



Monitoring cyfryzacji

Wrzesień 2026

Monitoring cyfryzacji: wrzesień 2026

Autorzy:

Krzysztof Kardaszewicz; Marcin Woźny; Mateusz Rozdżestwieński

Centrum Analiz i Strategii, Polska Agencja Rozwoju Przedsiębiorczości

Niniejsze opracowanie jest materiałem przygotowanym w ramach nowej serii wydawniczej PARP pt. „Monitoring Cyfryzacji”. Publikowane co kwartał raporty mają na celu analizę wybranych trendów w cyfryzacji.

Kontakt w sprawie Raportu: analizy@parp.gov.pl

Spis treści

Wstęp: AI, centra danych i rosnące koszty cyfryzacji	4
Rozwój centrów danych i zapotrzebowanie na energię	5
Wydajność infrastruktury i zużycie/dostępność wody	7
Działania i legislacja w Unii Europejskiej	8
Ustawa o systemach sztucznej inteligencji	10
Zadania i kompetencje Komisji:	11
Skład i ustrój Komisji:	11
Rada do spraw Sztucznej Inteligencji:	12
Postępowanie w sprawie naruszeń:.....	12
Układ w sprawie warunków nadzwyczajnego złagodzenia sankcji – n	13
owatorski mechanizm polubowny pozwalający na polubowne zakończenie sprawy:.....	13
Kary administracyjne:.....	13
Sankcje karne/wykroczeniowe:.....	14
AI Act	14
Cyber Resilience Act (CRA)	20
Ustawa o zarządzaniu danymi (Data Governance Act)	23
Lista źródeł.....	26
Organizacje – krajowe i międzynarodowe	26
Raporty i analizy	27
Sektor prywatny	28
Prasa.....	28

Wstęp: AI, centra danych i rosnące koszty cyfryzacji

W obecnej edycji Monitoringu Cyfryzacji przedstawiamy podsumowanie informacji dotyczących rozwoju centrów danych oraz ich przełożenie na realia funkcjonowania przedsiębiorców. Następnie podsumowujemy działania podejmowane przez Unię Europejską w celu przygotowania odpowiedzi dla nadchodzących wyzwań. Przedstawiamy również podsumowanie najważniejszych dla tej tematyki aktów prawnych i strategii, zarówno na poziomie Polski, jak i Unii Europejskiej.

Błyskawiczny rozwój sztucznej inteligencji¹ oraz jej rola w rozwoju gospodarczym przekładają się również na szybki wzrost zapotrzebowania na infrastrukturę i moce obliczeniowe, a co za tym idzie na koszty i dostępność energii, zasobów wodnych i komponentów. Najnowsze analizy zakładają światowy **wzrost nakładów na centra danych** z 800 mld do 1,8 bln USD do 2050 roku, przy czym dostęp do energii elektrycznej ma być decydujący dla ich lokalizacji oraz powiązanych inwestycji². Jednocześnie, według prognoz IEA, **globalne zużycie energii elektrycznej przez centra danych** może wzrosnąć ponad dwukrotnie w ciągu 5 lat (z około 415 TWh w 2024 r. do około 945 TWh w 2030 r.³. Do 2030 roku centra danych będą odpowiadały za ok. 20% wzrostu zapotrzebowania na energię elektryczną w gospodarkach rozwiniętych⁴.

Biorąc pod uwagę skalę i tempo rozwoju, ograniczona dostępność zasobów może przekładać się też na większy koszt wykorzystania AI dla przedsiębiorców. Ponieważ centra danych mają tendencję do koncentracji przestrzennej, stwarzają istotną presję na lokalne sieci elektroenergetyczne⁵. Trudności mogą wystąpić zwłaszcza w okresie szczytowego zapotrzebowania na energię (listopad-luty) jak również w okresie rosnącej presji na zasoby wodne (zwłaszcza latem) i zależeć od wydajności lokalnej infrastruktury.

Dlatego, choć pełne koszty obsługi sztucznej inteligencji obecnie nadal pozostają na drugim planie⁶, to wraz z jej rosnącym wykorzystaniem mogą stanowić realne obciążenie dla

¹ Według szacunków badaczy Google Deepmind, [możliwości obliczeniowe modeli AI](#) rozwijają się w tempie 10x rocznie; zaawansowane modele coraz łatwiej obchodzą też obecne systemy bezpieczeństwa. Ostatnie [incydenty](#), w których najnowsze modele AI [coraz regularnie wyłamują się](#) ze środowisk testowych skłoniły wiodące amerykańskie firmy technologiczne do rozmów ([w Białym Domu](#)) w celu uzgodnienia zasad nadzoru nad dalszym rozwojem sztucznej inteligencji.

² PwC, 2026 <https://www.pwc.com/gx/en/1/services/consulting/technology/data-centre-outlook.html>

³ Warto odnotować, że będzie to poziom porównywalny do zużycia energii w Japonii. Jednocześnie, jako sektor gospodarki, globalne zużycie energii przez centra danych osiągnie poziom porównywalny do zużycia w światowej produkcji aluminium (około 1000 TWh) oraz produkcji stali (około 1300 TWh): <https://pmc.ncbi.nlm.nih.gov/articles/PMC8972653/>

⁴ International Energy Association (IEA), [Energy and AI, 2025](#)

⁵ Przykładowo, w Irlandii centra danych zużywają około 20% dostaw energii elektrycznej. [Energy and AI, 2025](#)

⁶ Przykładowo, najnowszy raport EY (https://www.ey.com/pl_pl/newsroom/2026/08/badanie-ey-ponad-8-na-10-liderow-firm-obawia-sie-kosztow-korzystania-z-ai) wykazuje, że 82% przebadanych firm w USA obawia się rosnących wydatków, jednak omawiane jest wyłącznie wykorzystanie tokenów AI, bez uwzględnienia

przedsiębiorców – także w Polsce. Lokalizacja oraz koszty rozbudowy i obsługi powiązanej infrastruktury mogą okazać się kluczowe, nawet biorąc pod uwagę stopniowo malejące ceny tokenów dla bardziej zaawansowanych modeli AI⁷.

Oprócz skali planowanych inwestycji (przykładowo, największe firmy technologiczne w USA budują własne elektrownie mające sprostać prognozowanemu zapotrzebowaniu^{8,9}) wyzwaniem mogą okazać się również rosnące **koszty komponentów** – wafli krzemowych, procesorów i układów pamięci¹⁰ – oraz potrzeba ich cyklicznego zastępowania sprzętem nowszej generacji (typowo 3-5 razy w ciągu 20-letniego cyklu życia danego centrum danych)¹¹. Jednocześnie rozbudowa mocy obliczeniowych oznaczać będzie narastający wolumen **odpadów elektronicznych** oraz trudności z ich recyklingiem¹². Według ostatnich danych, jedynie 22,3% z 62 mln ton światowych e-odpadów zostało formalnie zebrane i poddane recyklingowi, z czego niemal 1/3 była zagospodarowana przez sektor nieformalny w krajach o niskich i niższych średnich dochodach¹³.

Rozwój centrów danych i zapotrzebowanie na energię

Cele przedstawione przez Komisję Europejską w projekcie rozporządzenia Cloud and AI Development Act (CADA), zakładają **potrojenie mocy obliczeniowych europejskich centrów danych do 2030 r.** oraz osiągnięcie poziomu odpowiadającego europejskiemu zapotrzebowaniu do 2035 r. Powiązane z tym prognozy zużycia energii przez centra danych przewidują wzrost z 12,4 GW w 2025 r. do co najmniej 31 GW w 2035 r. (najniższy zakładany scenariusz), co przełoży się na **wzrost zapotrzebowania na energię elektryczną** z obecnych ok. 100 TWh do co najmniej 314 TWh rocznie. Skalę planowanej zmiany może zobrazować

czynników mogących zmieniać ich cenę. Jednocześnie najwięksi gracze (tzw. Big Tech) budują własne elektrownie, starając się sprostać przyszłemu zapotrzebowaniu na moce obliczeniowe.

⁷ Na problem zwraca uwagę m.in. [raport IEA](#), odnotowując, że choć energia przypadająca na pojedyncze zadanie AI spada, to rośnie całkowite jej zużycie w związku z ogólnym wzrostem wykorzystania AI.

⁸ <https://www.weforum.org/stories/energy-transition/localized-approaches-vital-for-energy-transition-momentum-and-more-top-energy-stories/>; <https://www.wsj.com/business/energy-oil/ai-data-centers-desperate-for-electricity-are-building-their-own-power-plants-291f5c81>

⁹ Część [analiz](#) wskazuje, że rosnące koszty inwestycji w rozwój infrastruktury mogą znaleźć odbicie na rynku pracy – [przynajmniej część zwolnień w USA](#) miała na celu uwolnienie kapitału potrzebnego do budowy centrów danych i elektrowni mających sprostać ich zapotrzebowaniu.

¹⁰ <https://www.scmp.com/tech/tech-trends/article/3358907/chip-supply-chain-braces-more-price-hikes-upstream-parts-create-new-bottlenecks>; <https://www.jpmorgan.com/insights/global-research/artificial-intelligence/dram-memory-shortage-from-ai>

¹¹ PwC, 2026 <https://www.pwc.com/gx/en/1/services/consulting/technology/data-centre-outlook.html>

¹² Według danych Global E-waste monitor, światowy wolumen odpadów elektronicznych wzrósł o 16% (8,4 mln ton) w ciągu zaledwie 3 lat. Przedstawione prognozy zakładają wzrost o kolejne 32% do 2030 r., osiągając aż 82 mln ton odpadów <https://ewastemonitor.info/the-global-e-waste-monitor-2024/>. Z kolei najnowsza [analiza Basil Action Network](#), biorąca pod uwagę całość odpadów elektronicznych wytwarzanych pod wpływem AI (w tym infrastrukturę obsługi centrów danych oraz sprzęt elektroniczny zastępowany pod wpływem rozwoju mocy obliczeniowych) podaje zdecydowanie większy szacunek – do 211 mln ton odpadów rocznie w 2050 r.

¹³ <https://www.ilo.org/publications/e-waste-and-employment-around-world>

fakt, że jest to niemal dwukrotnie więcej niż całkowite obecne roczne zapotrzebowanie Polski na energię (167,5 TWh)¹⁴.

W Polsce, według prognoz Państwowych Sieci Elektroenergetycznych, do 2040 roku centra danych mogą stać się jednym z największych nowych odbiorców energii i odpowiadać za ok. 11% krajowego zużycia (29 TWh)¹⁵. Obecnie w kraju zlokalizowane są centra danych o łącznej mocy 200 MW, ale planowana jest rozbudowa ich mocy do 500 MW już w 2030^{16,17}. Ich rozbudowa wiązać się będzie z obciążeniem systemu energetycznego, przechodzącego z elektrowni węglowych na OZE i jednoczesną elektryfikacją kolejnych sektorów gospodarki (np. transport, ciepłownictwo)¹⁸. Prognozowane **zapotrzebowanie na energię** ma wzrosnąć z obecnych 167,5 TWh do 200 TWh w 2030 i do 270 TWh w 2040¹⁹. Jednocześnie już obecnym wyzwaniem pozostają koszty energii w Polsce, zaliczane do najwyższych w Europie i oceniane jako poważne ograniczenie dla konkurencyjności przemysłu^{20,21}. Jednym z istotnych elementów, wskazywanych również przez Komisję Europejską w skali całej Europy, są ograniczenia sieci przesyłowych i związane z tym koszty dystrybucji (m.in. w Polsce)²².

Rozwój centrów danych oraz ich lokalizacja stają się więc kluczowym elementem kosztów związanych z presją na infrastrukturę elektryczną i koszty działalności przedsiębiorców. Opisane wyzwania nie zostają bez odpowiedzi – od września 2026 r. wprowadzono zmiany taryf energii dla dużych odbiorców przemysłowych (zużywających co najmniej 50 GWh energii). Jednocześnie trwają prace nad wdrożeniem unijnego programu umożliwiającego

¹⁴ <https://pie.net.pl/tygodnik-gospodarczy-24-2026-18-czerwca-2026-r/#tyg-mat-37530-3>; <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

¹⁵ <https://pie.net.pl/tygodnik-gospodarczy-24-2026-18-czerwca-2026-r/#tyg-mat-37530-3>; <https://www.pse.pl/-/projekt-nowego-planu-rozwoju-sieci-przesylowej-na-lata-2027-2036>

¹⁶ <https://pie.net.pl/tygodnik-gospodarczy-24-2026-18-czerwca-2026-r/#tyg-mat-37530-3>

¹⁷ Oprócz planowanej rozbudowy obecnej infrastruktury obliczeniowej w ramach rozwoju dwóch Fabryk AI (*Gaia* w krakowskim AGH Cyfronocie, oraz *Piast* w poznańskim PCSS - w obu przypadkach zakładające budowę dedykowanego klastra o mocy obliczeniowej 1000 GPU, współfinansowanego z unijnego programu EuroHPC), Polska jest częścią międzynarodowego konsorcjum w partnerstwie z Litwą i Czechami, biorącego udział w przetargu na budowę jednej z siedmiu mających powstać w Europie Gigafabryk AI, o mocy 100 000 GPU – przewidzianych jako infrastruktura do rozwoju i obsługi zaawansowanych modeli sztucznej inteligencji.

¹⁸ Obecny miks energetyczny Polski to nadal w ponad 52% węgiel, natomiast już w 2030 r. ponad połowę produkowanej energii mają stanowić OZE (wzrost z 31 do 50% produkcji energii - do 100 TWh rocznie. Polska ma zainstalowane moce OZE w wysokości 77 GW, ale obecna produkcja wykorzystuje niecałe 38GW).

¹⁹ Krajowy Plan Energii i Klimatu (KPEiK) <https://www.gov.pl/web/klimat/projekt-krajowego-planu-w-dziedzinie-energii-i-klimatu-do-2030-r-z-perspektywa-do-2040-r-wersja-przekazana-do-dalszych-prac-przez-Ministra-Energii>

²⁰ <https://www.forum-energii.eu/rachunek-za-konkurencyjnosc>. Koszty w Polsce są oceniane jako 25% wyższe niż w Niemczech, 58% niż w Danii i 113% niż we Francji. Rolę odgrywa zarówno wysoka cena samej energii, jak też opłaty emisyjne (koszty CO₂) oraz wysokie opłaty sieciowe.

²¹ Raport: Transformacja Energetyczna w Praktyce: <https://kig.pl/wp-content/uploads/2026/09/Raport-Transformacja-energetyczna-online.pdf>

²² https://energy.ec.europa.eu/data-and-analysis/energy-prices-and-costs-europe_en

obniżenie do 50% kwalifikowanych kosztów zużycia energii elektrycznej w zamian za inwestycje w transformację energetyczną i obniżenie energochłonności przedsiębiorstwa²³.

Wydajność infrastruktury i zużycie/dostępność wody

Kolejnym ważnym ograniczeniem, obecnie często pomijanym w potencjalnych kosztach i planach rozwoju AI, jest rosnąca presja na zasoby wodne – niezbędne zarówno przy wytwarzaniu energii elektrycznej, chłodzeniu centrów danych, oraz produkcji komponentów, takich jak półprzewodniki. Od 2024 roku Komisja Europejska wprowadziła obowiązek raportowania zużycia energii i wody przez centra danych – i choć dostępne dane nadal są niepełne, to informacje wskazane w pierwszym raporcie z ubiegłego roku wskazują, że zużycie wody przez centra danych w Unii Europejskiej (WIN) wyniosło około 6,2 mln m³.²⁴ Z kolei dane z raportów największych firm technologicznych wykazują, że zużycie wody przez centra danych Microsoft i Google wzrosło około 20-30% (w okresie 2021-2023) i było związane przede wszystkim z rozwojem sztucznej inteligencji. W dostępnych analizach wyliczono też m.in., że trenowanie modelu GPT-3 w centrach danych Microsoftu pochłonęło 5,4 miliona litrów wody (w tym 700 tys. litrów dla samego chłodzenia)²⁵. Wreszcie, analiza International Energy Agency obrazuje potencjał zużycia na przykładzie, według którego olbrzymie centrum danych w USA o mocy 100MW może zużywać nawet do dwóch milionów litrów wody dziennie²⁶.

Na poziom i wydajność zużycia wody (WUE) ma wpływ szereg czynników – od zastosowanej technologii chłodzenia, przez wykorzystywany miks energii, po lokalne warunki pogodowe. Ma to znaczenie m.in. ze względu na coraz większy wpływ zmiany klimatycznej na temperatury i poziom wód, co może przekładać się na ograniczoną dostępność w okresach zwiększonego zapotrzebowania i wpłynąć na funkcjonowanie centrów danych – od możliwości chłodzenia, po samą dostępność energii. Przykładowo, w sierpniu 2026 r. odnotowano ograniczenie mocy elektrowni w związku z niskim poziomem wód w rzekach m.in. w Polsce, Rumunii, Węgrzech i Francji. Problem dotyczył zwłaszcza energii jądrowej, w skrajnym przypadku doprowadzając do wyłączenia dwóch z czterech reaktorów elektrowni dostarczającej połowę energii elektrycznej na Węgrzech²⁷. W Polsce, istotnym wyzwaniem pozostaje długotrwały stan suszy w 2/3 polskich gmin i rekordowe wzrosty temperatury

²³ Chodzi o Clean Industry Deal State Aid (2027-2030) przeznaczający na ten cel 4,8 mld złotych. Minimum 50% otrzymanej pomocy przedsiębiorca będzie musiał przeznaczyć na transformację energetyczną.

²⁴ Zużycie Polski wyniosło 20,359 m³, przy czym są to niepełne dane z 36 centrów danych. Raport KE jest dostępny na stronie: <https://op.europa.eu/en/publication-detail/-/publication/83be4c3e-5c79-11f0-a9d0-01aa75ed71a1/language-en>

²⁵ <https://arxiv.org/abs/2304.03271> "Making AI less thirsty" (2025)

²⁶ Dokładny przykład omówiono w raporcie [Energy and AI](https://www.congress.gov/crs-product/R48646), na stronie 242 (Box 5.4). Dodatkowo porównaj: <https://www.congress.gov/crs-product/R48646> „Data Centers and their Energy Consumption” (2026)

²⁷ <https://zielonagospodarka.pl/praca-trzech-reaktorow-atomowych-we-francji-zostala-wstrzymana-przez-upaly-23205>; <https://zielonagospodarka.pl/niski-stan-dunaju-uderza-w-atom-wegry-przechodza-kryzys-rumunia-wysadza-podwodna-skale-23329>

mające wpływ na wydajność infrastruktury – z przełożeniem na koszt mocy obliczeniowych. Dlatego wyzwanie może stanowić dostępność wody i koszt energii w określonych porach i lokalizacjach²⁸.

Wpływ rosnącej presji na zasoby wodne jest wyraźnie widoczny na przykładzie państw takich jak Tajwan, wiodących w światowej produkcji komponentów i rozwoju AI. Ponieważ strategia gospodarcza wyspy jest silnie skoncentrowana zarówno na produkcji półprzewodników jak i rozwoju sztucznej inteligencji (tj. powiązanej infrastruktury) zapotrzebowanie na wodę stale rośnie. W przypadku najważniejszego producenta (TSMC) pomimo dużych inwestycji w recykling i technologie odzysku oraz ograniczenia poboru wody, rozwój zaawansowanej produkcji oznaczał, że całkowite zużycie wody wzrosło z ok. 114 mln m³ w 2023 r., do 129 mln m³ rok później²⁹. Jednocześnie, pod wpływem suszy i ekstremalnych temperatur wzrasta ryzyko dla ciągłości pracy przemysłu³⁰.

Działania i legislacja w Unii Europejskiej

Poniżej przedstawiamy omówienie wybranych działań Komisji Europejskiej oraz aktów prawnych – w tym wdrażanych obecnie w Polsce – związanych z rozwojem sztucznej inteligencji, bezpieczeństwem i zarządzaniem danymi.

Wychodząc naprzeciw opisanym wcześniej wyzwaniom, Komisja opublikowała w czerwcu **mapę drogową** poświęconą wdrożeniu cyfryzacji i sztucznej inteligencji w energetyce³¹, zakładającą działania dotyczące trzech kluczowych obszarów i powiązanych z nimi działań.

Pierwszy z nich, Energia dla AI, zakładający sprawną integrację centrów z systemem energetycznym jest kluczowy, biorąc pod uwagę to, jak szybki przyrost wniosków o przyłączenie do sieci, bez odpowiedniego zarządzania, może zagrozić bezpieczeństwu dostaw, nasilić kongestię sieci i podbić ceny prądu. Obszar obejmuje m.in. wdrożenie modelu **trójstronnych umów** pomiędzy lokalnymi władzami, podmiotami energetycznymi i centrami danych mających usprawnić koordynację działań i wymianę informacji. Działanie ma

²⁸ Susza hydrologiczna: <https://www.gov.pl/web/wody-polskie-szczecin/susza-hydrologiczna-doswiadcza-regiony-polski-zachodniej-i-centralnej>; <https://www.susza.iung.pulawy.pl/>; <https://zielonagospodarka.pl/susza-panuje-w-calym-kraju-uderza-w-rolnictwo-i-dostepnosc-wody-23144>. Jednocześnie obawy o wpływ centrów danych na miejscowe zasoby wodne stały się przyczyną protestów lokalnych społeczności (m.in. w okolicach Warszawy): <https://www.rp.pl/biznes/art45162991-opor-wobec-centrow-danych-coraz-wiecej-polakow-mowi-nie>

²⁹ <https://investor.tsmc.com/static/annualReports/2024/english/ebook/index.html>

³⁰ <https://dset.tw/en/research/infrastructure-resilience2025/> Według dostępnych analiz, dzienne zużycie zaawansowanych fabryk półprzewodników jest porównywalne do zużycia średniej wielkości miasta.

³¹ Szczegółowe założenia mapy drogowej (UE Strategic Roadmap on Digitalization and AI in the Energy Sector) zostały omówione w czerwcowej edycji [Monitoringu Cyfryzacji](#). Dla przypomnienia przytaczane są tu jedynie najważniejsze informacje związane z rozwojem centrów danych. Pełen tekst aktu prawnego jest dostępny [tutaj](#).

przełożyć się na większą elastyczność, ograniczenie spekulacyjnych projektów i usprawnione mechanizmy obsługi kolejek przyłączeniowych oraz zakupu energii elektrycznej³².

Drugi obszar, cyfryzacja i AI dla systemu energetycznego, zakłada **rozwój inteligentnych sieci** (usprawniona kontrola i optymalizacja wykorzystania) oraz wdrażania rozwiązań AI w zarządzaniu systemem energetycznym, w tym do prognozowania zużycia, wykrywania awarii i planowania inwestycji. Planowane jest również wprowadzenie inteligentnych liczników energii.

Trzeci obszar stanowi **zarządzanie danymi**, niezbędnymi do wdrożenia inteligentnych usług energetycznych i sztucznej inteligencji. Działania będą miały na celu wypracowanie spójnego podejścia UE dotyczącego dostępu i transgranicznej wymiany danych dotyczących energii, umożliwiając m.in. trenowanie modeli AI i większą wydajność usług energetycznych.

Oprócz mapy drogowej, istotnym elementem jest również opublikowany w lipcu unijny **Plan Działania na Rzecz Elektryfikacji** zakładający podwojenie elektryfikacji końcowego zużycia energii elektrycznej (poprzez odejście od wykorzystania paliw kopalnych) z obecnych 23% do 46% do 2040 roku^{33,34}. Plan obejmuje zarówno transformację energetyczną przemysłu, jak również transport, ogrzewanie i magazynowanie energii. Pod względem rozwoju centrów danych kluczowe jest podpisanie trójstronnego porozumienia – pomiędzy Komisją Europejską, państwami członkowskimi i przedstawicielami sektora energetycznego – dotyczącego **budowy magazynów energii** i skutecznego wykorzystania odnawialnych źródeł energii. Według przyjętych założeń, do 2028 roku ma zostać zainstalowane około 45 GW nowych mocy magazynowania energii (wobec około 55 GW zainstalowanych na początku 2026 r.). Do 2030 r. łączna moc magazynów energii w UE ma wynieść około 200 GW. Całościowo ma to umożliwić podwojenie udziału magazynów w pokrywaniu szczytowego zapotrzebowania na energię elektryczną i pomóc w stabilizacji cen energii. W ramach porozumienia, Polska zadeklarowała plan zainstalowania 11GW³⁵. Wielkoskalowe magazyny są niezbędne w celu efektywnego wykorzystania rosnącej ilości energii wytwarzanej z OZE, jednak dopiero zaczynają powstawać – pod koniec 2025 w kraju zainstalowane było jedynie 0,9 GW mocy³⁶.

³² Działania te są prowadzone równolegle do inwestycji w modernizację i rozwój sieci przesyłowych, w tym w Polsce: <https://pie.net.pl/tygodnik-gospodarczy-39-2026-1-pazdziernika-2026-r/#tyg-mat-38205-5>

³³ Podsumowanie: https://energy.ec.europa.eu/topics/eus-energy-system/electrification_en

Akt prawny: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026DC0595&qid=1784715609929>

³⁴ Cel jest oceniany jako trudny do zrealizowania. Należy wziąć pod uwagę, że w samej Polsce wskaźnik elektryfikacji w 2024 r. wynosił 17 proc. i według założeń KPEiK miał osiągnąć unijną średnią (20%) dopiero w 2030 r. <https://pie.net.pl/tygodnik-gospodarczy-29-2026-23-lipca-2026-r/#tyg-mat-37738-6>

³⁵ https://energy.ec.europa.eu/publications/tripartite-agreement-energy-storage_en

³⁶ Warto zauważyć, że magazyny energii – w tym największy tego typu projekt powstający obecnie w Polsce – polegają na chińskiej technologii i współpracy m.in. z BYD Energy Storage. <https://zielonagospodarka.pl/w-siedlcach-powstanie-najwiekszy-magazyn-energii-w-polsce-zbuduja-go-portugalczyzy-z-chinczykami-23154>

Ważnym elementem działań jest również postęp w **raportowaniu i ocenie zużycia energii i wody przez centra danych**. Na podstawie unijnej dyrektywy o efektywności energetycznej, w 2024 roku przyjęto rozporządzenie nakładające na operatorów centrów danych o zainstalowanym zapotrzebowaniu mocy co najmniej 500 kW obowiązek przekazywania informacji i KPI do europejskiej bazy danych (dane są poufne i agregowane na poziomie każdego państwa członkowskiego)³⁷. We wrześniu 2026 r. Komisja przyjęła też projekt wspólnego unijnego systemu ratingowego dla centrów danych, który zostanie wdrożony w przyszłym roku (przyznane zostaną pierwsze etykiety)³⁸. Jednocześnie uruchomione zostały konsultacje nad wypracowaniem obowiązkowych standardów efektywności (PUE i WUE), z wnioskiem ustawodawczym przewidzianym na drugi kwartał 2027³⁹.

Na uwagę zasługuje również „AI Environmental Transparency Initiative” zaproponowana przez ONZ, w ramach której raportowanie śladu środowiskowego, w tym zużycia energii i wody ma być ogólnym obowiązkiem dla firm rozwijających sztuczną inteligencję. Jest to istotne, ponieważ obecnie brakuje jednolitych i obowiązkowych uzgodnień w tym obszarze⁴⁰.

Ustawa o systemach sztucznej inteligencji⁴¹

Ustawa o systemach sztucznej inteligencji, uchwalona w lipcu 2026 roku, ma zapewnić krajowe ramy dla stosowania unijnego Aktu o sztucznej inteligencji (AI Act). Kluczowe elementy ustawy obejmują ustanowienie Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI) jako organu nadzorującego rynek i prowadzącego postępowania oraz stworzenie ram dla rozwoju piaskownic regulacyjnych w ramach wsparcia rozwoju sztucznej inteligencji. Poniżej przedstawiamy szczegółowe streszczenie poszczególnych elementów ustawy.

ROZDZIAŁ 1: PRZEPISY OGÓLNE I ZAKRES STOSOWANIA

Ustawa określa krajowe ramy prawne i instytucjonalne służące wykonaniu unijnego rozporządzenia AI Act. Reguluje w szczególności:

1. Organizację i sposób nadzoru nad rynkiem systemów AI oraz modeli AI ogólnego przeznaczenia.
2. Zasady postępowania w sprawach o naruszenie AI Act oraz niniejszej ustawy.
3. Zasady akredytacji i notyfikacji jednostek oceniających zgodność.
4. Mechanizmy wspierające rozwój AI (m.in. piaskownice regulacyjne).
5. Zasady nakładania administracyjnych kar pieniężnych za naruszenia.

³⁷ https://eur-lex.europa.eu/eli/reg_del/2024/1364/2024-05-17

³⁸ https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1667

³⁹ https://energy.ec.europa.eu/news/minimum-performance-standards-data-centres-europe-public-consultation-launched-2026-09-21_en

⁴⁰ <https://www.reuters.com/legal/litigation/un-chief-calls-ai-firms-come-clean-environmental-costs-2026-06-23/>

⁴¹ <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260001003>

Wyłączenia ze stosowania ustawy:

- Sprawy obronności i bezpieczeństwa narodowego oraz działania służb specjalnych (ABW, AW, SKW, SWW). Kontrolę nad służbami w zakresie AI sprawuje Premier lub Minister – Koordynator Służb Specjalnych.
- Badań naukowych i prac rozwojowych (z wyjątkiem testów w warunkach rzeczywistych) oraz systemów wprowadzonych wyłącznie do tych celów przed wejściem w życie AI Act.
- Osoby fizyczne stosujące AI w celach wyłącznie osobistych (niezwiązanych z działalnością gospodarczą lub rolniczą).

ROZDZIAŁ 2: ORGANIZACJA NADZORU NAD RYNKIEM – KOMISJA ROZWOJU I BEZPIECZEŃSTWA AI

Głównym organem nadzoru rynku oraz pojedynczym punktem kontaktowym w rozumieniu AI Act staje się nowo utworzona Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (Komisja).

Zadania i kompetencje Komisji:

- Kontrola przestrzegania AI Act i ustawy, wydawanie decyzji i postanowień.
- Monitorowanie rynku, przeciwdziałanie zagrożeniom bezpieczeństwa oraz wspieranie innowacyjności i konkurencyjności.
- Opinie indywidualne: Podmioty obowiązane do stosowania AI Act (lub planujące takie działania) mogą złożyć wniosek o wydanie wiążącej opinii indywidualnej dotyczącej ich stanu faktycznego/przyszłego (opłata wynosi 150 zł, czas na wydanie: 30–60 dni).
- Wyjaśnienia ogólne: Komisja wydaje z urzędu lub na wniosek wyjaśnienia w celu zapewnienia jednolitego stosowania prawa.
- Prowadzenie piaskownic regulacyjnych oraz rejestru skarg.
- Współpraca z organami krajowymi (KNF, UOKiK, UODO, UKE, KRRiT, Prokurator Generalny i in.) oraz międzynarodowymi (Komisja Europejska, Rada ds. AI).

Skład i ustrój Komisji:

- Skład: Przewodniczący, 2 Zastępców oraz 4 członków wskazanych przez UOKiK, KNF, KRRiT i UKE.
- Przewodniczący Komisji: Powoływany przez Sejm za zgodą Senatu na 5-letnią kadencję (maksymalnie 2 kadencje). Zastępcy wyłaniani są w otwartym i konkurencyjnym naborze.
- Niezależność i bezstronność: Kierownictwo i członkowie są niezależni. Obowiązuje ich zakaz przynależności do partii politycznych, związków zawodowych, zakaz podejmowania zatrudnienia w podmiotach nadzorowanych oraz posiadania w nich udziałów/akcji.

Rada do spraw Sztucznej Inteligencji:

Przy Komisji działa Społeczna Rada do spraw Sztucznej Inteligencji – organ opiniotwórczo-doradczy składający się z 9–15 członków powoływanych na 2-letnią kadencję spośród kandydatów zgłoszonych m.in. przez RPO, RPD, izby gospodarcze, związki zawodowe, uczelnie i NGO.

ROZDZIAŁ 3: KONTROLA PRZESTRZEGANIA PRZEPISÓW O SZTUCZNEJ INTELIGENCJI (AI ACT)

Komisja przeprowadza kontrole planowe lub doraźne.

- Procedura: Zawiadomienie o kontroli doręcza się co najmniej 7 dni przed jej rozpoczęciem. Kontrola co do zasady odbywa się zdalnie; w przypadku zagrożenia dla życia, zdrowia lub praw podstawowych może być przeprowadzona stacjonarnie bez zachowania terminu 7 dni.
- Uprawnienia kontrolujących: Dostęp do dokumentów, systemów informatycznych, chmury obliczeniowej, kodów, żądanie wyjaśnień, sporządzanie kopii oraz rejestracja obrazu/dźwięku.
- Tajemnica adwokacka/radcowska: Materiały obejmujące poufną komunikację z prawnikiem chroniącym praw kontrolowanego są wyłączone z kontroli (spory rozstrzyga Sąd Okręgowy w Warszawie – Sąd Ochrony Konkurencji i Konsumentów).
- Zalecenia pokontrolne: W przypadku wykrycia nieprawidłowości Komisja wzywa do ich usunięcia (termin min. 30 dni). Niewykonanie zaleceń skutkuje wszczęciem formalnego postępowania.

ROZDZIAŁ 4 & 5: POSTĘPOWANIE PRZED ORGANEM NADZORU I INSTYTUCJA UKŁADU

Postępowanie w sprawie naruszeń:

- Wszczynane z urzędu (np. po kontroli, rozpatrzeniu skargi obywatela) lub na wniosek uprawnionych organów/Rady.
- Każda osoba fizyczna lub prawna ma prawo wnieść skargę do Komisji na system AI.
- Ostrzeżenia i nakazy: W toku postępowania Komisja może wydać ostrzeżenie, nakazać zablokowanie dostępu do systemu lub realizację obowiązków informacyjnych.
- Środki pilne: Jeśli system AI stwarza bezpośrednie ryzyko dla życia, zdrowia lub praw podstawowych, Komisja wydaje decyzję nakazującą natychmiastowe zaprzestanie jego stosowania lub wycofanie z rynku (z rygorem natychmiastowej wykonalności).
- Postępowanie powinno trwać maksymalnie 6 miesięcy (lub 7 dni w przypadku bezpośredniego ryzyka). Od decyzji przysługuje odwołanie do SOKiK.

Układ w sprawie warunków nadzwyczajnego złagodzenia sankcji – nowatorski mechanizm polubowny pozwalający na polubowne zakończenie sprawy:

- Jeśli strona zaprzestała naruszenia, ujawniła wszelkie istotne okoliczności i zobowiązała się do naprawienia szkody, Komisja może zawrzeć z nią Układ.
- Korzyści dla strony: Obniżenie administracyjnej kary pieniężnej o 20% do 70% (a w przypadku dobrowolnego zgłoszenia naruszenia z własnej inicjatywy – od 30% do nawet 90% lub całkowite odstąpienie od kary).
- Zawarcie układu oznacza zrzeczenie się prawa do odwołania do sądu.

ROZDZIAŁ 6: JEDNOSTKI NOTYFIKOWANE I AKREDYTACJA

- Organem notyfikującym w Polsce jest Minister właściwy do spraw informatyzacji.
- Polskie Centrum Akredytacji (PCA) odpowiada za opracowanie programów akredytacji oraz ocenę jednostek wnioskujących o status jednostki notyfikowanej do oceny zgodności systemów AI z wymogami AI Act.

ROZDZIAŁ 7: ŚRODKI WSPIERAJĄCE INNOWACYJNOŚĆ – PIASKOWNICE REGULACYJNE

- Piaskownica regulacyjna AI: Środowisko testowe tworzone przez Komisję (na okres od 6 do 12 miesięcy), umożliwiające bezpieczne rozwijanie i testowanie innowacyjnych systemów AI.
- Uczestnicy piaskownicy mogą uzyskać odstępstwa od niektórych formalnych wymogów AI Act (np. w zakresie pełnej dokumentacji technicznej czy oceny zgodności) na czas testów.
- Udział dla MŚP jest nieodpłatny.
- Rejestracja odbywa się w drodze konkursów ogłaszanych przez Komisję.
- Po pomyślnym ukończeniu piaskownicy podmiot ma prawo do uzyskania przyspieszonej opinii indywidualnej w ciągu 14 dni.
- Minister wspiera badania nad AI, przeznaczając dotacje celowe i środki UE na projekty rozwojowe.

ROZDZIAŁ 8: ADMINISTRACYJNE KARY PIENIĘŻNE I PRZEPISY KARNE

Kary administracyjne:

- Kary nakładane są na podstawie rozdziału XII AI Act. Przeliczenia stawek wyrażonych w EUR na PLN dokonuje się według kursu NBP z dnia 28 stycznia danego roku.
- Środki z kar stanowią dochód budżetu państwa.
- Ulgi: Komisja może obniżyć karę o 10%–50%, jeżeli podmiot w ciągu 3 miesięcy od decyzji wdroży zalecenia, a naruszenie nie spowodowało śmierci ani poważnego uszczerbku na zdrowiu. Możliwe jest też rozłożenie kary na raty lub odroczenie spłaty.

Sankcje karne/wykroczeniowe:

- Kara ograniczenia wolności albo grzywny grozi za:
 1. Utrudnianie lub udaremnianie przeprowadzenia kontroli lub czynności postępowania.
 2. Niewykonanie decyzji Komisji nakazującej zaprzestanie stosowania lub wycofanie z rynku systemu AI stwarzającego bezpośrednie zagrożenie.
- Orzekanie następuje w trybie Kodeksu postępowania w sprawach o wykroczenia.

AI Act⁴²

ROZDZIAŁ I: PRZEPISY OGÓLNE, CEL I ZAKRES STOSOWANIA

- **Przedmiot i cele rozporządzenia:**

Głównym celem aktu jest poprawa funkcjonowania rynku wewnętrznego Unii Europejskiej oraz promowanie rozwoju i upowszechniania zorientowanej na człowieka, godnej zaufania sztucznej inteligencji (AI). Regulacja dąży do zapewnienia wysokiego poziomu ochrony zdrowia, bezpieczeństwa oraz praw podstawowych zawartych w Karcie Praw Podstawowych UE (w tym praworządności, demokracji i ochrony środowiska) przed szkodliwymi skutkami systemów AI, przy jednoczesnym wspieraniu innowacji i swobodnego przepływu produktów oraz usług na rynku wewnętrznym.

- **Zakres stosowania i ekstraterytorialność:**

Przepisy mają zastosowanie do:

1. Dostawców (*providers*) wprowadzających do obrotu lub oddających do użytku systemy AI bądź modele AI ogólnego przeznaczenia (GPAI) w UE, niezależnie od tego, czy mają siedzibę w UE, czy w kraju trzecim.
2. Podmiotów stosujących (*deployers*) systemy AI mających siedzibę lub znajdujących się w granicach UE.
3. Dostawców i podmiotów stosujących z państw trzecich, jeżeli wyniki (*outputs*) wytworzone przez system AI są wykorzystywane na terytorium Unii.
4. Importerów, dystrybutorów, producentów produktów z wbudowanymi systemami AI oraz upoważnionych przedstawicieli.

- **Wyłączenia z zakresu stosowania:**

1. Systemy AI wykorzystywane wyłącznie do celów wojskowych, obronnych lub bezpieczeństwa narodowego.

⁴² <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689>

2. Działalność badawczo-rozwojowa (B+R) oraz testowanie systemów lub modeli AI przed ich wprowadzeniem do obrotu (z wyjątkiem testów w warunkach rzeczywistych).
3. Korzystanie z AI przez osoby fizyczne w celach czysto osobistych i pozazawodowych.
4. Systemy udostępniane na bezpłatnych licencjach open-source (z wyjątkiem systemów zakazanych lub wysokiego ryzyka).

- **Definicje systemowe:**

1. **System AI:** System maszynowy zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po wdrożeniu, który na podstawie danych wejściowych wnioskuje, jak generować wyniki (predykcje, treści, zalecenia lub decyzje) wpływające na środowisko fizyczne lub wirtualne.
2. **Model AI Ogólnego Przeznaczenia (GPAI):** Model AI wykazujący znaczną ogólność i zdolny do kompetentnego wykonywania szerokiego zakresu odrębnych zadań, niezależnie od sposobu wprowadzania na rynek i który można zintegrować z różnymi systemami lub aplikacjami niższego szczebla – z wyłączeniem modeli AI, które są wykorzystywane na potrzeby badań, rozwoju i tworzenia prototypów przed wprowadzeniem ich do obrotu.

ROZDZIAŁ II: ZAKAZANE PRAKTYKI W ZAKRESIE SZTUCZNEJ INTELIGENCJI

Rozporządzenie kategorycznie zakazuje wprowadzania do obrotu, oddawania do użytku lub stosowania systemów AI uznanych za stwarzające niedopuszczalne ryzyko:

- **Techniki podprogowe i manipulacyjne:** Stosowanie bodźców podprogowych lub celowych technik manipulacyjnych zmierzających do znaczącej zmiany zachowania człowieka w sposób, który wyrządza lub może wyrządzić poważną szkodę fizyczną, psychiczną lub finansową.
- **Wykorzystywanie słabości osób:** Eksploatacja podatności wynikających z wieku, niepełnosprawności lub szczególnej sytuacji społeczno-ekonomicznej.
- **Ocena społeczna (Social Scoring):** Ocena lub klasyfikacja osób fizycznych na podstawie zachowań społecznych lub cech osobowości, prowadząca do nieuzasadnionego lub dyskryminującego traktowania w innych kontekstach społecznych.
- **Predykcja przestępczości (Predictive Policing):** Ocena ryzyka popełnienia przestępstwa oparta wyłącznie na profilowaniu cech osobowościowych człowieka (z wyłączeniem wsparcia ocen opartych na obiektywnych i weryfikowalnych faktach).
- **Pozyskiwanie wizerunków twarzy (Untargeted Scraping):** Tworzenie lub rozbudowa baz danych do rozpoznawania twarzy poprzez masowe, nieukierunkowane pobieranie zdjęć z Internetu lub monitoringu CCTV.

- **Wnioskowanie o emocjach:** Wykorzystywanie AI do rozpoznawania emocji pracowników w miejscu pracy oraz uczniów w instytucjach edukacyjnych (wyjątek stanowią względy medyczne i bezpieczeństwa).
- **Kategoryzacja biometryczna:** Wnioskowanie na podstawie danych biometrycznych o cechach wrażliwych (rasa, poglądy polityczne, przekonania religijne, orientacja seksualna, przynależność związkowa).
- **Zdalna identyfikacja biometryczna w czasie rzeczywistym:** Stosowanie systemów rozpoznawania twarzy na żywo w przestrzeni publicznej przez organy ścigania, z wyjątkiem ściśle zdefiniowanych sytuacji (poszukiwanie ofiar uprowadzeń, zapobieganie bezpośrednim zagrożeniom terrorystycznym, ściganie sprawców ciężkich przestępstw zagrożonych karą min. 4 lat pozbawienia wolności na podstawie uprzedniego zezwolenia sądowego).

ROZDZIAŁ III: SYSTEMY AI WYSOKIEGO RYZYKA

Sekcja 1: Klasyfikacja Systemów Wysokiego Ryzyka

System AI uznaje się za system wysokiego ryzyka, jeżeli:

1. Jest przeznaczony do wykorzystania jako element bezpieczeństwa produktu objętego prawodawstwem harmonizacyjnym UE (np. wyroby medyczne, maszyny, zabawki, dźwigi, wyposażenie morskie) i podlega ocenie zgodności przez stronę trzecią.
2. Należy do obszarów krytycznych określonych w **Załączniku III**:
 - **Biometria:** Zdalna identyfikacja biometryczna post factum, kategoryzacja biometryczna na podstawie cech chronionych, rozpoznawanie emocji.
 - **Infrastruktura krytyczna:** Związany z bezpieczeństwem zarządzanie ruchem drogowym, zaopatrzeniem w wodę, gaz, ciepło i energię elektryczną oraz krytyczną infrastrukturą cyfrową.
 - **Edukacja i szkolenie zawodowe:** Ocena rekrutacyjna, przydział do instytucji, ocena wyników nauki oraz monitorowanie uczciwości egzaminów.
 - **Zatrudnienie i zarządzanie pracownikami:** Rekrutacja, selekcja kandydatów, podejmowanie decyzji o awansach, zwolnieniach, przydzielanie zadań oraz monitorowanie wydajności pracowników.
 - **Dostęp do podstawowych usług prywatnych i publicznych:** Ocena wniosków o świadczenia socjalne, scoring kredytowy, wycena ubezpieczeń zdrowotnych i na życie, priorytetyzacja zgłoszeń w ramach służb ratunkowych.
 - **Ściganie przestępstw:** Ocena wariograficzna, analiza dowodów, profilowanie osób w trakcie postępowań przygotowawczych.
 - **Zarządzanie migracją, azylem i kontrolą granic:** Ocena ryzyka osób wjeżdżających, analiza wniosków wizowych i azylantów.
 - **Sprawowanie wymiaru sprawiedliwości i procesy demokratyczne:** Wspomaganie sędziów w wyszukiwaniu i interpretacji faktów/prawa oraz systemy przeznaczone do wpływania na wyniki wyborów lub referendów.

Sekcja 2: Obowiązkowe Wymogi dla Systemów Wysokiego Ryzyka

- **System zarządzania ryzykiem:** Wdrożenie ciągłego, iteracyjnego procesu identyfikacji, analizy i minimalizowania ryzyka przez cały cykl życia systemu AI.
- **Zarządzanie danymi:** Zbiory danych treningowych, walidacyjnych i testowych muszą spełniać wysokie standardy jakości (być odpowiednio reprezentatywne, adekwatne, wolne od błędów oraz przebadane pod kątem stronniczości i dyskryminacji).
- **Dokumentacja techniczna:** Sporządzenie i aktualizowanie szczegółowej dokumentacji wykazującej zgodność z wymogami przed wprowadzeniem produktu do obrotu.
- **Rejestrowanie zdarzeń:** Automatyczne zapisywanie zdarzeń operacyjnych zapewniające identyfikowalność działania systemu przez minimalny okres 6 miesięcy.
- **Przejrzystość i informowanie użytkowników:** Projektowanie systemu umożliwiające interpretację wyników oraz dostarczenie przejrzystej instrukcji obsługi określającej specyfikację, wydajność i ograniczenia AI.
- **Nadzór ze strony człowieka:** Wyposażenie systemu w interfejsy umożliwiające kontrolę, zapobieganie błędowi automatyzacji oraz możliwość natychmiastowego zatrzymania operacji.
- **Dokładność, solidność i cyberbezpieczeństwo:** Odporność systemu na błędy, awarie, usterki oraz próby manipulacji danymi wejściowymi.

Sekcja 3: Obowiązki Dostawców i Podmiotów Stosujących

- **Dostawcy:** Muszą wdrożyć system zarządzania jakością, przechowywać dokumentację techniczną przez 10 lat, przeprowadzić procedurę oceny zgodności, umieścić oznakowanie CE, wystawić deklarację zgodności UE oraz zarejestrować system w unijnej bazie danych.
- **Podmioty stosujące:** Zobowiązani są do użytkowania systemów zgodnie z instrukcją, powierzenia nadzoru osobom przeszkolonym, ciągłego monitorowania działania, przechowywania automatycznych logów oraz informowania pracowników i obywateli o poddawaniu ich działaniu systemów wysokiego ryzyka.
- **Ocena skutków dla praw podstawowych:** Podmioty sektora publicznego oraz wyznaczone podmioty prywatne (np. banki, ubezpieczyciele) muszą przed wdrożeniem systemu wysokiego ryzyka przeprowadzić formalną ocenę jego wpływu na prawa podstawowe obywateli.

Sekcja 4: Jednostki Notyfikowane i Ocena Zgodności

Określa zasady wyznaczania przez państwa członkowskie organów notyfikujących i niezależnych jednostek notyfikowanych odpowiedzialnych za przeprowadzanie zewnętrznych ocen zgodności systemów AI wysokiego ryzyka przed ich dopuszczeniem do obrotu.

ROZDZIAŁ IV: OBOWIĄZKI W ZAKRESIE PRZEJRZYSTOŚCI DLA NIEKTÓRYCH SYSTEMÓW AI

Niezależnie od kwalifikacji ryzyka, określone kategorie systemów AI podlegają obowiązkowym wymogom informacyjnym:

1. **Interakcja z ludźmi:** Systemy AI wchodzące w bezpośrednią interakcję z ludźmi (np. chatboty, wirtualni asystenci) muszą wyraźnie informować użytkownika, że rozmawia z maszyną.
2. **Oznaczanie treści syntetycznych:** Systemy generujące treść tekstową, audio, obraz lub wideo muszą kodować swoje wyniki w formacie nadającym się do odczytu masowego i umożliwiającym wykrycie ich syntetycznego pochodzenia (np. poprzez cyfrowe znaki wodne).
3. **Ujawnianie treści typu Deepfake:** Podmioty stosujące AI do generowania zmanipulowanych obrazów, nagrań dźwiękowych lub wideo, które łudząco przypominają prawdziwe osoby, obiekty lub wydarzenia (*deepfake*), mają obowiązek jawnego i widocznego oznaczania tych treści jako sztucznie wytworzonych.
4. **Teksty informacyjne:** Teksty generowane przez AI publikowane w celu informowania opinii publicznej o sprawach leżących w interesie społecznym muszą być oznaczone jako wygenerowane przez AI, chyba że podlegają pełnej kontroli redakcyjnej człowieka.

ROZDZIAŁ V: MODELE AI OGÓLNEGO PRZEZNACZENIA (GPAI MODELS)

W reakcji na rozwój generatywnej sztucznej inteligencji AI Act wprowadza się dwupoziomowy reżim prawny dla modeli stanowiących fundament dla aplikacji niższych szczebli:

1. Standardowe Obowiązki Dostawców Modeli GPAI

Każdy dostawca modelu GPAI wprowadzanego do obrotu w UE zobowiązany jest do:

- Sporządzenia i aktualizowania dokumentacji technicznej modelu dla Urzędu ds. AI.
- Przekazywania informacji i dokumentacji dostawcom niższych szczebli, integrującym model ze swoimi aplikacjami.
- Wdrożenia polityki poszanowania unijnego prawa autorskiego.
- Sporządzania i podawania do wiadomości publicznej szczegółowego podsumowania treści wykorzystanych do trenowania modelu.

2. Modele GPAI o Ryzyku Systemowym

- **Kryterium kwalifikacji:** Model GPAI uznaje się za stwarzający ryzyko systemowe, jeśli posiada zdolności dużego oddziaływania (*high impact capabilities*) – skumulowana moc obliczeniowa użyta do jego trenowania przekracza 10^{25} operacji zmiennoprzecinkowych (FLOPs) – lub gdy Komisja Europejska podejmie indywidualną decyzję kwalifikacyjną.

- **Dodatkowe obowiązki:** Dostawcy modeli GPAI o ryzyku systemowym muszą przeprowadzać ewaluacje modeli, wykonywać testy odbiorcze (*red-teaming*), oceniać i łagodzić potencjalne ryzyka systemowe na poziomie UE, zgłaszać poważne incydenty do Urzędu ds. AI oraz zapewniać odpowiedni poziom cyberbezpieczeństwa wag i infrastruktury modelu.

ROZDZIAŁ VI: ŚRODKI WSPIERAJĄCE INNOWACJE

- **Piaskownice Regulacyjne AI:** Państwa członkowskie mają obowiązek utworzenia co najmniej jednej piaskownicy regulacyjnej na poziomie krajowym. Piaskownice stanowią kontrolowane środowiska testowe umożliwiające rozwijanie, trenowanie i walidację innowacyjnych systemów AI pod ścisłym nadzorem organów regulacyjnych przed ich wprowadzeniem na rynek.
- **Testy w warunkach rzeczywistych:** Umożliwienie prowadzenia testów systemów wysokiego ryzyka w otoczeniu rzeczywistym poza laboratoriami przy zastosowaniu rygorystycznych gwarancji i po uzyskaniu świadomej zgody uczestników.
- **Ułatwienia dla MŚP i startupów:** Dedykowane środki wsparcia obejmujące priorytetowy dostęp do piaskownic regulacyjnych, obniżone opłaty za procedury oceny zgodności, uproszczone wzory dokumentacji technicznej dla mikro- i małych przedsiębiorstw oraz organizację szkoleń.

ROZDZIAŁ VII, VIII, IX: ZARZĄDZANIE, NADZÓR RYNKU I EGZEKWOWANIE PRZEPISÓW

1. Architektura Instytucjonalna UE

- **Europejski Urząd ds. Sztucznej Inteligencji (EU AI Office):** Utworzony w strukturach Komisji Europejskiej; odpowiada za nadzór nad modelami GPAI, egzekwowanie przepisów i wspieranie innowacji.
- **Europejska Rada ds. Sztucznej Inteligencji (AI Board):** Składa się z przedstawicieli państw członkowskich; wydaje opinie, doradza Komisji i zapewnia spójność stosowania prawa w całej Unii.
- **Panel Naukowy Niezależnych Ekspertów:** Wspiera Urząd ds. AI w ewaluacji modeli GPAI i wydaje ostrzeżenia o ryzykach systemowych.
- **Forum Doradcze:** Ciało reprezentujące przemysł, MŚP, środowiska akademickie oraz społeczeństwo obywatelskie.

2. Nadzór Rynku na Poziomie Krajowym

Państwa członkowskie wyznaczają właściwe organy krajowe (organy notyfikujące oraz organy nadzoru rynku) odpowiedzialne za kontrolę wprowadzanych systemów AI, rozpatrywanie skarg, prowadzenie kontroli oraz podejmowanie środków naprawczych na rynku lokalnym.

ROZDZIAŁ X, XI, XII: KODEKSY POSTĘPOWANIA, POUFNOŚĆ I SANKCJE FINANSOWE

- **Kodeksy postępowania:** Zachęcanie dostawców systemów AI niebędących systemami wysokiego ryzyka do dobrowolnego przyjmowania zasad etycznych, wymogów zrównoważonego rozwoju oraz wytycznych dotyczących dostępności.
- **Poufność informacji:** Wszystkie strony zaangażowane w stosowanie aktu mają obowiązek zachowania poufności tajemnic handlowych i praw własności intelektualnej.
- **Wysokość administracyjnych kar pieniężnych:** Sankcje finansowe za naruszenie przepisów rozporządzenia należą do najwyższych w prawie unijnym i są stopniowalne:
 - Naruszenie zakazanych praktyk AI – do 35 000 000 EUR lub 7% globalnego obrotu.
 - Naruszenie wymogów ws. wysokiego ryzyka – do 15 000 000 EUR lub 3% globalnego obrotu.
 - Podanie nieprawdziwych informacji organom – do 7 500 000 EUR lub 1,5% globalnego obrotu.

ROZDZIAŁ XIII: PRZEPISY KOŃCOWE I HARMONOGRAM WDRAŻANIA

Rozporządzenie weszło w życie w sierpniu 2024 r., a jego stosowanie podzielono na następujące etapy (Art. 113):

- **Luty 2025 r.:** Obowiązywanie zakazów dotyczących niedozwolonych praktyk AI.
- **Sierpień 2026 r.:** Zastosowanie większości obowiązujących przepisów, w tym dotyczących modeli GPAI, organów zarządczych, wymogów przejrzystości oraz przepisów o karach.
- **Sierpień 2027 r.:** Obowiązek wdrożenia piaskownic regulacyjnych.
- **Grudzień 2027 r.:** Zastosowanie wymogów dla systemów wysokiego ryzyka z Załącznika III.
- **Sierpień 2028 r.:** Zastosowanie wymogów dla systemów wysokiego ryzyka wbudowanych w produkty objęte załącznikiem I.

Cyber Resilience Act (CRA)

Cyber Resilience Act (CRA), czyli unijne rozporządzenie dotyczące cyberodporności produktów z elementami cyfrowymi, wprowadza jednolite w całej Unii Europejskiej wymagania dotyczące ich cyberbezpieczeństwa. Celem regulacji jest zwiększenie bezpieczeństwa oprogramowania i urządzeń oraz zapewnienie skuteczniejszego reagowania na podatności i incydenty.

Regulacja została wprowadzona m.in. w odpowiedzi na rosnącą liczbę podatności i cyberataków dotyczących produktów cyfrowych oraz brak jednolitych, horyzontalnych

wymagań dotyczących cyberbezpieczeństwa takich produktów na rynku UE. Przed CRA wymagania dotyczące bezpieczeństwa były w dużej mierze rozproszone pomiędzy regulacje sektorowe, a obowiązki producentów dotyczące zarządzania podatnościami po wprowadzeniu produktu na rynek nie były jednolicie określone.

CRA zmienia ten model, przenosząc większą odpowiedzialność na producentów. Cyberbezpieczeństwo ma być uwzględniane już na etapie projektowania produktu, a następnie utrzymywane przez cały okres jego wsparcia. Producent odpowiada nie tylko za bezpieczeństwo produktu w momencie wprowadzenia go na rynek, ale również za zarządzanie podatnościami i zapewnienie odpowiednich aktualizacji.

CRA obejmuje m.in. oprogramowanie, sprzęt komputerowy oraz produkty wykorzystujące rozwiązania do zdalnego przetwarzania danych. Regulacja nie obejmuje niektórych kategorii, m.in. wyrobów medycznych, pojazdów, systemów wojskowych oraz oprogramowania świadczonego wyłącznie jako usługa (SaaS).

O tym, czy produkt jest objęty CRA, decyduje przede wszystkim jego charakter i funkcjonalność. Regulacja obejmuje produkty z elementami cyfrowymi, których przeznaczenie lub możliwe do przewidzenia wykorzystanie zakłada bezpośrednio lub pośrednio połączenie logiczne albo fizyczne z urządzeniem lub siecią.

Wyłączenia dotyczą przede wszystkim produktów, dla których obowiązują już szczegółowe regulacje sektorowe. Obejmują one m.in. określone wyroby medyczne, produkty motoryzacyjne, produkty lotnicze i wyposażenie morskie. Wyłączone są również produkty opracowane lub zmodyfikowane wyłącznie do celów obronnych lub bezpieczeństwa narodowego oraz produkty przeznaczone do przetwarzania informacji niejawnych.

Samo świadczenie usługi SaaS nie oznacza automatycznie objęcia CRA. CRA może natomiast obejmować funkcjonalność chmurową, która jest integralną częścią produktu z elementami cyfrowymi i została zaprojektowana przez producenta lub na jego odpowiedzialność.

Jednym z kluczowych elementów CRA jest obowiązek systematycznego zarządzania podatnościami przez cały cykl życia produktu. Producenci będą zobowiązani m.in. do:

1. przeprowadzania oceny ryzyka cyberbezpieczeństwa;
2. uwzględniania bezpieczeństwa już na etapie projektowania i rozwoju produktu;
3. monitorowania i usuwania wykrytych podatności;
4. prowadzenia odpowiedniej dokumentacji technicznej;
5. zapewnienia mechanizmów aktualizacji bezpieczeństwa.

Do tych obowiązków należy również m.in. prowadzenie polityki skoordynowanego ujawniania podatności, zapewnienie mechanizmu zgłaszania podatności, identyfikowanie i dokumentowanie komponentów oprogramowania oraz – w odpowiednim zakresie – przygotowanie software bill of materials (SBOM).

Od 11 września 2026 r. producenci mają również obowiązek zgłaszania aktywnie wykorzystywanych podatności oraz poważnych incydentów dotyczących produktów z elementami cyfrowymi. Wczesne ostrzeżenie należy przekazać w ciągu 24 godzin, a pełne zgłoszenie w ciągu 72 godzin od uzyskania informacji o podatności lub incydencie.

Zgłoszenia są składane za pośrednictwem unijnej Single Reporting Platform prowadzonej przez ENISA. W przypadku aktywnie wykorzystywanej podatności przewidziano również dalsze raportowanie, w tym raport końcowy po udostępnieniu środka zaradczego.

CRA przewiduje również domyślną możliwość stosowania automatycznych aktualizacji bezpieczeństwa, przy jednoczesnym zachowaniu przez użytkownika możliwości ich odroczenia lub rezygnacji. Producent powinien ponadto zapewnić wsparcie produktu przez co najmniej pięć lat, chyba że przewidywany okres jego użytkowania jest krótszy.

Obowiązek dotyczący automatycznych aktualizacji nie ma charakteru absolutnego – przewidziano wyjątki m.in. dla określonych produktów przeznaczonych do integracji z innymi produktami oraz profesjonalnych środowisk ICT, w których automatyczna aktualizacja mogłaby zakłócić działanie infrastruktury.

Dla producentów oprogramowania i sprzętu nowe przepisy oznaczają konieczność uwzględnienia cyberbezpieczeństwa w całym procesie projektowania, wdrażania, utrzymania i aktualizacji produktu. Istotne będzie również przygotowanie wewnętrznych procedur dotyczących identyfikacji, obsługi i raportowania podatności oraz incydentów.

W praktyce przedsiębiorcy powinni również przygotować procedury pozwalające na spełnienie bardzo krótkich terminów raportowania – przede wszystkim 24 i 72 godzin – oraz wyznaczyć osoby odpowiedzialne za obsługę zgłoszeń i kontakt z właściwymi organami.

Z perspektywy użytkowników biznesowych regulacja powinna zwiększyć przejrzystość i bezpieczeństwo wykorzystywanych produktów cyfrowych, m.in. poprzez zapewnienie dłuższego wsparcia oraz regularnych poprawek bezpieczeństwa.

CRA przewiduje również mechanizmy nadzoru rynku. Organy nadzoru mogą kontrolować zgodność produktów z wymaganiami, żądać informacji i dokumentacji oraz podejmować działania w odniesieniu do produktów niespełniających wymogów, włącznie z ograniczeniem ich dostępności na rynku.

Rozporządzenie przewiduje wysokie maksymalne poziomy kar. Za określone najpoważniejsze naruszenia kara może wynieść do 15 mln euro lub 2,5% całkowitego światowego rocznego obrotu przedsiębiorstwa z poprzedniego roku obrotowego – zależnie od tego, która kwota jest wyższa. Za inne naruszenia przewidziano maksymalnie 10 mln euro lub 2% światowego obrotu, a za przekazywanie nieprawidłowych, niekompletnych lub wprowadzających w błąd informacji – do 5 mln euro lub 1% światowego obrotu.

Szczegółowe zasady nakładania sankcji są określone również na poziomie państw członkowskich. Sankcje powinny być skuteczne, proporcjonalne i odstraszające.

Wdrożenie CRA jest etapowe. Najważniejsze terminy to:

1. 10 grudnia 2024 r. – wejście rozporządzenia w życie;
2. 11 czerwca 2026 r. – rozpoczęcie stosowania przepisów dotyczących notyfikacji jednostek oceny zgodności;
3. 11 września 2026 r. – rozpoczęcie stosowania obowiązków raportowania aktywnie wykorzystywanych podatności i poważnych incydentów;
4. 11 grudnia 2027 r. – rozpoczęcie pełnego stosowania zasad CRA, w tym zasadniczych wymogów dotyczących projektowania, produkcji, oceny zgodności, dokumentacji i zarządzania podatnościami.

Oznacza to, że 11 września 2026 r. nie jest datą pełnego wdrożenia CRA. Jest to pierwszy istotny termin dla producentów, związany z raportowaniem podatności i incydentów. Dla większości producentów najważniejszym terminem pozostaje 11 grudnia 2027 r.

Małe i mikroprzedsiębiorstwa

CRA nie przewiduje generalnego zwolnienia mikroprzedsiębiorstw i małych przedsiębiorstw z obowiązków. Jeżeli taki podmiot jest producentem produktu objętego CRA, musi co do zasady spełnić wymagania rozporządzenia.

Jednocześnie przewidziano rozwiązania mające ułatwić MŚP dostosowanie się do regulacji. Państwa członkowskie mogą organizować szkolenia, działania informacyjne, testowanie produktów, wsparcie w ocenie zgodności i piaskownice regulacyjne. Komisja Europejska może również przygotowywać uproszczone materiały i dokumentację dostosowane do potrzeb mikro- i małych przedsiębiorstw.

Szczególne rozwiązanie dotyczy obowiązków raportowania: mikroprzedsiębiorstwa i małe przedsiębiorstwa nie mogą zostać ukarane za niedochowanie określonych 24-godzinnych terminów raportowania. Nie oznacza to jednak zwolnienia z pozostałych obowiązków CRA.

Ustawa o zarządzaniu danymi (Data Governance Act)

23 lipca 2026 r. weszła w życie ustawa o zarządzaniu danymi, która uzupełnia polskie ramy prawne dotyczące stosowania unijnego Data Governance Act (DGA). Regulacja ma na celu stworzenie warunków do bezpiecznego, uporządkowanego i efektywnego udostępniania oraz wykorzystywania danych, a także zwiększenie zaufania do wymiany danych pomiędzy przedsiębiorstwami, obywatelami i podmiotami publicznymi.

Sama regulacja unijna obowiązuje już od 24 września 2023 r.; polska ustawa nie wprowadza więc od tej daty nowego, generalnego obowiązku dla wszystkich przedsiębiorców, lecz

przede wszystkim ustanawia krajowe organy, procedury i sankcje potrzebne do pełnego stosowania DGA w Polsce.

Z perspektywy przedsiębiorstw szczególne znaczenie ma wprowadzenie ram prawnych dla usług pośrednictwa w dostępie do danych. Pośrednicy mają umożliwiać bezpieczną wymianę zarówno danych osobowych, jak i nieosobowych, działając w sposób neutralny i bezstronny. Usługa pośrednictwa danych polega przede wszystkim na ułatwianiu nawiązywania relacji pomiędzy podmiotami posiadającymi dane a ich potencjalnymi użytkownikami. Pośrednik może zapewniać m.in. infrastrukturę do bezpiecznego przekazywania danych, mechanizmy uzyskiwania zgód lub zezwoleń czy anonimizacji i pseudonimizacji. Nie może jednak wykorzystywać danych będących przedmiotem pośrednictwa do własnych celów – jego działalność powinna być neutralna wobec stron wymiany.

Podmioty zamierzające świadczyć takie usługi w UE muszą dokonać zgłoszenia do właściwego organu krajowego. W Polsce organem właściwym jest Prezes UODO. Pośrednik musi również spełniać określone w DGA wymogi dotyczące m.in. neutralności, bezpieczeństwa danych, rozdzielenia usługi pośrednictwa od innych działalności oraz zapobiegania nieuprawnionemu dostępowi do danych.

Regulacja przewiduje również możliwość dobrowolnego udostępniania danych w celach altruistycznych, m.in. na potrzeby badań naukowych lub medycznych. Organizacje zajmujące się takim pośrednictwem będą podlegały rejestracji oraz nadzorowi UODO. Dla przedsiębiorstw oznacza to powstanie dodatkowego, formalnie uregulowanego mechanizmu dobrowolnego przekazywania danych na cele realizujące interes publiczny.

Istotnym elementem nowych regulacji są również zasady dostępu do chronionych danych pozostających w dyspozycji podmiotów publicznych. Chodzi m.in. o dane objęte tajemnicą przedsiębiorstwa, prawami własności intelektualnej lub ochroną danych osobowych. DGA ustanawia procedury umożliwiające przedsiębiorcom i innym uprawnionym podmiotom występowanie o dostęp do takich zasobów, przy jednoczesnym obowiązku zachowania poufności oraz poszanowania praw osób trzecich.

DGA nie oznacza jednak automatycznego prawa przedsiębiorcy do uzyskania takich danych. Podmiot publiczny może określić warunki ich ponownego wykorzystania, które powinny być przejrzyste, proporcjonalne, niedyskryminacyjne i obiektywnie uzasadnione. W zależności od rodzaju danych dostęp może być uzależniony m.in. od ich anonimizacji, agregacji lub modyfikacji albo od korzystania z bezpiecznego środowiska przetwarzania kontrolowanego przez podmiot publiczny.

W praktyce oznacza to, że przedsiębiorstwo chcące korzystać z takich danych powinno uwzględnić w swoich procedurach m.in. ocenę podstawy prawnej przetwarzania danych osobowych, zasady minimalizacji i ograniczenia celu, wymogi dotyczące poufności i bezpieczeństwa oraz ograniczenia dotyczące dalszego udostępniania danych.

Ustawa określa ponadto kompetencje polskich organów odpowiedzialnych za stosowanie DGA. Prezes UODO został wskazany jako organ właściwy m.in. w zakresie usług pośrednictwa danych, rejestracji organizacji altruizmu danych oraz wybranych obowiązków dotyczących przekazywania danych nieosobowych do państw trzecich.

Prezes UODO uzyskuje w tym zakresie nowe kompetencje nadzorcze. Może m.in. monitorować przestrzeganie wymogów przez dostawców usług pośrednictwa danych, żądać informacji i dokumentów niezbędnych do kontroli oraz podejmować działania w przypadku stwierdzenia naruszeń. W przypadku poważnych lub powtarzających się naruszeń możliwe jest również zawieszenie lub zaprzestanie świadczenia usługi.

Polska ustawa przewiduje również konkretne sankcje finansowe. W przypadku dostawcy usług pośrednictwa danych kara może wynieść do 200 tys. zł za naruszenie obowiązku zgłoszenia oraz do 2 mln zł za naruszenie warunków świadczenia usług pośrednictwa. Uznana organizacja altruizmu danych może zostać ukarana karą do 20 tys. zł, natomiast za naruszenie określonych obowiązków dotyczących przekazywania danych nieosobowych do państw trzecich kara może wynieść do 2 mln zł.

Przy ustalaniu wysokości kary Prezes UODO bierze pod uwagę m.in. charakter, wagę, skalę i czas trwania naruszenia, działania podjęte w celu usunięcia jego skutków oraz możliwości finansowe podmiotu. Nie są to nowe kary za samo nieprzestrzeganie RODO – naruszenia RODO nadal podlegają odrębnemu reżimowi sankcji.

Dla organizacji korporacyjnych regulacja oznacza przede wszystkim dalsze formalizowanie zasad pozyskiwania, udostępniania i ponownego wykorzystywania danych w ramach europejskiego rynku danych. W praktyce przedsiębiorstwa powinny zwrócić uwagę na:

1. procesy udostępniania danych podmiotom zewnętrznym;
2. korzystanie z usług pośredników danych;
3. zasady dostępu do danych znajdujących się w posiadaniu sektora publicznego;
4. ochronę tajemnicy przedsiębiorstwa, praw własności intelektualnej i danych osobowych przy wymianie danych;
5. potencjalne wykorzystanie danych w ramach nowych mechanizmów europejskiej gospodarki opartej na danych;
6. obowiązki regulacyjne, jeżeli przedsiębiorstwo samo będzie świadczyć usługi objęte zakresem DGA.

Dla większości przedsiębiorstw nie powstaje jednak obowiązek wdrożenia odrębnego systemu compliance wyłącznie z powodu wejścia w życie polskiej ustawy. Szczególne obowiązki dotyczą przede wszystkim przedsiębiorstw działających jako dostawcy usług pośrednictwa danych, uznane organizacje altruizmu danych lub podmioty korzystające z określonych mechanizmów ponownego wykorzystywania chronionych danych sektora publicznego.

Ustawa nie stanowi odrębnego reżimu zastępującego RODO. DGA oraz polska ustawa o zarządzaniu danymi tworzą dodatkowe ramy dla zarządzania i udostępniania danych, przy jednoczesnym zachowaniu wymogów dotyczących ochrony danych osobowych i praw osób trzecich.

23 lipca 2026 r. – od tego dnia obowiązuje polska ustawa o zarządzaniu danymi. Nie oznacza to jednak, że każda firma musi od tej daty wdrożyć nowe procedury. Przedsiębiorcy powinni przede wszystkim ustalić, czy ich działalność mieści się w szczególnych rolach objętych DGA oraz czy korzystają z mechanizmów udostępniania danych, które wymagają dodatkowych działań organizacyjnych lub prawnych.

Lista źródeł

Organizacje – krajowe i międzynarodowe

Komisja Europejska

CADA: <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

AI Act: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689>

Cyber Resilience Act: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation>

Data Governance Act: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation>

Koszty energii i plan elektryfikacji:

https://energy.ec.europa.eu/data-and-analysis/energy-prices-and-costs-europe_en

https://energy.ec.europa.eu/topics/eus-energy-system/electrification_en

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52026DC0595&qid=1784715609929>

https://energy.ec.europa.eu/publications/tripartite-agreement-energy-storage_en

Raportowanie Centrów Danych:

https://eur-lex.europa.eu/eli/reg_del/2024/1364/2024-05-17

https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1667

https://energy.ec.europa.eu/news/minimum-performance-standards-data-centres-europe-public-consultation-launched-2026-09-21_en

Assessment of the energy performance and sustainability of data centres in EU - first technical report:

<https://op.europa.eu/en/publication-detail/-/publication/83be4c3e-5c79-11f0-a9d0-01aa75ed71a1/language-en>

Sejm RP

Ustawa o systemach sztucznej inteligencji:

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260001003>

Ustawa o zarządzaniu danymi: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260000548>

Ministerstwo Energii

<https://www.gov.pl/web/klimat/projekt-krajowego-planu-w-dziedzinie-energii-i-klimatu-do-2030-r-z-perspektywa-do-2040-r-wersja-przekazana-do-dalszych-prac-przez-Ministra-Energii>

Ministerstwo Cyfryzacji

<https://www.gov.pl/web/baza-wiedzy/cra--nowe-obowiazki-dla-producentow-oprogramowania-i-korzystosci-dla-uzytkownikow>

<https://www.gov.pl/web/baza-wiedzy/ustawa-o-zarzadzaniu-danymi-juz-obowiazuje>

Instytut Łączności

<https://www.gov.pl/web/instytut-lacznosci/zbuntowani-agenci-ai-wnioski-dla-technologicznego-biznesu-i-dla-administracji-panstwowej>

Polskie Sieci Energetyczne

<https://www.pse.pl/-/projekt-nowego-planu-rozwoju-sieci-przesylowej-na-lata-2027-2036>

Wody Polskie

<https://www.gov.pl/web/wody-polskie-szczecin/susza-hydrologiczna-doswiadcza-regiony-polski-zachodniej-i-centralnej>

Krajowa Izba Gospodarcza

<https://kig.pl/wp-content/uploads/2026/09/Raport-Transformacja-energetyczna-online.pdf>

Administracja USA

<https://www.congress.gov/crs-product/R48646>

Raporty i analizy

International Energy Agency

<https://www.iea.org/reports/energy-and-ai>

PwC

<https://www.pwc.com/gx/en/1/services/consulting/technology/data-centre-outlook.html>

Ernst&Young

https://www.ey.com/pl_pl/newsroom/2026/08/badanie-ey-ponad-8-na-10-liderow-firm-obawia-sie-kosztow-korzystania-z-ai

World Economic Forum

<https://www.weforum.org/stories/energy-transition/localized-approaches-vital-for-energy-transition-momentum-and-more-top-energy-stories/>

ILO

<https://www.ilo.org/publications/e-waste-and-employment-around-world>

Forum Energii

<https://www.forum-energii.eu/rachunek-za-konkurencyjnosc>

Global E-waste Monitor

<https://ewastemonitor.info/the-global-e-waste-monitor-2024/>

Basil Action Network: The Coming AI Waste Wave

https://wiki.ban.org/images/1/16/AI_Waste_Wave_Part_1.pdf

Making AI Less Thirsty (Li et al, 2025)

<https://arxiv.org/abs/2304.03271>

DSET

<https://dset.tw/en/research/infrastructure-resilience2025/>

IMF

<https://www.elibrary.imf.org/view/journals/001/2025/081/article-A001-en.xml>

Rzeczpospolita – Infrastruktura przyszłości: Data Center i rewolucja AI

https://ebooki.rp.pl/wp-content/uploads/2026/09/Infrastruktura_Przyszlosci.pdf

Sektor prywatny

TSMC

<https://investor.tsmc.com/static/annualReports/2024/english/ebook/index.html>

Google DeepMind

<https://storage.googleapis.com/deepmind-media/DeepMind.com/Blog/securing-the-future-of-ai-agents/gdm-ai-control-roadmap.pdf>

Prasa

Rzeczpospolita

<https://www.rp.pl/dyplomacja/art45184941-ai-to-zagrozenie-dla-calej-ludzkosci-usa-w-rb-onz-bagatelizuja-ostrezenia>

<https://www.rp.pl/biznes/art45162991-opor-wobec-centrow-danych-coraz-wiecej-polakow-mowi-nie>

<https://cyfrowa.rp.pl/ai/art45213241-w-usa-juz-nie-ma-sztucznej-inteligencji-donald-trump-oficjalnie-zmienil-jej-nazwe>

South China Morning Post

<https://www.scmp.com/tech/tech-trends/article/3358907/chip-supply-chain-braces-more-price-hikes-upstream-parts-create-new-bottlenecks>

Wall Street Journal

<https://www.wsj.com/business/energy-oil/ai-data-centers-desperate-for-electricity-are-building-their-own-power-plants-291f5c81>

PIE Tygodnik Gospodarczy

<https://pie.net.pl/tygodnik-gospodarczy-24-2026-18-czerwca-2026-r/#tyg-mat-37530-3>

<https://pie.net.pl/tygodnik-gospodarczy-29-2026-23-lipca-2026-r/#tyg-mat-37738-6>

<https://pie.net.pl/tygodnik-gospodarczy-39-2026-1-pazdziernika-2026-r/#tyg-mat-38205-5>

Reuters

<https://www.reuters.com/legal/litigation/un-chief-calls-ai-firms-come-clean-environmental-costs-2026-06-23/>
<https://www.investing.com/news/stock-market-news/meta-ceo-attributes-layoffs-plan-to-capex-wont-rule-out-further-job-cuts-4651387>

Portale Branżowe

<https://www.euractiv.com/news/anthropics-models-gained-unauthorized-real-world-access/>

<https://ewastemonitor.info/the-global-e-waste-monitor-2024/>

<https://zielonagospodarka.pl/praca-trzech-reaktorow-atomowych-we-francji-zostala-wstrzymana-przez-upaly-23205>;

<https://zielonagospodarka.pl/niski-stan-dunaju-uderza-w-atom-wegry-przechodza-kryzys-rumunia-wysadza-podwodna-skale-23329>

<https://zielonagospodarka.pl/susza-panuje-w-calym-kraju-uderza-w-rolnictwo-i-dostepnosc-wody-23144>.

<https://www.susza.iung.pulawy.pl/>

<https://zielonagospodarka.pl/w-siedlcach-powstanie-najwiekszy-magazyn-energii-w-polsce-zbuduja-go-portuglaczyzy-z-chinczykami-23154>



Infolinia: 801 332 202

kontakt@parp.gov.pl

Obserwuj nas także na:

