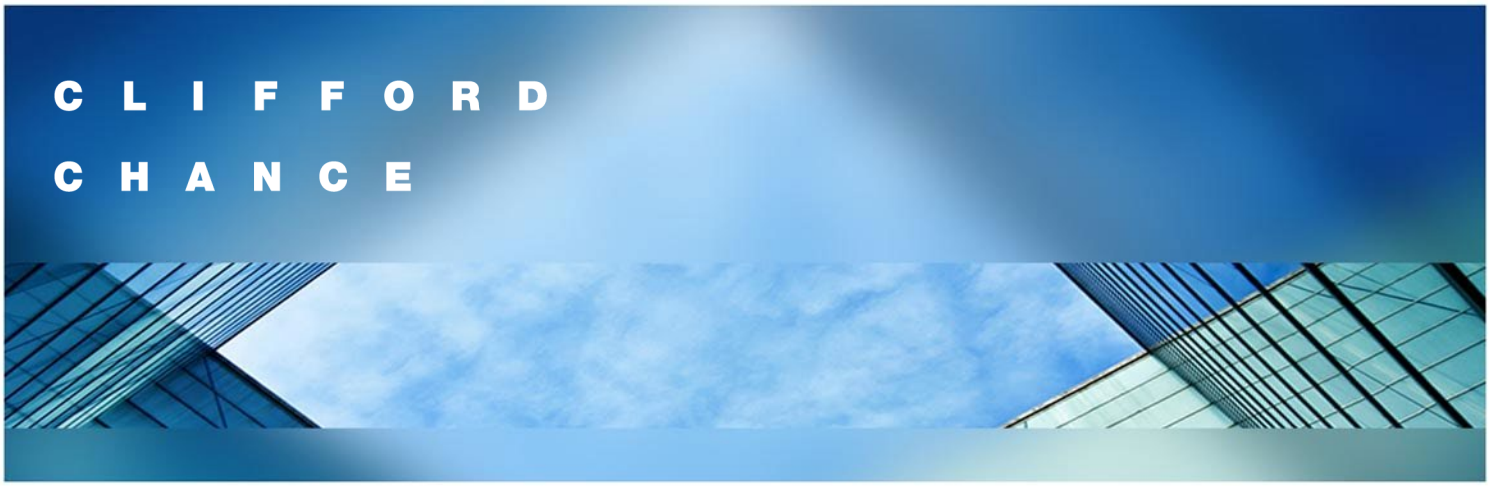


# NOWA POLSKA USTAWA O KRAJOWYM SYSTEMIE CERTYFIKACJI CYBERBEZPIECZEŃSTWA I JEJ KLUCZOWE ZAŁOŻENIA

W dniu 28 lipca w Dzienniku Ustaw Rzeczypospolitej Polskiej została opublikowana ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa („**Ustawa**”), która wejdzie w życie 30 dni po jej ogłoszeniu, tj. 28 sierpnia 2025 r. Jej przewodnim celem jest zapewnienie właściwej organizacji systemu certyfikacji cyberbezpieczeństwa na terytorium Rzeczypospolitej Polskiej poprzez ustanowienie odpowiednich procedur wydawania krajowych i europejskich certyfikatów, które będą uznawane przez wszystkie państwa członkowskie Unii Europejskiej oraz określenie zasad nadzoru i kontroli związanymi z takimi certyfikatami.

### Zgodność z ramami europejskiej certyfikacji cyberbezpieczeństwa

Wprowadzenie procedury certyfikacji wynika z obowiązku wdrożenia przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa ("**ENISA**") oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Cybersecurity Act) ("**Akt o cyberbezpieczeństwie**"). Akt o cyberbezpieczeństwie stanowi wiodący akt prawny regulujący kwestie podniesienia poziomu bezpieczeństwa usług informacyjno-komunikacyjnych (ICT) na rynku wewnętrznym Unii Europejskiej. Jego założenia obejmują m.in. wzmocnienie ENISA oraz zapewnienie harmonijnego stosowania procedur certyfikacji cyberbezpieczeństwa we wszystkich państwach członkowskich Unii Europejskiej.

### Założenia procedur certyfikacji

Uregulowanie systemu certyfikacji ma na celu stworzenie jednolitych standardów bezpieczeństwa w ramach Unii Europejskiej i tym samym zwiększenie zaufania konsumentów, klientów czy przedsiębiorstw do produktów, usług oraz procesów informacyjno-komunikacyjnych (ICT) oraz zapobiegnięcie rozdrobnieniu rynku w dziedzinie cyberbezpieczeństwa. Zgodnie z definicją "certyfikacji" z art. 2 ust. 3 Ustawy, certyfikacja ma stanowić potwierdzenie spełnienia wymogów określonych w europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym schemacie certyfikacji cyberbezpieczeństwa.

Krajowe schematy certyfikacji cyberbezpieczeństwa stanowią nową instytucję prawną, będącą uzupełnieniem Aktu o cyberbezpieczeństwie. Jest to krajowy program certyfikacji, za którego przygotowanie ma być odpowiedzialny minister cyfryzacji.

Certyfikacja ma być procesem całkowicie **dobrowolnym**, nie nakłada więc żadnych obowiązków na podmioty działające na rynku. Jej zakres będzie określany na podstawie umowy zawartej między dostawcą a jednostką oceniającą zgodność. Ponadto, w ramach krajowych schematów certyfikacji cyberbezpieczeństwa przewidziano także możliwość certyfikacji zarówno osób fizycznych, jak i systemów zarządzania cyberbezpieczeństwem.

**Właściwe organy krajowe**

Akt o cyberbezpieczeństwie nakłada na państwa członkowskie Unii Europejskiej obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa dla celów nadzorowania rynku i kontroli prawidłowości procedur certyfikacyjnych. Artykuł 4 Ustawy ustanawia **ministra cyfryzacji** ("**Minister**") jako organ właściwy do spraw certyfikacji cyberbezpieczeństwa. Do zadań Ministra należy m.in. sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji, przeprowadzanie kontroli podmiotów krajowego systemu certyfikacji, wyrażanie zgody na wydanie europejskich certyfikatów o poziomie uzasadnienia zaufania "wysoki" czy rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań w ramach europejskich programów certyfikacji cyberbezpieczeństwa.

Istotna rola została również przypisana **Polskiemu Centrum Akredytacji** ("**PCA**"), któremu Ustawodawca wskazuje określone obowiązki informacyjne oraz nadzorcze. Dla przeprowadzenia oceny zgodności produktów, usług oraz procesów ICT, jak i usług zarządzanych w zakresie bezpieczeństwa systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych, podmioty zainteresowane będą zobowiązane do uzyskania uprzedniej akredytacji PCA. PCA będzie miało obowiązek do przekazywania informacji o udzielonych akredytacjach oraz odmowach ich udzielenia.

**Rozpatrywanie skarg**

Przewidziano dwie niezależne od siebie procedury skargowe. Zgodnie z pierwszą określono termin, w jakim organ powinien odnieść się do skargi. Natomiast druga przewiduje możliwość wniesienia skargi na przewlekłość postępowania, o ile osoba zainteresowana posiada interes prawny[1]. Art. 24 Ustawy dotyczy pierwszej procedury oraz przewiduje możliwość złożenia skargi na działania jednostki certyfikującej przez każdy podmiot. Rozstrzygnięcie skargi ma nie trwać dłużej niż 2 miesiące, a sama skarga powinna być rozpatrywana przez inne osoby niż te, które pierwotnie podejmowały działania z procedury certyfikacyjnej. Zgodnie z przepisami, organem właściwym do rozpatrywania skarg na podmioty, które wydały deklaracje zgodności, jest Minister.

**Kary administracyjne**

Ustawa wprowadza także kary administracyjne za brak realizacji określonych obowiązków m.in. dla jednostki oceniającej zgodność, która wydaje certyfikat pomimo działania bez wymaganej akredytacji, dla jednostki oceniającej zgodność, która będąc do tego obowiązaną, nie przekazuje wymaganych przez Ustawę danych czy dla dostawców produktów ICT, nie wykonujących obowiązków związanych z badaniami, przeprowadzanymi dla celów ustalenia

[1] Art. 26 w zw. z art. 25 Ustawy.

spełnienia wymogów danego europejskiego programu certyfikacji czy w krajowym schemacie certyfikacji cyberbezpieczeństwa[2]. Niedopełnienie obowiązków przez jednostki oceniające zgodność lub dostawców produktów i usług ICT, takich jak przekazywanie nieprawdziwych danych czy brak wymaganej akredytacji, może skutkować nałożeniem kary pieniężnej w wysokości nawet do dwudziestokrotności przeciętnego wynagrodzenia, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" za rok poprzedzający rok nałożenia kary pieniężnej[3].

**Co dalej?**

Wejście w życie ustawy - 28 sierpnia 2025 r. - otwiera nowy rozdział dla przedsiębiorstw i administracji. Kluczowe będą działania Ministerstwa ds. cyfryzacji, które przygotuje krajowe schematy certyfikacji oraz zapewni skuteczny nadzór. Warto jednak już teraz analizować, jak certyfikacja może przełożyć się na przewagę rynkową, a także dostosować swoje produkty i usługi do przyszłych wymogów.

Nowa ustawa bowiem nie tylko zwiększa poziom cyberbezpieczeństwa w Polsce, lecz także stanowi realną szansę na wzmocnienie pozycji polskich firm na wymagającym, coraz bardziej świadomym rynku europejskim – a zaufanie i bezpieczeństwo cyfrowe już dziś stają się kluczowymi przewagami konkurencyjnymi.

## KONTAKT

**Agnieszka Janicka**
Partner

T +48 22 627 11 77
E agnieszka.janicka@cliffordchance.com

**Krzysztof Hajdamowicz**
Counsel

T +48 22 627 11 77
E krzysztof.hajdamowicz@cliffordchance.com

**Martyna Sieczka**
Associate

T +48 22 627 11 77
E martyna.sieczka@cliffordchance.com

**Agata Wężyk**
Legal Intern

T +48 22 627 11 77
E agata.wezyk@cliffordchance.com

[2] Art. 28 oraz 33 Ustawy.
[3] Art. 2 pkt 19 Ustawy.

Niniejsza publikacja nie omawia wszystkich istotnych zagadnień i nie obejmuje wszystkich aspektów przedstawionych zagadnień. Niniejsza publikacja nie stanowi porady prawnej ani żadnej innej porady

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2025

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest** • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague** • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.