

# Nowe przepisy zwiększające cyberbezpieczeństwo krytycznych podmiotów i sieci w UE

Posted on 2024-11-29

17 października 2024 r. Komisja Europejska przyjęła pierwsze przepisy wykonawcze dotyczące cyberbezpieczeństwa podmiotów i sieci o znaczeniu krytycznym. Podstawą jest dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS2).

Akt wykonawczy szczegółowo określa środki zarządzania ryzykiem cybernetycznym, a także przypadki, w których incydent należy uznać za istotny, a przedsiębiorstwa dostarczające infrastrukturę cyfrową i usługi cyfrowe powinny zgłosić go organom krajowym. Jest to kolejny ważny krok w kierunku zwiększenia cyberodporności krytycznej infrastruktury cyfrowej w Europie.

Przyjęte rozporządzenie wykonawcze będzie miało zastosowanie do określonych kategorii firm świadczących usługi cyfrowe, takich jak:

## Nowe przepisy zwiększające cyberbezpieczeństwo krytycznych podmiotów i sieci w UE

- dostawcy usług przetwarzania w chmurze,
- dostawcy usług centrów danych,
- internetowe platformy handlowe,
- wyszukiwarki internetowe,
- i platformy społecznościowe, by wymienić tylko kilka z nich.

Dla każdej kategorii dostawców usług akt wykonawczy określa również, kiedy incydent jest uznawany za istotny.

Przyjęcie rozporządzenia wykonawczego zbiega się z terminem transpozycji dyrektywy NIS2 do prawa krajowego przez państwa członkowskie. Od 18 października 2024 r., wszystkie państwa członkowskie muszą stosować środki niezbędne do przestrzegania zasad cyberbezpieczeństwa NIS2, w tym środki nadzoru i egzekwowania.

# Kolejne kroki

Rozporządzenie wykonawcze zostanie opublikowane w Dzienniku Urzędowym w odpowiednim czasie i wejdzie w życie 20 dni później.

# Kontekst

Pierwszy ogólnounijny akt prawny dotyczący cyberbezpieczeństwa, dyrektywa NIS, wszedł w życie w 2016 r. i pomógł osiągnąć wspólny poziom bezpieczeństwa sieci i systemów informatycznych w całej UE. W ramach swojego kluczowego celu politycznego, jakim jest dostosowanie Europy do ery cyfrowej, Komisja zaproponowała w grudniu 2020 r. przegląd dyrektywy w sprawie bezpieczeństwa sieci i informacji. Po wejściu w życie w styczniu 2023 r. państwa członkowskie musiały dokonać transpozycji dyrektywy NIS2 do prawa krajowego do dnia 17 października 2024 r.

## Nowe przepisy zwiększające cyberbezpieczeństwo krytycznych podmiotów i sieci w UE

Dyrektywa NIS2 ma na celu zapewnienie wysokiego poziomu cyberbezpieczeństwa w całej Unii. Obejmuje ona podmioty działające w sektorach o krytycznym znaczeniu dla gospodarki i społeczeństwa, w tym dostawców publicznych usług łączności elektronicznej, zarządzania usługami ICT, usług cyfrowych, gospodarki ściekami i odpadami, przestrzeni kosmicznej, zdrowia, energii, transportu, wytwarzania produktów o krytycznym znaczeniu, usług pocztowych i kurierskich oraz administracji publicznej.

Dyrektywa zaostrza wymogi bezpieczeństwa nałożone na firmy i odnosi się do bezpieczeństwa łańcuchów dostaw i relacji z dostawcami. Usprawnia ona obowiązki sprawozdawcze, wprowadza bardziej rygorystyczne środki nadzorcze dla organów krajowych, a także surowsze wymogi w zakresie egzekwowania prawa i ma na celu harmonizację sankcji we wszystkich państwach członkowskich. Pomoże to zwiększyć wymianę informacji i współpracę w zakresie zarządzania kryzysami cybernetycznymi na poziomie krajowym i unijnym.

## Więcej informacji:

- Akt wykonawczy
- Zestawienie informacji na temat dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS2)
- Pytania i odpowiedzi na temat NIS2: Nowa strategia UE w zakresie cyberbezpieczeństwa i nowe przepisy zwiększające odporność fizycznych i cyfrowych podmiotów krytycznych

## Źródło:

komunikat Komisji Europejskiej