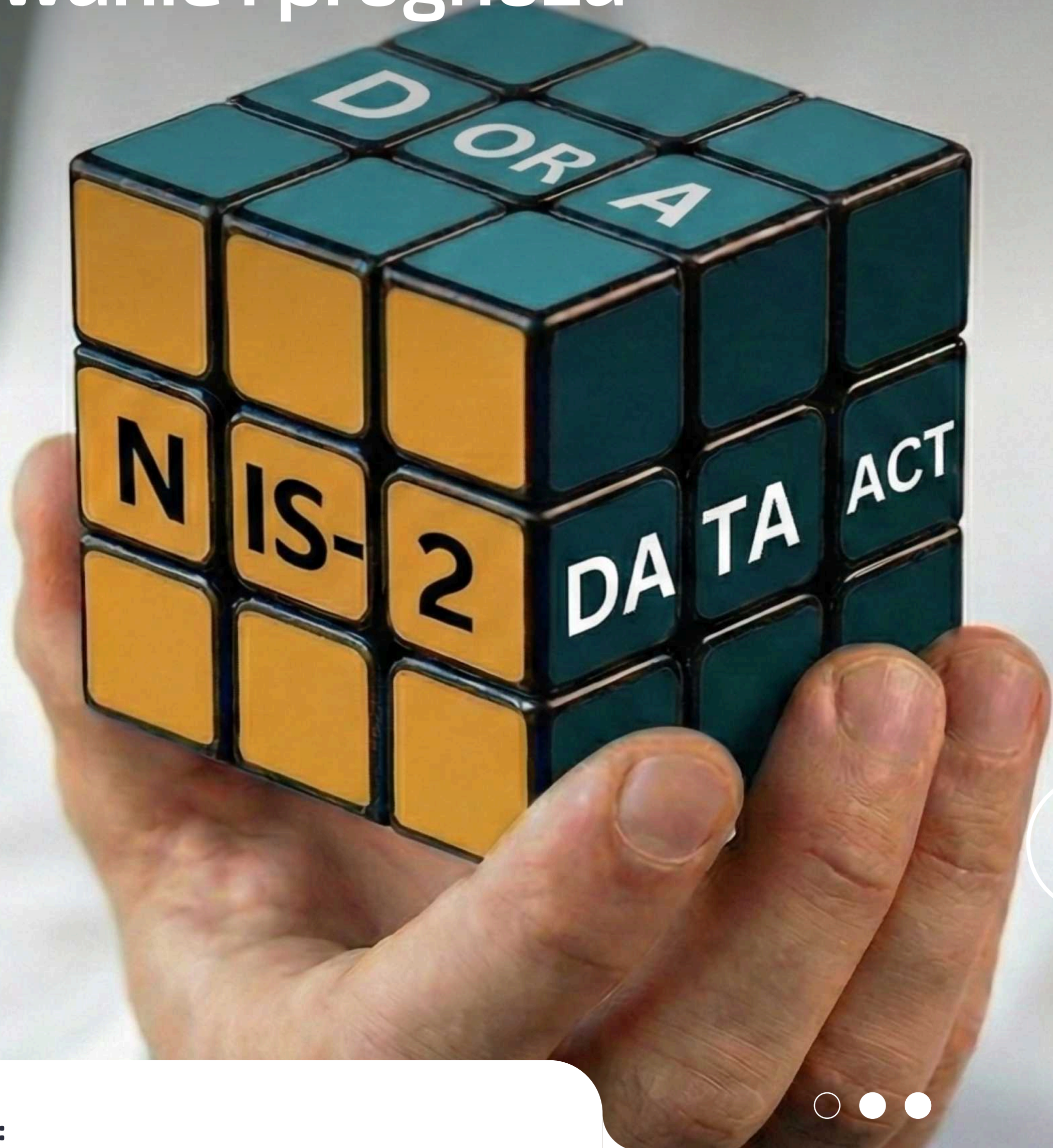


Rok 2025 w ochronie danych osobowych podsumowanie i prognoza



W TYM WYDANIU:

Przegląd zmian prawnych	1
Przegląd decyzji UODO	4
Wnioski na 2026	10



Patrycja Żarska-Cynk
Data Protection Expert

Rok 2025 w ochronie danych osobowych

Podsumowanie i prognoza

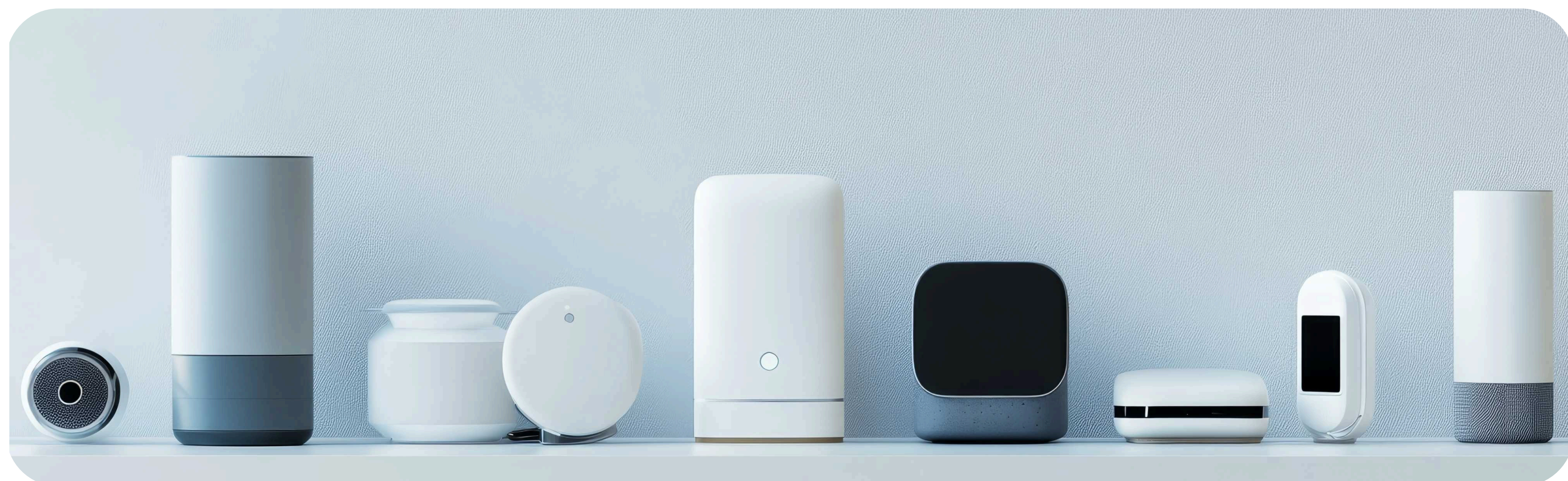
Rok 2025 był przełomowym okresem dla ochrony danych osobowych w Polsce i całej Unii Europejskiej. **Nowa fala regulacji cyfrowych (w tym Data Act, DORA, AI Act oraz dyrektywa NIS 2) gruntownie przeformułuje otoczenie prawne, w którym działają polscy przedsiębiorcy.** Dla firm, niezależnie od ich wielkości, oznacza to konieczność nie tylko dostosowania się do nowych przepisów, ale także strategicznego przemyślenia, jak zarządzać danymi i cyberbezpieczeństwem.

Niniejszy artykuł stanowi merytoryczne podsumowanie kluczowych zmian, które miały

miejsce w 2025 roku, oraz wskazuje na najważniejsze wyzwania i obszary, na które organizacje powinny położyć szczególny nacisk w nadchodzącym 2026 roku.

Przegląd zmian prawnych

Krajobraz regulacyjny w Unii Europejskiej uległ w 2025 roku znaczącym zmianom. Tabela na następnej stronie przedstawia status kluczowych aktów prawnych, które weszły w życie lub są w trakcie wdrażania, wraz z głównymi implikacjami dla przedsiębiorców.



Regulacja	Status	Data wejścia w życie	Implikacje dla organizacji
Data Act	✓ Obowiązuje	12 września 2025 r.	Konieczność umożliwienia użytkownikom dostępu do danych generowanych przez inteligentne urządzenia (IoT). Wymaga to zmian w umowach, procedurach operacyjnych i potencjalnie w projektowaniu produktów. Przykład: producent inteligentnych pralek musi zapewnić klientowi dostęp do danych o zużyciu wody i energii.
DORA	✓ Obowiązuje	17 stycznia 2025 r.	Sektor finansowy i jego kluczowi dostawcy ICT muszą wykazać cyfrową odporność operacyjną. Wymaga to rygorystycznego zarządzania ryzykiem, a także testowania i przeglądu umów z dostawcami. Przykład: bank musi regularnie testować swoje systemy pod kątem odporności na cyberataki i weryfikować zabezpieczenia stosowane przez dostawcę chmury.
AI Act	✓ Częściowo obowiązuje	Od 1 sierpnia 2024 r., przepisy zakazujące od lutego 2025 r.	Wprowadzenie zakazów stosowania niebezpiecznych praktyk w systemach AI. Wymaga klasyfikacji ryzyka dla wszystkich systemów AI, zapewnienia dokumentacji technicznej i transparentności. Przykład: systemy AI do analizy CV / dopasowania kandydatów są dozwolone, ale są to systemy wysokiego ryzyka i wymagają wdrożenia pełnego systemu zarządzania ryzykiem, oceny zgodności, nadzoru człowieka i logowania zdarzeń.
NIS-2	⌚ W trakcie wdrażania	Termin transpozycji: 17 października 2024 r. (Polska opóźniona)	Organizacje z kluczowych sektorów (energia, transport, zdrowie, bankowość, infrastruktura cyfrowa) muszą przygotować się na nowe, bardziej rygorystyczne obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa i zgłaszania incydentów. Przykład: firma kurierska będzie musiała wdrożyć zaawansowane środki ochrony swoich systemów logistycznych i zgłaszać poważne incydenty do odpowiednich organów.



Data Act

To **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854** z 22 listopada 2023 r. w sprawie sprawiedliwego dostępu do danych i ich wykorzystania (ang. Data Act), obowiązujące bezpośrednio od 12 września 2025 r. we wszystkich państwach UE. Akt wprowadził prawo użytkowników do dostępu do danych generowanych przez inteligentne urządzenia. **Dla przedsiębiorców oznacza to konieczność wdrożenia mechanizmów umożliwiających realizację tych praw, przeglądu umów z klientami oraz dostosowania procedur operacyjnych.** W Polsce nie wdrożono jeszcze ustawy dostosowującej porządek prawny do Data Act,

ale Ministerstwo Cyfryzacji prowadzi prace nad projektem ustawy o sprawiedliwym dostępie do danych i ich wykorzystywaniu. Projekt określa kompetencje Prezesa Urzędu Komunikacji Elektronicznej (PUKE) jako organu nadzorczego, procedury administracyjne, katalog naruszeń oraz kary pieniężne za nieprzestrzeganie Data Act; konsultacje publiczne trwały do 3 grudnia 2025 r., z planowanym przyjęciem przez Radę Ministrów w IV kw. 2025 r. Ustawa uzupełnia rozporządzenie o krajowe mechanizmy egzekucji, bez wprowadzania nowych obowiązków – Data Act stosuje się bezpośrednio od 12 września 2025 r.

DORA (ang. Digital Operational Resilience Act)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego, obowiązujące bezpośrednio od 17 stycznia 2025 r. we wszystkich państwach UE. DORA stosuje się bezpośrednio we wszystkich państwach członkowskich UE, bez potrzeby transpozycji jak w przypadku dyrektyw. Polska opracowała ustawę zmieniającą ustawy sektorowe (np. Prawo bankowe, ustawę o usługach płatniczych) w związku z zapewnieniem operacyjnej odporności cyfrowej

sektora finansowego dostosowująca polski porządek prawny do rozporządzenia DORA. Weszła ona w życie 7 sierpnia 2025 r., z vacatio legis trwającym jeden dzień, co umożliwiło Komisji Nadzoru Finansowego (KNF) bezpośredni nadzór i nakładanie kar za naruszenia. **Instytucje finansowe musiały dokonać kompleksowego przeglądu umów z dostawcami usług ICT, wdrożyć testy odporności oraz ustanowić procedury zarządzania ryzykiem operacyjnym.** Dla sektora finansowego rok 2025 był rokiem intensywnych przygotowań i wdrażania.

AI Act

To **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689** z 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (ang. Artificial Intelligence Act), opublikowane 12 lipca 2024 r. i obowiązujące od 2 sierpnia 2024 r., z fazowanym wdrożeniem. Już od lutego 2025 r. zaczęły obowiązywać zakazy dotyczące niektórych, szczególnie niebezpiecznych systemów AI. **Przedsiębiorcy wykorzystujący lub tworzący systemy AI musieli dokonać ich klasyfikacji pod**

kątem ryzyka, by w przyszłości sprostać wymogom AI Act i zapewnić odpowiednią dokumentację techniczną oraz transparentność działania.

W Polsce nie wdrożono jeszcze ustawy dostosowującej porządek prawny do rozporządzenia AI Act (UE), ale Ministerstwo Cyfryzacji opracowało projekt ustawy o systemach sztucznej inteligencji (nr UC71), który wyznacza organy nadzorcze, wprowadza kary administracyjne i procedury skargowe. Projekt przeszedł

prekonsultacje (zakończone maj 2024 r., ponad 2000 uwag), konsultacje publiczne (do 15 listopada 2024 r., zakończone grudzień 2024 r.) oraz aktualizacje (nowa wersja luty 2025 r., zmiany w lipcu 2025 r. usuwające kary dla menedżerów); obecnie trwa analiza i prace rządowe bez podanego terminu uchwalenia. Ustawa

uzupełnia AI Act o krajowe mechanizmy: Krajowy Rejestr Systemów AI (KRiBSI), Radę Społeczną ds. AI, interpretacje i rekomendacje praktyk, notyfikację jednostek oceniających zgodność; rozporządzenie stosuje się bezpośrednio z fazowanym wdrożeniem.

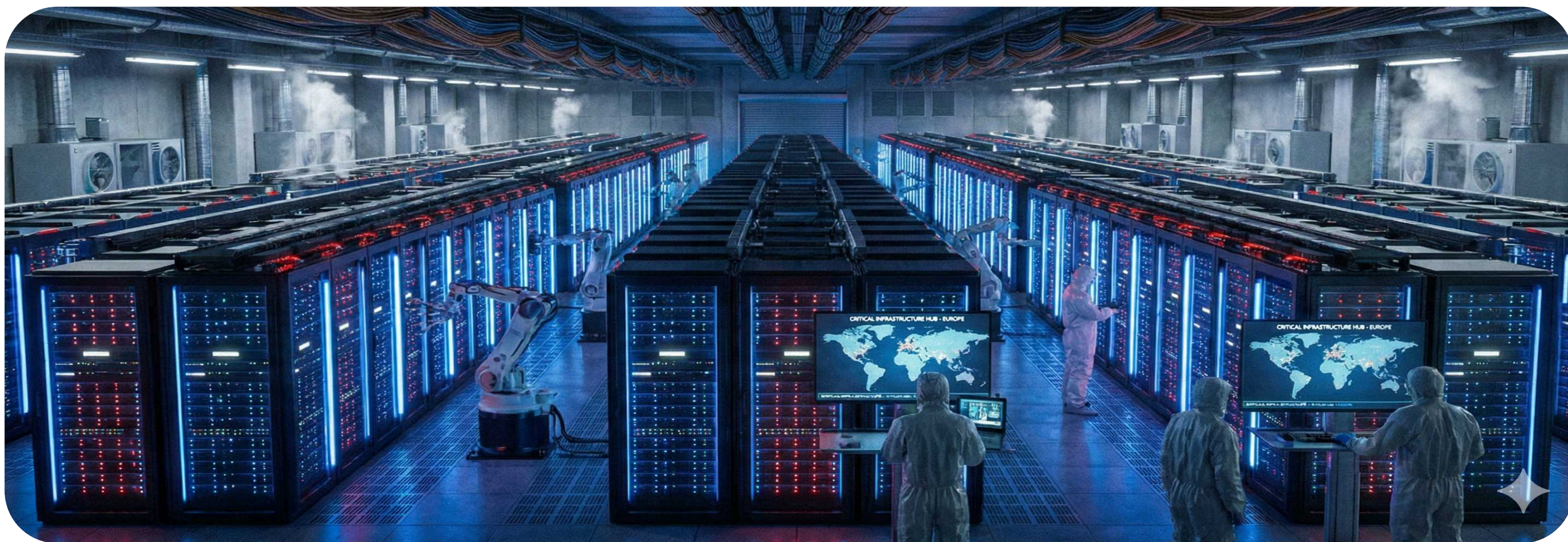
Dyrektywa NIS2

(Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14 grudnia 2022 r.) to unijny akt prawny wzmacniający cyberbezpieczeństwo sieci i systemów informatycznych (Network and Information Systems), zastępujący NIS1 i rozszerzający zakres na 18 sektorów krytycznych.

Dyrektywa nakłada na podmioty kluczowe i ważne (m.in. energetyka, transport, zdrowie, bankowość, infrastruktura cyfrowa) obowiązki zarządzania ryzykiem cybernetycznym, w tym ocenę zagrożeń, środki techniczne i organizacyjne, raportowanie incydentów oraz wymianę informacji o zagrożeniach.

(Dyrektywa Parlamentu Europejskiego i Rady (UE)

2022/2555 z 14 grudnia 2022 r.) to unijny akt prawny wywiązała się z tego terminu. Wdrożenie Dyrektywy NIS 2 poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC) jest opóźnione; projekt ustawy skierowano do dalszych prac w Sejmie, z planowanym zakończeniem procesu legislacyjnego do końca 2025 r. i wejściem w życie w pierwszej połowie 2026 r. po vacatio legis. Mimo opóźnienia, organizacje z kluczowych sektorów gospodarki (m.in. energetyka, transport, zdrowie, bankowość, infrastruktura cyfrowa) powinny już przygotowywać się na nowe, bardziej rygorystyczne obowiązki w zakresie zarządzania ryzykiem cyberbezpieczeństwa i zgłaszania incydentów.



Wnioski na podstawie aktywności PUODO w 2025 roku.

Aby zrozumieć, jak poważnie Urząd Ochrony Danych Osobowych podchodzi do egzekwowania przepisów RODO, warto przyrzeć się konkretnym decyzjom. Trzy przypadki z 2025 roku pokazują, że UODO nie

toleruje błędów w ochronie danych, niezależnie od tego, czy naruszenie dotyczy jednej osoby, czy milionów obywateli. Kary rosną – w 2025 roku UODO nałożyło ponad 64 milionów złotych kar, co stanowi wielokrotny wzrost w stosunku do lat poprzednich.

Rok	Suma kar (w zł)	Liczba kar	Uwagi
2025	>64 000 000	Dokładna liczba wiarygodna będzie podana w sprawozdaniu rocznym za 2025	Rekordowy wzrost, m.in. kary dla Poczty Polskiej (27 mln zł) i banków
2024	13 907 740,96	27	Wzrost o 1030% r/r, najwyższa kara: 4,05 mln zł
2023	1 230 331,28	31	Niski poziom w porównaniu do 2022



Kara dla ING Banku Śląskiego

W sierpniu 2025 roku Prezes UODO nałożył na ING Bank Śląski jedną z najwyższych kar w historii urzędu, w wysokości ponad **18,4 mln zł**. Powodem było masowe i nieuzasadnione skanowanie dowodów tożsamości klientów i potencjalnych klientów, co stanowiło naruszenie fundamentalnych zasad RODO, w tym zasady minimalizacji danych.

Według UODO bank, w okresie od 1 kwietnia 2019 r. do 23 września 2020 r., wdrożył procedury, które zakładały kopiowanie dokumentu tożsamości w szerokim zakresie sytuacji, często bez indywidualnej analizy i rzeczywistej potrzeby. Jak wskazał organ nadzorczy, praktyka ta obejmowała nawet przypadki niezwiązane z obowiązkami wynikającymi z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML), takie jak składanie reklamacji dotyczącej działania bankomatu. **UODO podkreśliło, że bank nie dokonywał indywidualnej oceny ryzyka, która uzasadniałaby konieczność wykonania kopii dokumentu w każdym przypadku, a zamiast tego stosował tę praktykę w sposób zautomatyzowany.**

„Bank nie dokonywał więc indywidualnej oceny ryzyka wiążącego się z danym klientem

i podejmowanymi przez niego działaniami. Dokumenty tożsamości skanowane były także w przypadkach niewiążących się z realizacją obowiązków określonych przepisami ustawy AML (np. przy reklamacji dotyczącej bankomatu).” – czytamy w komunikacie UODO. [2]

Prezes UODO uznał, że takie działanie naruszało art. 5 ust. 1 lit. c RODO, czyli **zasadę minimalizacji**, która wymaga, aby zakres przetwarzanych danych był adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są one przetwarzane. Gromadzenie pełnych skanów dowodów osobistych, które zawierają szeroki katalog danych (m.in. wizerunek, numer PESEL, imiona rodziców), bez konkretnej podstawy prawnej i analizy niezbędności, stwarzało wysokie ryzyko dla praw i wolności osób, których dane dotyczą. Bank zapowiedział odwołanie od decyzji.

Lekcja dla przedsiębiorców

Decyzja w sprawie ING Banku Śląskiego stanowi ważną przestrożę dla wszystkich administratorów danych, a w szczególności dla instytucji obowiązanych w rozumieniu ustawy AML.

1 Obowiązki wynikające z przepisów sektorowych (jak AML) nie zwalniają z przestrzegania RODO.

Wręcz przeciwnie, należy je interpretować w sposób spójny z ogólnym rozporządzeniem o ochronie danych. Kopiowanie dokumentu tożsamości jest dopuszczalne tylko wtedy, gdy jest to niezbędne do

zastosowania konkretnego środka bezpieczeństwa finansowego, a nie jako standardowa procedura „na zapas”.

2 Kluczowa jest indywidualna ocena ryzyka (risk-based approach).

Zamiast tworzyć sztywne procedury nakazujące zbieranie maksymalnego zakresu danych w każdej sytuacji, należy analizować każdy przypadek osobno. Czy do weryfikacji tożsamości klienta składającego prostą reklamację naprawdę potrzebny jest skan całego dowodu? Często wystarczający będzie wgląd do dokumentu bez jego kopiowania. Należy zawsze zadać sobie pytanie: „Czy osiągnięcie tego konkretnego celu jest niemożliwe bez przetwarzania tych danych?”

3 Zasada minimalizacji danych musi być wbudowana w procesy biznesowe (privacy by design).

Już na etapie projektowania procedur należy dążyć do ograniczania zbieranych danych. Jeśli celem jest identyfikacja klienta, można rozważyć inne, mniej inwazyjne metody. Przetwarzanie numeru PESEL czy wizerunku, gdy nie jest to absolutnie konieczne, generuje niepotrzebne ryzyko, za które administrator ponosi pełną odpowiedzialność.



Kara dla McDonald's Polska za błędy w nadzorze nad procesorem

W lipcu 2025 roku Prezes UODO nałożył na McDonald's Polska Sp. z o.o. karę w łącznej wysokości niemal **17 mln zł**. Sankcja była konsekwencją serii zaniedbań, które doprowadziły do wycieku danych osobowych pracowników w wyniku błędu podmiotu przetwarzającego (procesora), któremu firma powierzyła zarządzanie grafikami pracy [3].

McDonald's Polska zlecił zewnętrznej firmie obsługę systemu do zarządzania grafikami pracy. Wskutek błędnej konfiguracji serwera przez ten podmiot, dane pracowników – w tym tak wrażliwe informacje jak numery PESEL i paszportów – stały się publicznie dostępne. Postępowanie UODO wykazało, że McDonald's jako administrator danych ponosił współodpowiedzialność za to zdarzenie z powodu licznych uchybień. Firma nie zweryfikowała w wystarczający sposób swojego procesora pod kątem gwarancji bezpieczeństwa, nie przeprowadziła analizy ryzyka związanej z tym procesem i nie sprawowała należytego nadzoru nad jego działaniami. Co więcej, UODO stwierdziło naruszenie zasady minimalizacji danych, ponieważ w systemie przetwarzano numery PESEL i paszportów jako identyfikatory, choć można było użyć do tego celu mniej wrażliwych danych.

„Postępowanie wykazało, że spółka McDonald's nie zweryfikowała podmiotu przetwarzającego pod kątem zdolności do zabezpieczenia danych – oparto się jedynie na wcześniejszej współpracy w zakresie PR. Tym samym naruszono art. 28 ust. 1 RODO, który wymaga, by przetwarzanie w imieniu administratora odbywało się przez podmioty przetwarzające, zapewniające wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.” [3]

Lekcja dla przedsiębiorców

Sprawa McDonald's to fundamentalna lekcja na temat odpowiedzialności administratora za działania procesora.

1 Wybór podmiotu przetwarzającego to krytyczny proces.

Nie można opierać się wyłącznie na dotychczasowej współpracy w innych obszarach czy na reputacji firmy. Należy przeprowadzić formalną weryfikację (due diligence), żądając dowodów na wdrożenie odpowiednich środków technicznych i organizacyjnych, takich jak certyfikaty, wyniki audytów bezpieczeństwa czy szczegółowe opisy stosowanych zabezpieczeń. Artykuł 28 ust. 1 RODO nakłada na administratora obowiązek korzystania wyłącznie z usług takich podmiotów, które dają „wystarczające gwarancje”.

2 Umowa powierzenia to początek, a nie koniec obowiązków.

Administrator musi aktywnie nadzorować procesora przez cały okres współpracy. Oznacza to korzystanie z prawa do audytu, regularne przeglądy raportów bezpieczeństwa i stałą komunikację. Bierność i pełne zaufanie, bez mechanizmów weryfikacji, jest prostą drogą do naruszenia.

3 Administrator pozostaje odpowiedzialny za zgodność z zasadami RODO, nawet gdy dane przetwarza ktoś inny.

To McDonald's, a nie procesor, został ukarany za naruszenie zasady minimalizacji. Administrator decydując o celach i sposobach przetwarzania musi



zadbać, aby systemy (nawet te obsługiwane przez zewnętrzną firmę) nie zbierały nadmiarowych danych. Odpowiedzialność za bezpieczeństwo danych jest wspólna, a kara może dotknąć zarówno administratora, jak i procesora, co w tej sprawie miało miejsce.



Wybory kopertowe – Poczta Polska

Najbardziej spektakularnym przykładem jest kara dla Poczty Polskiej w wysokości **27 milionów złotych** (oraz 100 tysięcy złotych dla Ministra Cyfryzacji) za przetwarzanie bez podstawy prawnej danych 30 milionów obywateli z bazy PESEL [4].

W 2020 roku, podczas pandemii COVID-19, rząd planował przeprowadzenie wyborów prezydenckich wyłącznie w formie korespondencyjnej. Poczta Polska otrzymała decyzję administracyjną zobowiązującą ją do przygotowań. Na tej podstawie Poczta wnioskowała o dostęp do danych wszystkich pełnoletnich obywateli Polski z rejestru PESEL – imiona, nazwiska, numery PESEL, adresy. Minister Cyfryzacji wyraził zgodę i przekazał dane na płycie DVD.

Dane dotyczyły niemalże 80 procent populacji kraju. Były przetwarzane przez Poczta Polską przez kilka tygodni, aż do zniszczenia w maju 2020 roku, już po tym, gdy wybory się nie odbyły.

Prezes UODO uznał, że naruszenie ma charakter fundamentalny. Mimo że Poczta Polska działała na podstawie decyzji administracyjnej, powinna była przeprowadzić analizę prawną, czy decyzja ta stanowi wystarczającą podstawę do przetwarzania danych. Wysokość kary uzasadniona była zakresem przetwarzanych danych, liczbą osób dotkniętych naruszeniem (30 milionów) oraz możliwością szkód niematerialnych, takich jak obawa i niepewność wynikająca z niemożności sprawowania kontroli nad własnymi danymi.

Lekcja dla przedsiębiorców

Nawet decyzja administracyjna nie stanowi automatycznie podstawy prawnej do przetwarzania danych osobowych. Konieczna jest zawsze analiza prawna. Jeśli otrzymasz polecenie przetwarzania danych, sprawdź, czy ma ono podstawę w prawie. Spółki Skarbu Państwa mają szczególne obowiązki w zakresie ochrony danych i powinny odznaczać się najwyższą starannością.

Plan działania na 2026 rok: Na co położyć nacisk?

Prezes UODO już w planach prac na 2025 r. wśród priorytetów kontrolnych wymienił sztuczną inteligencję – nadzór nad zgodnością systemów AI

wzmożoną kontrolę procedur detekcji i zgłaszania incydentów. Oznacza to, że i w najbliższym czasie możemy spodziewać się szczególnej uwagi w wyżej wskazanych obszarach polskiego organu nadzorczego.

Zwróciłabym też uwagę na raport Organizational Digital Governance Report 2025 opublikowany przez IAPP, który pokazuje, że organizacje na całym świecie muszą przyjąć kompleksowe podejście do zarządzania danymi i cyberbezpieczeństwem.

Raport wskazuje, że:

ryzyko dla prywatności i ochrony danych (58% respondentów)

sztuczna inteligencja jako źródło zagrożeń (54% respondentów)

są postrzegane jako najważniejsze wyzwania cyfrowe [5]. Organizacje, które chcą być gotowe na przyszłość, muszą integrować ochronę danych z zarządzaniem cyberbezpieczeństwem, budować świadomość zagrożeń na wszystkich poziomach, inwestować w narzędzia wspierające zgodność oraz monitorować zmiany regulacyjne i dostosowywać się do nich proaktywnie.



Ryzyko cyfrowe	Procent wskazań	Kategoria
Ryzyko dla prywatności i ochrony danych	58%	Społeczne i środowiskowe
Technologie sztucznej inteligencji jako czynnik przyspieszający lub zwiększający ryzyko wystąpienia niekorzystnych skutków	54%	Społeczne i środowiskowe
Zależność od dostawców zewnętrznych (stron trzecich) i ryzyka z tym związane	51%	Technologiczne
Brak wystarczającego budżetu i zasobów na inwestycje w specjalistów ds. nadzoru (governance), praktyki i w narzędzia	48%	Organizacyjne
Cyberataki, szpiegostwo i działania wojenne sponsorowane przez państwa	42%	Geopolityczne
Przestarzała infrastruktura (legacy) i narzędzia nieadekwatne do potrzeb	41%	Technologiczne
Polityczne i legislacyjne działania zmierzające do obniżenia znaczenia zarządzania i zgodności z przepisami (compliance)	39%	Geopolityczne
Niejasność lub brak świadomości w zakresie mapowania danych i systemów	39%	Technologiczne
Identyfikacja i zarządzanie dezinformacją oraz fałszywymi informacjami w sieci	37%	Społeczne i środowiskowe
Biznesowe obniżenie priorytetu nadzoru i zgodności, np. na rzecz innowacji, monetyzacji i konkurencyjności	38%	Organizacyjne

Źródło: IAPP, Organizational Digital Governance Report 2025 [5]

Biorąc pod uwagę te trendy, przedsiębiorcy powinni w 2026 r. położyć nacisk na te kwestie:

- ✓

przegląd i aktualizacja procedur oceny ryzyka naruszeń: niezbędnym jest wypracowanie jasnych kryteriów i przeszkolenie zespołów odpowiedzialnych za reagowanie na incydenty
- ✓

opracowanie ram zarządzania sztuczną inteligencją: biorąc pod uwagę priorytety UODO i przepisy AI Act, organizacje powinny dokonać inwentaryzacji wszystkich systemów AI, sklasyfikować je pod kątem ryzyka i udokumentować podstawę prawną przetwarzania danych, zwłaszcza w kontekście „prawnie uzasadnionego interesu”
- ✓

wdrożenie NIS2 w organizacji: mimo opóźnień, ustawa wdrażająca NIS2 wejdzie w życie prawdopodobnie w pierwszej połowie 2026 roku [6], więc firmy z kluczowych sektorów powinny już teraz ocenić, czy podlegają nowym wymogom i przygotowywać się na wdrożenie środków zarządzania ryzykiem cyberbezpieczeństwa
- ✓

budowanie kultury ochrony danych w powiązaniu z cyberbezpieczeństwem: fundamentem zgodności jest świadomość, a to oznacza regularne szkolenia dla pracowników, zaangażowanie kierownictwa oraz wdrożenie prostych mechanizmów zgłaszania incydentów i zagrożeń.

Perspektywa na przyszłość: rola współpracy i harmonizacji

Rok 2026 zapowiada się jako okres konsolidacji i pogłębiania wysiłków w zakresie ochrony danych. Komisja Europejska wystąpiła z inicjatywą zaproponowania pakietu zmian obejmujących również RODO, znanego jako **“Digital Omnibus”**.

Zmiany w przepisach UE mają na celu uproszczenie i harmonizację tzw. legislacji cyfrowej (Digital Omnibus Regulation Proposal). Choć zmiany te mają zmniejszyć obciążenia administracyjne, będą wymagać od firm proaktywnego przygotowania. Poniżej wymieniamy te najbardziej kluczowe propozycje zmian w RODO:

Obszar	Przepis dotychczasowy (RODO)	Proponowana zmiana (Digital Omnibus)	Implikacje
Zgłaszanie naruszeń	Zgłoszenie w ciągu 72 godzin każdego naruszenia, chyba że jest mało prawdopodobne, by powodowało ryzyko naruszenia praw lub wolności.	Zgłoszenie tylko naruszeń stwarzających „wysokie ryzyko” dla praw i wolności; wydłużenie terminu do 96 godzin.	Wymaga zmiany procedur oceny ryzyka; mniej zgłoszeń, ale bardziej rygorystyczna ocena
Ocena skutków (DPIA)	Obowiązek przeprowadzenia DPIA dla operacji wysokiego ryzyka; krajowe organy nadzorcze publikują własne wykazy operacji wymagających DPIA.	Harmonizacja wymogów dotyczących DPIA na poziomie UE; EROD stworzy ogólnounijne listy operacji i standardowe szablony.	Uproszczenie procedur poprzez standaryzację; mniej niepewności w interpretacji wymogów
Definicja danych osobowych	Szeroka definicja obejmująca wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.	Doprecyzowanie, że dane pseudonimizowane nie są danymi osobowymi, jeśli administrator nie ma możliwości ponownej identyfikacji osoby.	Zmiana klasyfikacji niektórych danych; potencjalne zmniejszenie zakresu obowiązków dla niektórych operacji
Podstawa prawna dla AI	Przetwarzanie danych na potrzeby AI wymaga znalezienia odpowiedniej podstawy prawnej (np. zgoda, umowa).	Rozwój i testowanie AI może być uznane za „prawnie uzasadniony interes” administratora, co ułatwi przetwarzanie danych w tym celu.	Ułatwianie innowacji w AI; wymaga jednak dokumentacji uzasadniającej interes i oceny wpływu na prawa osób



Podsumowanie LexDigital: kompleksowe podejście do zmian regulacyjnych

Nowe regulacje, choć mogą wydawać się obciążeniem, mają na celu stworzenie wspólnego, bezpiecznego standardu w gospodarce cyfrowej. **Dla przedsiębiorców proaktywne podejście do ochrony danych i cyberbezpieczeństwa nie jest już tylko obowiązkiem prawnym, ale staje się kluczowym elementem budowania zaufania klientów i trwałej przewagi konkurencyjnej w coraz bardziej cyfrowym świecie.** Organizacje, które podejmą działania opisane w niniejszym artykule i będą współpracować z partnerami rozumiejącymi złożoność regulacyjnego otoczenia, będą lepiej przygotowane na wyzwania 2026.

W obliczu dynamicznie zmieniającego się otoczenia prawnego wokół ochrony danych osobowych, przedsiębiorcy potrzebują partnera, który rozumie nie tylko obecne wymagania RODO, ale także antycypuje przyszłe zmiany.

LexDigital podchodzi kompleksowo do potrzeb swoich klientów, biorąc kierunek zmian i otoczenia prawnego w swoją pracę. Nasze podejście opiera się na monitorowaniu zmian legislacyjnych (m.in. śledzeniu prac nad wspomnianym Digital Omnibus), analizie orzeczeń UODO (wyciąganiu wniosków z decyzji administracyjnych), integracji ochrony danych z innymi aspektami zarządzania (łączeniu RODO z wymogami AI Act, DORA, NIS2 i Data Act) oraz edukacji klientów (pomaganiu przedsiębiorcom zrozumieć strategiczny wymiar ochrony danych).



Pamiętajmy, że dobre szkolenia to nie tylko zgodność z RODO – to także **budowanie kultury bezpieczeństwa w organizacji**, która minimalizuje ryzyko incydentów i zapewnia większą ochronę zarówno firmie, jak i jej klientom.



LexDigital

**Napisz, w czym możemy Ci
pomóc, a my skontaktujemy się
z Tobą w ciągu 24 godzin.**

Umów bezpłatną konsultację

Źródła:

1. Money.pl. (2025). 64 mln zł sankcji za naruszenia danych. UODO tłumaczy, skąd ten skok.
<https://www.money.pl/gospodarka/64-mln-zl-sankcji-za-naruszenia-danych-uodo-tlumaczy-skad-ten-skok-7226053487008384a.html>
2. Urząd Ochrony Danych Osobowych. (2025, 26 sierpnia). Bank nie może skanować dowodów osobistych klientów bez stosownej analizy celowości. Pobrano z
<https://uodo.gov.pl/pl/138/3854>
3. Urząd Ochrony Danych Osobowych. (2025, 21 lipca). Za ochronę danych osobowych są odpowiedzialni zarówno administrator, jak i podmiot przetwarzający. Pobrano z
<https://uodo.gov.pl/pl/138/3827>
4. Urząd Ochrony Danych Osobowych. (2025). Kary za naruszenie RODO przy organizacji wyborów korespondencyjnych 2020. Pobrane z
<https://uodo.gov.pl/pl/138/3590>
5. IAPP. (2025). Organizational Digital Governance Report 2025. Pobrane z
<https://iapp.org/>
6. White & Case. (2025). GDPR under revision: Key takeaways from the Digital Omnibus Regulation proposal. Pobrane z
<https://www.whitecase.com/insight-alert/gdpr-under-revision-key-takeaways-from-digital-omnibus-regulation-proposal>



Newsletter RODO

Grudzień 2025 nr 12/2025

Dziękujemy za przeczytanie naszego newslettera!

Masz pytania?

SKONTAKTUJ SIĘ Z NAMI