu – dotychczas nie zapłacono).
- **Zaliczenie płatności:** jeśli 1 600 euro zostanie zapłacone w ramach obowiązku probacyjnego, kwota ta **ma zostać zaliczona** na poczet zasądzonych 8 000 euro. Jednocześnie wykonanie obowiązku probacyjnego **zwykle nie wyczerpuje** roszczeń cywilnych w całości.
- **RODO:** sąd wskazał, że nie musiał rozstrzygać, czy oprócz tych podstaw odpowiedzialności istniało także odrębne roszczenie z **art. 82 RODO** (czyli odszkodowanie za naruszenie przepisów o ochronie danych).
- **Wniosek praktyczny dla pracodawców:** bezprawny monitoring może prowadzić do **odpowiedzialności cywilnej** nawet wtedy, gdy nagrania nie zostały publicznie ujawnione.

Źródło: https://judykatura.pl/sad-pracy-w-weiden-zasadzil-8-tys-euro-od-wlasciciela-baru-za-tajne-nagrania/

Duży cyberatak na lodówki i zamrażarki sklepowe we Francji

- **Kontekst:** media informują o cyberataku na systemy sterowania lodówkami i zamrażarkami firmy Danfoss, używane m.in. w sieciach sklepów (wymieniane są Intermarché / Leclerc / Super U). Skala zdarzenia ma obejmować **kilkaset sklepów**.
- **Na czym polegał atak:** napastnicy mieli zdalnie manipulować temperaturą urządzeń chłodniczych, uruchamiając w pętli funkcję **odmrażania** z ustawieniem temperatury na ok. **+50°C**.
- **Możliwe skutki biznesowe:** straty (np. zepsuty towar, przestoje operacyjne) mogą sięgać **kilku milionów euro**.
- **Jakie podatności mogły zostać wykorzystane:** nie ma jeszcze oficjalnego potwierdzenia, ale podejrzenia dotyczą niedawno opisanych luk w urządzeniach Danfoss, w tym mechanizmu umożliwiającego **obejście logowania do panelu administracyjnego**.
- **Kluczowa luka (CVE-2025-41451):** „ukryte" hasło/sekret do uwierzytelnienia miało być **generowane wyłącznie na podstawie bieżącej daty** urządzenia. Jeśli atakujący odtworzy algorytm, może wygenerować poprawny kod dla dowolnego dnia i **zalogować się z uprawnieniami administratora**.
- **Dlaczego to groźne:** skuteczne użycie tego mechanizmu daje **w pełni uwierzytelnioną sesję administracyjną** i uprzywilejowany dostęp do webowego interfejsu zarządzania (czyli możliwość zmiany ustawień pracy urządzeń).
- **Ekspozycja urządzeń w internecie:** badacze wskazują, że byli w stanie znaleźć na Shodanie **ponad 2000** urządzeń, a dokładniej **interfejsy administracyjne wystawione do internetu**, co zwiększa ryzyko masowych ataków.
- **Aktualizacje i ryzyko „niezałatania":** producent wydał poprawki, ale istnieje ryzyko, że **nie wszyscy użytkownicy/organizacje je wdrożyli**, co mogło umożliwić wykorzystanie luk w praktyce.

Źródło: https://sekurak.pl/duzy-cyberatak-na-lodowki-i-zamrazarki-sklepowe-we-francji/

Dostęp Policji do monitoringu prowadzonego przez gminy – uwagi Prezesa UODO dla MSWiA

- **Kontekst:** Policja zwraca się do jednostek samorządu terytorialnego (gmin/miast) z propozycjami porozumień, które miałyby zapewnić jej **stały dostęp** do gminnego monitoringu wizyjnego. Dodatkowe wątpliwości budzi używanie przez Policję i straże gminne monitoringu z **rozpoznawaniem twarzy** lub analizą innych **cech biometrycznych**.
- **Działanie UODO:** Prezes Urzędu Ochrony Danych Osobowych (Mirosław Wróblewski) skierował pismo do Ministra SWiA (Marcina Kierwińskiego), wskazując na potrzebę stworzenia **jasnych regulacji prawnych** dotyczących dostępu Policji do monitoringu samorządowego (sygn. DPNT.413.7.2026).
- **Cel i warunek:** UODO podkreśla, że zapewnienie Policji możliwości wykonywania ustawowych zadań jest ważne, ale musi się odbywać **z poszanowaniem konstytucyjnych praw i wolności** oraz przepisów o ochronie danych.
- **Główny problem:** Zdaniem UODO w polskim prawie **brakuje wyczerpujących i przejrzystych przepisów** dotyczących stosowania monitoringu wizyjnego przez Policję, zwłaszcza w modelu stałego, systematycznego dostępu.
- **Stały dostęp do monitoringu – wątpliwości prawne:** UODO otrzymuje sygnały z samorządów, że proponowane porozumienia mogą być **niezgodne** z prawem krajowym i prawem UE, bo zmierzają do szerokiego, stałego nadzoru.
- **Zakres uprawnień Policji obecnie:** Obecne przepisy pozwalają Policji przetwarzać tylko dane **niezbędne** do realizacji **konkretnego** zadania. W praktyce może to oznaczać **częściowy dostęp** do nagrań w konkretnej sprawie, ale nie automatycznie stały, szeroki dostęp do obrazu „na bieżąco".
- **Rola samorządu:** Gminy mają ustawowe zadania w zakresie porządku publicznego i bezpieczeństwa oraz uprawnienia do rejestrowania obrazu w przestrzeni publicznej. UODO wskazuje, że tych zadań i uprawnień **nie należy rozszerzać ani przenosić** na Policję poprzez ogólne porozumienia.
- **Ryzyka dla praw obywatelskich:** Szerokie korzystanie z monitoringu przez służby w **niedookreślonych celach** i bez odpowiednich gwarancji może zagrażać m.in. **prawu do prywatności**, **godności**, **równości** i **autonomii informacyjnej**, zwłaszcza gdy pozyskiwanie danych ma charakter niejawny.
- **Biometria i rozpoznawanie twarzy:** Przetwarzanie danych biometrycznych jest dopuszczalne tylko w szczególnych okolicznościach (wskazanych w RODO), a w obszarze ścigania przestępstw tylko wtedy, gdy jest **ściśle niezbędne** do konkretnych celów (zapobieganie, wykrywanie, dochodzenia, ściganie, wykonywanie kar).
- **Wymóg podstawy ustawowej:** Monitoring wykorzystujący biometrię wymaga **jasnej i konkretnej podstawy prawnej rangi ustawy** (nie ogólnych porozumień).
- **Postulat UODO – przygotowanie regulacji:** Prezes UODO wnioskuje o rozpoczęcie prac legislacyjnych, które kompleksowo uregulują:
  - zasady dostępu Policji do monitoringu samorządowego,
  - zasady stosowania monitoringu połączonego z biometrią,
  - warunki, w których takie narzędzia mogą być używane (tylko do zadań ustawowych, w zakresie niezbędnym i adekwatnym).

- **Test prywatności i zgodność z prawem UE:** UODO postuluje, aby przed wprowadzeniem przepisów przeprowadzić **test prywatności** oraz analizę zgodności z prawem europejskim, w tym pod kątem **systemów wysokiego ryzyka** i potencjalnie **zakazanych praktyk**.
- **Dodatkowa kwestia – profilowanie:** UODO zwraca uwagę na ryzyko **profilowania**, czyli zautomatyzowanej analizy danych służącej ocenie cech osoby lub prognozowaniu jej zachowań, co wymaga szczególnej ostrożności i zabezpieczeń.
- **Najważniejszy wniosek:** Potrzebne są jednoznaczne, ustawowe reguły, które pozwolą Policji skutecznie działać, ale jednocześnie zapewnią **proporcjonalność** i **realne gwarancje ochrony danych** oraz praw obywatelskich.

Źródło: https://uodo.gov.pl/pl/138/4606