AURACO

N E W S L E T T E R

OCHRONA DANYCH • CYBERBEZPIECZEŃSTWO • REGULACJE

Wrzesień 2026 – Wyciek u dostawcy, obowiązki po stronie administratora – czego uczy sierpniowy incydent w ochronie zdrowia

SPIS TREŚCI

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

ARTYKUŁ AUTORSKI

Tekst: **Piotr Janiszewski**

Wyciek u dostawcy, obowiązki po stronie administratora – czego uczy sierpniowy incydent w ochronie zdrowia

Sierpień przyniósł zdarzenie, które w polskiej praktyce ochrony danych może stać się punktem odniesienia na lata. Do systemów spółki MyDr, jednego z największych dostawców oprogramowania do prowadzenia elektronicznej dokumentacji medycznej, uzyskano nieuprawniony dostęp. Po spotkaniu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa 12 sierpnia 2026 r. Ministerstwo Cyfryzacji podało, że firma potwierdziła nieuprawniony dostęp do danych historycznych, obejmujących okres do kwietnia 2024 r., i że zdarzenie może dotyczyć 18,8 mln osób oraz ponad 12 tys. placówek medycznych. Dzień później Prezes UODO wszczął kontrolę w spółce.

Zwracam uwagę na sformułowanie „może dotyczyć". Liczba 18 814 422 unikatowych numerów PESEL, która obiegła media, pochodzi z deklaracji samych sprawców, przekazanej redakcji Zaufanej Trzeciej Strony. Podobnie rzecz się ma z rozmiarem skradzionego zbioru i z opisem drogi, którą napastnicy weszli do infrastruktury. To są twierdzenia strony atakującej, a nie ustalenia organu. Piszę o tym na wstępie, bo pierwszym zadaniem inspektora ochrony danych w takiej sytuacji jest oddzielenie tego, co wiadomo, od tego, co ktoś powiedział.

Dlaczego to nie jest historia o cudzej firmie

Łatwo przeczytać ten incydent jako problem jednego dostawcy i jednej branży. Byłby to błąd. Konstrukcja odpowiedzialności w RODO jest tu jednoznaczna: administratorem danych pacjenta pozostaje przychodnia, gabinet, szpital. Spółka dostarczająca oprogramowanie jest podmiotem przetwarzającym. Kiedy więc Urząd Ochrony Danych Osobowych 12 sierpnia 2026 r. przypomniał, że obowiązek powiadomienia osób dotkniętych wyciekiem spoczywa na administratorach korzystających z usług dostawcy, nie było w tym niczego zaskakującego. Zaskakująca była tylko skala, w jakiej ta zasada nagle stała się widoczna.

Każda organizacja, która powierza przetwarzanie danych zewnętrznemu podmiotowi – a więc praktycznie każda – jest w tej samej strukturalnej sytuacji. Kadry w chmurze, system CRM, hosting poczty, firma niszcząca dokumenty, biuro rachunkowe. Jeżeli dostawca zostanie zaatakowany, to my oceniamy ryzyko i to my zgłaszamy naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem dla praw lub wolności. Jeżeli ryzyko okaże się wysokie, to również my zawiadamiamy osoby, których dane dotyczą. Dostawca ma obowiązek nas o zdarzeniu poinformować i pomóc, ale nie może przejąć naszej odpowiedzialności ani jej z nas zdjąć.

Zegar, który rusza nie wtedy, kiedy byśmy chcieli

Artykuł 33 ust. 1 RODO wiąże bieg siedemdziesięciu dwóch godzin ze stwierdzeniem naruszenia przez administratora, a nie z chwilą, w której doszło do włamania u dostawcy. Podmiot przetwarzający zgłasza naruszenie administratorowi po jego stwierdzeniu, bez zbędnej zwłoki, zgodnie z art. 33 ust. 2, a umowa powierzenia zwykle doprecyzowuje termin i zakres tego powiadomienia. W teorii łańcuch jest domknięty. W praktyce sierpień pokazał jego słaby punkt: administrator dowiaduje się z mediów, że jego dostawca został zaatakowany, i przez wiele dni nie otrzymuje potwierdzenia, czy zdarzenie objęto akurat powierzone przez niego dane.

Urząd zajął w tej sprawie stanowisko praktyczne. W opublikowanym 27 sierpnia 2026 r. zestawie odpowiedzi wskazał, że po otrzymaniu od dostawcy potwierdzenia, iż incydent objął dane, których jesteśmy administratorem, należy przeanalizować zdarzenie pod kątem ryzyka naruszenia praw lub wolności osób fizycznych i dokonać zgłoszenia. Urząd dodał też coś, co warto zapamiętać: jeżeli zgłoszenie nastąpi po upływie terminu, trzeba dołączyć wyjaśnienie przyczyn opóźnienia. To zdanie mówi więcej, niż się na pierwszy rzut oka wydaje. W moim odczytaniu organ przyjmuje do wiadomości, że w takich sytuacjach termin bywa przekroczony, i za istotne uznaje udokumentowanie przyczyn opóźnienia.

W mojej ocenie to właśnie dokumentowanie własnych działań jest tu kluczowe. Kiedy nie wiemy jeszcze, czy i co wyciekło, wartość ma zapis tego, kiedy dowiedzieliśmy się o zdarzeniu, o co i kiedy zapytaliśmy dostawcę, jaką odpowiedź otrzymaliśmy i jaką decyzję na jej podstawie podjęliśmy. Rejestr naruszeń z art. 33 ust. 5 nie jest formalnością dla audytora, tylko podstawowym dowodem na to, że organizacja działała rozsądnie w warunkach niepewności.

Ocena ryzyka, gdy nikt nie zna zakresu

Najtrudniejszy moment tego incydentu polega na tym, że przez pewien czas ani administratorzy, ani dostawca nie znali dokładnego zakresu ujawnionych danych. Sama spółka podkreślała, że nie zna dokładnej skali zdarzenia. Administrator ma tymczasem ocenić prawdopodobieństwo i wagę ryzyka dla osób, których dane dotyczą.

Odradzam w takiej sytuacji dwa skrajne odruchy. Pierwszy to czekanie na pełną informację, bo pełna informacja może nie przyjść przez wiele tygodni. Drugi to odnotowanie sprawy wyłącznie w rejestrze wewnętrznym z konkluzją, że skoro nic pewnego nie wiadomo, to ryzyko jest małe. Jak pokazuje omawiany w tym wydaniu wyrok Naczelnego Sądu Administracyjnego z 26 sierpnia 2026 r. (sygn. III OSK 251/24), taka konkluzja bez udokumentowanej analizy jest nie do obrony przed organem.

Rozsądniejsza jest ocena oparta na charakterze zbioru, który powierzyliśmy. Jeżeli dostawca przetwarzał w naszym imieniu numery PESEL wraz z informacjami o świadczeniach zdrowotnych, to znamy najgorszy realistyczny scenariusz nawet wtedy, gdy nie znamy liczby rekordów. Połączenie danych identyfikacyjnych z danymi o zdrowiu daje ryzyko, którego nie da się uznać za mało prawdopodobne. Warto też pamiętać, że przy danych należących do szczególnych kategorii lub numerze PESEL skutki nie ograniczają się do wyłudzeń finansowych, których część ogranicza zastrzeżenie numeru PESEL. Informacja o leczeniu bywa podstawą do nacisku na osobę i ta perspektywa powinna wchodzić do oceny.

Umowa powierzenia jako narzędzie, nie jako załącznik

Sierpień był dobrym testem jakości umów powierzenia. Artykuł 28 ust. 3 lit. f RODO zobowiązuje podmiot przetwarzający do pomocy administratorowi w wywiązaniu się z obowiązków z art. 32–36, w tym z obowiązków zgłoszeniowych. Przepis mówi jednak o pomocy, nie o terminach ani o formie. Te trzeba sobie wynegocjować samemu.

Z mojego doświadczenia wynika, że w umowach najczęściej brakuje trzech rzeczy. Po pierwsze, konkretnego terminu na powiadomienie administratora, liczonego w godzinach od stwierdzenia naruszenia przez dostawcę. Po drugie, minimalnego zakresu informacji w takim powiadomieniu, obejmującego kategorie i przybliżoną liczbę osób oraz rekordów, bo bez tego administrator nie ma z czego zbudować oceny ryzyka. Po trzecie, zobowiązania do przekazywania aktualizacji w miarę postępu analizy, ponieważ pierwsza informacja z natury rzeczy jest niepełna. Kto ma te trzy elementy w umowie, ten w sierpniu miał do kogo napisać i o co się upomnieć.

Warto również sprawdzić coś, co brzmi banalnie: czy wiemy, kto po stronie dostawcy jest adresatem takiego pytania i czy ta osoba nadal tam pracuje. Kontakt ustalony przy podpisywaniu umowy trzy lata temu bywa nieaktualny akurat w tygodniu, w którym jest potrzebny.

Reakcja regulacyjna, która już się zaczęła

31 sierpnia 2026 r. Ministerstwo Cyfryzacji przedstawiło pakiet propozycji legislacyjnych nazwany „Cyber Piątką". Wiceminister Dariusz Standerski ujął jego założenie tak: „Pogoń za zyskiem czy brzmienie umowy między prywatnymi podmiotami nie może być usprawiedliwieniem dla zaniedbań w cyberbezpieczeństwie". Propozycje obejmują certyfikację podmiotów przetwarzających dane medyczne, minimalne wymagania technologiczne dla systemów przetwarzających takie dane, obowiązek informowania pacjenta o powierzeniu jego danych podmiotom zewnętrznym, powiadomienia o zdarzeniach medycznych w aplikacjach mObywatel i mojeIKP oraz dodatkowe obowiązki dla podmiotów przetwarzających dane na dużą skalę, zdefiniowanych jako świadczące usługi dla ponad stu administratorów albo przetwarzające dane łącznie ponad stu tysięcy osób.

To na razie zapowiedzi, a nie obowiązujące przepisy, i będę je oceniał, kiedy pojawią się projekty. Jedna rzecz zwraca jednak uwagę już teraz. Próg „ponad stu administratorów albo ponad stu tysięcy osób" wprowadza do polskiego porządku kategorię dostawcy systemowo istotnego, która w RODO nie istnieje. Rozporządzenie różnicuje obowiązki według ryzyka konkretnego przetwarzania, nie według liczby obsługiwanych klientów. Kierunek uważam za trafny, bo koncentracja rynku realnie zmienia skalę skutków pojedynczego włamania. Rozstrzygające będzie jednak to, jak te nowe obowiązki zostaną zestrojone z art. 28 RODO i z wymaganiami, które ci sami dostawcy mają już z ustawy o krajowym systemie cyberbezpieczeństwa.

Co zrobiłbym we wrześniu

Gdybym miał wskazać jedno działanie na wrzesień, byłby to przegląd rejestru czynności pod kątem pytania, którzy dostawcy przetwarzają w naszym imieniu dane szczególnych kategorii lub numery PESEL na dużą skalę. Nie chodzi o pełny audyt, tylko o listę podmiotów, przy których incydent oznaczałby dla nas obowiązek zawiadomienia osób. Przy każdej takiej pozycji warto sprawdzić dwie rzeczy: czy umowa powierzenia określa termin i zakres powiadomienia o naruszeniu oraz czy mamy aktualny kanał kontaktu.

Sierpniowy incydent nie postawił przed administratorami nowych obowiązków. Pokazał tylko, jak wyglądają te istniejące, kiedy trzeba je wykonać naprawdę, pod presją czasu i przy niepełnych informacjach. To dobry moment, by sprawdzić własne przygotowanie, zanim sprawdzi je zdarzenie.

PRZEGLĄD NEWSÓW

Przegląd newsów

Sierpień 2026 r. był w Brukseli i w Warszawie miesiącem umiarkowanego tempa legislacyjnego, ale przyniósł kilka rozstrzygnięć o realnym znaczeniu dla organizacji. Komisja Europejska objęła obowiązkami dla największych platform trzy kolejne usługi, w tym po raz pierwszy asystenta opartego na modelu językowym. Prezes UODO zajął stanowisko w sprawie urządzeń noszonych rejestrujących obraz i dźwięk, a także kontynuował spór z resortem spraw wewnętrznych o dane biometryczne funkcjonariuszy. Do resortu zdrowia trafiło również wystąpienie organu o doprecyzowanie przepisów o monitoringu w izbach wytrzeźwień.

Komisja Europejska wyznaczyła ChatGPT, Reddit i Roblox jako bardzo duże usługi cyfrowe (31.08.2026)

Komisja Europejska wyznaczyła 31 sierpnia 2026 r. ChatGPT jako bardzo dużą wyszukiwarkę internetową (VLOSE) oraz Reddit i Roblox jako bardzo duże platformy internetowe (VLOP) w rozumieniu aktu o usługach cyfrowych. Podstawą były oświadczenia samych usług o osiąganiu co najmniej 45 mln średnich miesięcznych użytkowników w Unii Europejskiej, czyli progu wyznaczonego rozporządzeniem. Od notyfikacji decyzji usługi mają cztery miesiące, to jest czas do stycznia 2027 r., na wdrożenie dodatkowych obowiązków. Obejmują one ocenę i ograniczanie ryzyk systemowych wynikających z usługi i jej systemów algorytmicznych, odnoszących się do rozpowszechniania nielegalnych treści, negatywnego wpływu na małoletnich, dobrostanu fizycznego i psychicznego użytkowników, praw podstawowych, procesów wyborczych oraz bezpieczeństwa publicznego.

W naszej ocenie najciekawsza jest kwalifikacja ChatGPT jako wyszukiwarki, a nie platformy. Przesądza o niej funkcja przeszukiwania sieci, a nie sam charakter modelu językowego, i pokazuje, że kategorie z aktu o usługach cyfrowych będą stosowane do usług AI według realizowanej funkcji. Dla organizacji korzystających z takich narzędzi w pracy oznacza to, że po upływie okresu przejściowego usługi te będą musiały udostępnić mechanizmy przewidziane dla największych platform, w tym zgłaszanie nielegalnych treści, uzasadnianie decyzji moderacyjnych oraz publikowanie ocen ryzyka systemowego.

Źródło: Komunikat Komisji Europejskiej

Prezes UODO ostrzega przed inteligentnymi okularami (13.08.2026)

Prezes UODO Mirosław Wróblewski zwrócił uwagę na ryzyka związane z okularami wyposażonymi w miniaturowe urządzenia rejestrujące obraz i dźwięk, łączące się z siecią i coraz częściej współpracujące z systemami sztucznej inteligencji. Urząd przypomniał, że przetwarzanie danych w celach innych niż osobiste lub domowe podlega co do zasady RODO, a odpowiedzialność za gromadzenie i rozpowszechnianie nagrań spoczywa na użytkowniku sprzętu, stosownie do jego roli w tym przetwarzaniu. Wśród wskazanych zagrożeń znalazły się nagrywanie bez wiedzy osób w otoczeniu, poczucie stałej kontroli, przekazywanie danych do państw trzecich niezapewniających odpowiedniego poziomu ochrony oraz łączenie nagrań z innymi informacjami przez narzędzia sztucznej inteligencji. Urząd powołał się na badania francuskiego ogranu ochrony danych, według których ryzyko dla prywatności dostrzega 67 proc. badanych.

Zalecenia obejmują zapoznanie się z zasadami przetwarzania danych przez urządzenie, ograniczenie uprawnień i powiązań z aplikacjami, wyłączanie kamery i mikrofonu poza użyciem, informowanie osób w pobliżu o nagrywaniu oraz powstrzymanie się od korzystania z takich urządzeń w miejscach wymagających wysokiego stopnia prywatności, w tym w gabinetach lekarskich i szkołach. Rekomendujemy uwzględnienie tej kategorii sprzętu w regulaminach pracy i politykach dotyczących urządzeń prywatnych. Dotychczasowe zapisy o zakazie nagrywania zwykle odnoszą się do telefonów i nie obejmują wprost urządzeń, których funkcja rejestrowania nie jest widoczna dla otoczenia.

Źródło: Komunikat UODO

MSWiA odpowiada Prezesowi UODO w sprawie danych biometrycznych funkcjonariuszy (12.08.2026)

Ministerstwo Spraw Wewnętrznych i Administracji odniosło się do lipcowego wystąpienia Prezesa UODO dotyczącego modelu retencji odcisków palców i wymazów z jamy ustnej pobieranych od funkcjonariuszy i pracowników Policji. Organ nadzorczy kwestionował uregulowanie istotnych elementów w rozporządzeniu zamiast w ustawie, sztywny pięcioletni okres przechowywania danych po zakończeniu służby oraz zgodność takiego rozwiązania ze standardem „bezwzględnej konieczności" wynikającym z zasady minimalizacji.

Resort odpowiedział, że art. 20 ust. 1l ustawy o Policji nie tworzy generalnego uprawnienia do pobierania danych od wszystkich funkcjonariuszy, lecz obejmuje wyłącznie osoby wykonujące czynności służbowe związane z ujawnianiem, zabezpieczaniem i badaniem śladów. Celem jest odróżnienie śladów pozostawionych legalnie w toku czynności od śladów innych osób, co ma chronić wartość dowodową materiału. Zdaniem ministerstwa ustawa określa kwestie zasadnicze, a nie każdy aspekt techniczny musi być uregulowany na poziomie ustawowym; pięcioletni okres uzasadniono ciągłością czynności wykrywczych i procesowych. Resort zadeklarował jednocześnie, że prowadzi analizę zgłoszonych wątpliwości pod kątem zasadności zmian legislacyjnych.

Spór ma znaczenie wykraczające poza służby. Dotyczy pytania, jak głęboko ustawa musi regulować przetwarzanie danych biometrycznych pracowników, gdy podstawą jest realizacja zadania publicznego. Będziemy śledzić wynik analizy resortu.

Źródło: Komunikat UODO

Monitoring w izbach wytrzeźwień wymaga doprecyzowania przepisów (11.08.2026)

Do ministry zdrowia Jolanty Sobierańskiej-Grendy trafiło wystąpienie Prezesa UODO o doprecyzowanie przepisów ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi w zakresie monitoringu w izbach wytrzeźwień. Obowiązujące regulacje nie rozstrzygają wprost, czy dopuszczalne jest wyłączenie rejestrowanie obrazu, czy również dźwięku. Zdaniem organu utrwalanie dźwięku w pomieszczeniach izolacyjnych jest działaniem nadmiarowym, a obecne przepisy nie stanowią dla niego dostatecznej podstawy prawnej. Wątpliwości zgłaszają organowi także same izby wytrzeźwień jako administratorzy.

Urząd przypomniał przy tej okazji regułę o szerszym zastosowaniu: podstawa prawna monitoringu prowadzonego przez podmiot publiczny musi precyzyjnie określać granice ingerencji w autonomię informacyjną, wynikającą z art. 47 i art. 51 Konstytucji RP. Wskazał również na drugą stronę zagadnienia, jaką jest rola nagrań w przeciwdziałaniu nieludzkiemu traktowaniu. Zapisy z monitoringu w miejscach odosobnienia, w tym w izbach wytrzeźwień, od lat analizują eksperci Krajowego Mechanizmu Prewencji Tortur działającego przy Biurze RPO.

Źródło: Komunikat UODO

ORZECZENIA I DECYZJE

Decyzje i orzeczenia

Sierpień 2026 r. przyniósł rozstrzygnięcia dotyczące dwóch fundamentów systemu ochrony danych: udziału człowieka w decyzjach dotyczących ludzi oraz niezależności osoby, która ma w organizacji pilnować zgodności. Holenderski organ nadzorczy nałożył na Ubera jedną z najwyższych kar w historii stosowania RODO za automatyczne blokowanie kont kierowców, a Prezes UODO ukarał administratora, który przez pięć lat sam pełnił u siebie funkcję inspektora ochrony danych. Naczelny Sąd Administracyjny rozstrzygnął z kolei spór o to, czy ujawnienie numeru PESEL wraz z danymi adresowymi rodzi obowiązek zgłoszenia naruszenia. Trybunał Sprawiedliwości Unii Europejskiej pozostawał w okresie wakacji sądowych, dlatego w tym wydaniu nie omawiamy jego orzeczeń.

Holandia: kara 824 990 000 euro nałożona na Ubera za w pełni zautomatyzowane blokowanie kont kierowców (21.08.2026)

- **Organ**: Autoriteit Persoonsgegevens (holenderski organ ochrony danych) jako organ wiodący, przy ścisłej współpracy z francuską CNIL
- **Podmioty**: Uber B.V. z siedzibą w Amsterdamie oraz Uber Technologies Inc. z siedzibą w San Francisco
- **Kara/nakaz**: administracyjna kara pieniężna w wysokości 824 990 000 euro; spółka wniosła odwołanie, rozstrzygnięcie nie jest prawomocne
- **Istota**: Uber wykorzystywał oprogramowanie śledzące sposób jazdy kierowców oraz oceny wystawiane przez klientów. Gdy system wykrył podejrzenie oszustwa, konto kierowcy było automatycznie dezaktywowane czasowo; przy utrzymujących się niskich ocenach dochodziło do dezaktywacji trwałej. Organ ustalił, że w procesie nie występowała żadna ocena dokonywana przez człowieka, a praktyka trwała w latach 2018–2022. Skutkiem dezaktywacji była utrata możliwości zarobkowania za pośrednictwem platformy. Autoriteit Persoonsgegevens stwierdził naruszenie zakazu podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, wywołujących istotne skutki dla osoby, oraz odrębnie naruszenie obowiązku poinformowania kierowców o automatycznym charakterze tych decyzji. Postępowanie zainicjowało zgłoszenie 171 francuskich kierowców do organizacji Ligue des droits de l'Homme, która złożyła skargę do CNIL; sprawę przejął organ holenderski jako właściwy dla europejskiej siedziby grupy w mechanizmie kompleksowej współpracy. Wysokość kary odniesiono do globalnego obrotu spółki wynoszącego około 44,5 mld euro w 2025 r. Spółka zaprzestała kwestionowanej praktyki. Jest to czwarta kara nałożona na Ubera przez organ holenderski: po 600 tys. euro w 2018 r., 10 mln euro w 2023 r. oraz 290 mln euro w 2024 r. za przekazywanie danych kierowców do Stanów Zjednoczonych.
- **Znaczenie dla praktyki**: Rozstrzygnięcie pokazuje, że o zakwalifikowaniu procesu jako decyzji zautomatyzowanej przesądza faktyczny brak udziału człowieka, a nie nazwa procedury ani deklaracja w dokumentacji. W naszej ocenie warto na tym tle przejrzeć własne procesy, w których system samodzielnie ogranicza komuś dostęp do usługi lub świadczenia: blokady kont, automatyczne odrzucenia wniosków, algorytmy antyfraudowe i narzędzia scoringowe. Rekomendujemy sprawdzenie trzech rzeczy. Po pierwsze, czy przewidziana interwencja człowieka jest realna, to znaczy czy osoba ją wykonująca ma kompetencje i faktyczną możliwość zmiany rozstrzygnięcia, a nie wyłącznie zatwierdza wynik systemu. Po drugie, czy osoby objęte takim procesem są o jego automatycznym charakterze informowane, ponieważ organ potraktował ten brak jako odrębne naruszenie. Po trzecie, czy istnieje udokumentowana ścieżka odwoławcza. Warto przy tym pamiętać, że jeżeli taki proces opiera się na systemie sztucznej inteligencji, obowiązki z RODO nakładają się na wymagania AI Act, a od 28 października 2026 r. egzekwowaniem tych drugich zajmie się w Polsce odrębny organ.
- **Źródło**: Komunikat Autoriteit Persoonsgegevens
- **Źródło**: Komunikat CNIL

Kara 15 500 zł za brak niezależności inspektora i niezawiadomienie organu o jego wyznaczeniu (komunikat z 31.08.2026)

- **Organ**: Prezes Urzędu Ochrony Danych Osobowych
- **Podmiot**: komornik sądowy prowadzący kancelarię, występujący jako administrator danych
- **Kara/nakaz**: administracyjna kara pieniężna w łącznej wysokości 15 500 zł, na którą składa się 3,5 tys. zł za niezawiadomienie organu nadzorczego o wyznaczeniu inspektora w terminie 14 dni oraz 12 tys. zł za niezapewnienie inspektorowi statusu gwarantującego niezależność (sygn. DKN.5131.24.2025, decyzja nieprawomocna)
- **Istota**: Sprawa wyszła na jaw przy okazji weryfikacji zgłoszenia naruszenia polegającego na wysłaniu pisma o zajęciu rachunku bankowego do osoby niebędącej właścicwym adresatem. Przy sprawdzaniu formularza organ ustalił, że administrator przez pięć lat sam pełnił w swojej kancelarii funkcję inspektora ochrony danych, przyjmując, że takie rozwiązanie nie powoduje konfliktu interesów, oraz że nie dokonał obowiązkowego zawiadomienia Prezesa UODO o wyznaczeniu inspektora. Organ przypomniał, że inspektor może wykonywać inne zadania wyłącznie wtedy, gdy nie powodują one konfliktu interesów, a łączenie obu ról prowadzi do sytuacji, w której inspektor zgłasza uwagi administratorowi, czyli samemu sobie. Prezes UODO powołał wcześniejsze stanowiska, zgodnie z którymi „niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem, (zarządzającym) podmiotem, posiadającym status administratora lub podmiotu przetwarzającego, takich jak np. członka zarządu stowarzyszenia, dyrektora szkoły, wójta, członka zarządu spółki". Organ uznał, że upomnienie byłoby nieproporcjonalne: komornik sądowy jako funkcjonariusz publiczny i profesjonalista podlega ponadprzeciętnemu standardowi staranności, a decyzja o powierzeniu funkcji samemu sobie była świadoma i miała przynieść oszczędność.
- **Znaczenie dla praktyki**: To rzadki przypadek, w którym organ nadzorczy karze nie za skutek w postaci wycieku, lecz za konstrukcję funkcji inspektora. Zalecamy sprawdzenie w organizacji dwóch kwestii formalnych i jednej merytorycznej. Formalne to zawiadomienie Prezesa UODO o wyznaczeniu inspektora oraz publikacja jego danych kontaktowych; obie bywają pomijane przy zmianie osoby na stanowisku. Merytoryczna dotyczy zakresu pozostałych obowiązków inspektora. Zbieżnie wypowiedział się francuski organ ochrony danych, który 10 sierpnia 2026 r. opublikował wskazówki dotyczące identyfikowania i usuwania konfliktu interesów. CNIL zaleca przeprowadzenie analizy jeszcze przed wyznaczeniem inspektora lub przed powierzeniem mu nowych zadań i wskazuje, że funkcje kierownicze wyższego szczebla są z reguły nie do pogodzenia z rolą inspektora, podobnie jak każda rola pozwalająca współdecydować o celach i sposobach przetwarzania. Wśród środków naprawczych francuski organ wymienia odebranie zadań powodujących konflikt oraz wyznaczenie zastępcy inspektora dla obszaru objętego konfliktem, zastrzegając, że takie wyłączenie nie może być czynnością wyłącznie formalną. Zwracamy uwagę, że stanowiska obu organów są zbieżne również w odniesieniu do inspektorów zewnętrznych i współdzielonych między podmiotami.
- **Źródło**: Komunikat UODO
- **Źródło**: Wskazówki CNIL dotyczące konfliktu interesów inspektora

NSA: ujawnienie numeru PESEL z danymi adresowymi rodzi obowiązek zgłoszenia naruszenia (wyrok z 26.08.2026, sygn. III OSK 251/24)

- **Organ**: Naczelny Sąd Administracyjny, po skardze kasacyjnej Prezesa UODO
- **Podmiot**: spółdzielnia mieszkaniowa jako administrator danych
- **Kara/nakaz**: utrzymana administracyjna kara pieniężna w wysokości niemal 52 tys. zł oraz nakaz zawiadomienia osoby, której dane dotyczą (wyrok z 26 sierpnia 2026 r., sygn. III OSK 251/24)
- **Istota**: Podczas konferencji prasowej administrator udostępnił osobie nieuprawnionej informacje o sporze z członkiem spółdzielni, w tym kserokopię zawiadomienia o podejrzeniu popełnienia przestępstwa wraz z imieniem, nazwiskiem, numerem PESEL i adresem zamieszkania. Postępowanie wszczęto z urzędu po tym, jak do Urzędu wpłynęła wiadomość od osoby, której te informacje udostępniono. Administrator odnotował zdarzenie w wewnętrznym rejestrze naruszeń i uznał ryzyko za niskie, nie zgłosił go jednak organowi nadzorczemu i nie zawiadomił osoby, której dotyczyło. Wojewódzki Sąd Administracyjny w Warszawie uchylił decyzję Prezesa UODO, uznając, że organ nie przedstawił przekonujących argumentów za wystąpieniem ryzyka wyższego niż małe, a także kwestionując zakwalifikowanie spółdzielni jako przedsiębiorcy. Naczelny Sąd Administracyjny uchylił ten wyrok i oddalił skargę administratora, podzielając w całości argumentację skargi kasacyjnej. Sąd przyjął, że organ wykazał w uzasadnieniu, dlaczego ujawnienie numeru PESEL wraz z imieniem, nazwiskiem i adresem zamieszkania stanowi wysokie ryzyko naruszenia praw i wolności osoby fizycznej, oraz że spółdzielnia mieszkaniowa jest „przedsiębiorcą" w rozumieniu art. 83 ust. 4 RODO, co przesądza o sposobie wyliczenia kary.
- **Znaczenie dla praktyki**: Wyrok wzmacnia dwie tezy o szerokim zastosowaniu. Pierwsza dotyczy oceny ryzyka: organ i sąd oczekują, że administrator będzie potrafił przedstawić analizę, a nie samo twierdzenie, że ryzyko jest małe. Prezes UODO podkreślił przy tym, że analiza ma uwzględniać zagrożenia dla osoby, której dane dotyczą, a nie interesy administratora, a w tej sprawie administrator nie był w stanie przedstawić takiej analizy. Druga teza ma znaczenie dla podmiotów, które nie postrzegają się jako przedsiębiorcy. Wyrok zapadł w sprawie spółdzielni mieszkaniowej, ale dla wspólnot i organizacji członkowskich stanowi wskazówkę, że kara może zostać wyliczona według zasad przewidzianych dla przedsiębiorstw; każdorazowo wymaga to jednak odrębnej oceny. Rekomendujemy przegląd wewnętrznych rejestrów naruszeń pod kątem zdarzeń zamkniętych wpisem bez udokumentowanej analizy ryzyka. Zestaw danych obejmujący numer PESEL i adres zamieszkania warto traktować jako przypadek, w którym rezygnacja ze zgłoszenia wymaga szczególnie starannego uzasadnienia.
- **Źródło**: Komunikat UODO o wyroku
- **Źródło**: Pierwotna decyzja Prezesa UODO

Upomnienie dla Prezydenta Wejherowa: wniosek o informację publiczną to nie postępowanie administracyjne (komunikat z 24.08.2026)

- **Organ**: Prezes Urzędu Ochrony Danych Osobowych
- **Podmiot**: Prezydent Wejherowa jako administrator danych
- **Kara/nakaz**: upomnienie
- **Istota**: Mieszkaniec złożył wniosek o dostęp do informacji publicznej dotyczącej umów zawartych przez samorząd z określoną firmą oraz skanów faktur. Właściciel tej firmy złożył odrębny wniosek, pytając, czy i komu urząd udzielał informacji w jego sprawie. Prezydent uznał, że skoro sprawa dotyczy więcej niż jednego wnioskodawcy, należy prowadzić ją w jednym postępowaniu według Kodeksu postępowania administracyjnego, i przekazał przedsiębiorcy odpowiedź wraz z danymi osobowymi mieszkańca, bez anonimizacji. Prezes UODO wskazał, że procedura rozpatrzenia wniosku o dostęp do informacji publicznej nie jest postępowaniem administracyjnym w rozumieniu KPA, lecz odrębną procedurą o charakterze informacyjnym. Złożenie dwóch lub więcej wniosków, nawet o tożsamym zakresie, nie prowadzi do jednej wspólnej procedury; każdy wniosek podlega samodzielnemu rozpatrzeniu. Skutkiem błędnej kwalifikacji było udostępnienie danych bez podstawy prawnej i naruszenie zasady poufności.
- **Znaczenie dla praktyki**: Sprawa jest istotna dla wszystkich podmiotów zobowiązanych do udostępniania informacji publicznej, a więc dla jednostek samorządu, instytucji kultury oraz spółek komunalnych. Warto zweryfikować, czy w organizacji obowiązuje procedura anonimizacji danych wnioskodawcy przed przekazaniem korespondencji podmiotom trzecim oraz czy wnioski o informację publiczną nie są rutynowo włączane do akt postępowań administracyjnych. Dobrym rozwiązaniem jest rozdzielenie rejestrów obu rodzajów spraw, ponieważ to właśnie ich połączenie doprowadziło w tym przypadku do ujawnienia danych.
- **Źródło**: Komunikat UODO

NIS2

NIS2 – co nowego

CERT Polska uzupełnia raport o grudniowym ataku na sektor energii: prywatny APN jako ścieżka do sieci przemysłowej

Ministerstwo Cyfryzacji opublikowało 8 sierpnia 2026 r. raport uzupełniający CERT Polska dotyczący skoordynowanych ataków na infrastrukturę sektora energii z 29 grudnia 2025 r. Pierwotny raport ze stycznia 2026 r. opisywał uderzenie w około trzydzieści obiektów wykorzystujących odnawialne źródła energii oraz w dużą elektrociepłownię. Dokument uzupełniający dotyczy drugiej elektrociepłowni i szczegółowo przedstawia działania napastnika w środowisku technologicznym.

Najważniejsze ustalenie dotyczy wykorzystania prywatnego APN, czyli konfiguracji określającej, do jakiej sieci w infrastrukturze operatora komórkowego podłącza się urządzenie. CERT Polska opisuje go jako element ścieżki ataku, obok rekonesansu sieci przemysłowej, działań wymierzonych w urządzenia firmy Moxa oraz ataku na sterowniki PLC firmy Siemens. Raport zawiera także chronologię rozpoznania, kompromitacji infrastruktury i zacierania śladów przez napastnika.

Zalecenia zespołu są konkretne i w naszej ocenie warte przełożenia na listę zadań wszędzie tam, gdzie prywatny APN zapewnia dostęp do środowiska przemysłowego lub sąsiaduje z siecią OT. CERT Polska rekomenduje przeprowadzenie audytu konfiguracji takiej sieci, a przede wszystkim traktowanie prywatnego APN jako sieci niezaufanej względem środowiska OT. Dalsze zalecenia obejmują ścisłe ograniczenie komunikacji między siecią przemysłową a urządzeniem pełniącym funkcję bramy do APN, monitorowanie ruchu na tym styku, centralne logowanie i monitorowanie zdarzeń, ograniczenie liczby otwartych portów dostępnych z APN do niezbędnego minimum oraz objęcie prywatnych APN i urządzeń dostępowych testami penetracyjnymi. Zwracamy uwagę, że prywatny APN bywa w organizacjach postrzegany jako rozwiązanie z natury bezpieczne, ponieważ nie jest publicznym internetem. Raport pokazuje, dlaczego to założenie jest ryzykowne.

Źródło: Raport uzupełniający CERT Polska

Dostawcy wysokiego ryzyka: procedura istnieje, listy nie ma, obowiązek oceny pozostaje

Ministerstwo Cyfryzacji przypomniało 6 sierpnia 2026 r. zasady postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na gruncie ustawy o krajowym systemie cyberbezpieczeństwa. Komunikat zawiera informację, która porządkuje wiele nieporozumień rynkowych: do tej pory nie wszczęto żadnego postępowania w tej sprawie ani nie wydano decyzji uznającej któregokolwiek dostawcę za dostawcę wysokiego ryzyka.

Sama procedura prowadzona jest przez ministra cyfryzacji w trybie postępowania administracyjnego. Po wszczęciu minister zawiadamia dostawcę i publikuje informację w Biuletynie Informacji Publicznej, a organizacje społeczne mają czternaście dni na przedstawienie stanowiska. Przed wydaniem decyzji zasięgana jest opinia Kolegium do Spraw Cyberbezpieczeństwa, które ma na nią trzy miesiące, a minister publikuje raport w BIP. Decyzja obejmuje wyłącznie wskazane w niej typy produktów, rodzaje usług lub procesów ICT, a nie całą działalność dostawcy, podlega natychmiastowemu wykonaniu i jest ogłaszana w „Monitorze Polskim". Podmioty objęte ustawą nie mogą wówczas wprowadzać wskazanych rozwiązań do użytkowania, a już używane muszą wycofać w terminie do siedmiu lat od ogłoszenia decyzji; dla określonych przedsiębiorców komunikacji elektronicznej termin ten wynosi cztery lata.

Ministerstwo wyraźnie zaznacza, że brak listy nie zwalnia podmiotów z obowiązku oceny ryzyka przy zakupie produktów, usług i procesów ICT. Przypominamy w tym kontekście o powiązaniu z zamówieniami publicznymi: zgodnie z art. 226 ust. 1 pkt 17 Prawa zamówień publicznych zamawiający ma obowiązek odrzucić ofertę dotyczącą rozwiązań objętych rekomendacjami wydanymi w trybie art. 33 ustawy o krajowym systemie cyberbezpieczeństwa. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa mają więc bezpośredni skutek proceduralny, niezależnie od tego, że żadnej decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka dotąd nie wydano. Jedna z takich rekomendacji, dotycząca krytycznych podatności w oprogramowaniu WordPress, została wydana 5 sierpnia 2026 r.

Źródło: Komunikat Ministerstwa Cyfryzacji

Wrzesień i październik: raportowanie z aktu o cyberodporności oraz zamknięcie samorejestracji w Wykazie KSC

We wrześniu i październiku 2026 r. zbiegają się dwa terminy,