OGÓLNOPOLSKIE STOWARZYSZENIE
SZPITALI PRYWATNYCH

81-350 Gdynia
Plac Kaszubski 1
www.ossp.pl

Gdynia, 26.05.2026 r.

Pan Tomasz Maciejewski
Podsekretarz Stanu
Ministerstwo Zdrowia

ul. Miodowa 15
00-952 Warszawa

Szanowny Panie Ministrze

Zwracamy się z uprzejmą prośbą o udzielenie informacji na temat sposobu stosowania przepisów znowelizowanej ustawy z dnia 05 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 z późn. zm.) - dalej jako: „**Ustawa**", w zakresie przesłanek kwalifikowania podmiotów sektora ochrony zdrowia jako podmiotów kluczowych lub ważnych na podstawie decyzji właściwego organu oraz jako podmiotów krytycznych.

Zgodnie z Ustawą, aby być podmiotem kluczowym albo podmiotem ważnym, przede wszystkim ocenia się przynależność danego podmiotu do określonego sektora, a także skalę działalności. Podmioty lecznicze są kwalifikowane do sektora kluczowego, wymienionego w Załączniku 1 do Ustawy. Zatem, weryfikacja skali działalności (poziomu zatrudnienia i rocznego obrotu) powinna dawać jednoznaczną odpowiedź na pytanie czy dany podmiot leczniczy jest objęty krajowym systemem cyberbezpieczeństwa.

Jednakże, Ustawa poza mierzalnymi kwalifikatorami, przewiduje szczególne przesłanki kwalifikacyjne, oparte na uznaniowości organów krajowych, w związku z czym istnieje niepewność prawna co do podlegania obowiązkom wynikającym z Ustawy, np. przez podmioty lecznicze, które nie spełniają kryteriów wielkościowych (zatrudnienia, obrotu), ale mogą mieć istotne znaczenie dla systemu zdrowia publicznego.

W szczególności, jak stanowi art. 5 ust. 4 Ustawy, podmiotem kluczowym jest, niezależnie od wielkości podmiotu, **podmiot krytyczny**. Zgodnie z definicją zawartą w art. 2 pkt 11c) Ustawy, „podmiot krytyczny" to podmiot krytyczny w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557".

Z kolei, w świetle art. 6 dyrektywy 2022/2557, do dnia 17 lipca 2026 r. każde państwo członkowskie identyfikuje podmioty krytyczne dla sektorów i podsektorów określonych w załączniku biorąc pod uwagę wyniki swojej oceny ryzyka państwa członkowskiego i strategię oraz stosuje wszystkie następujące kryteria:

a. podmiot świadczy co najmniej jedną usługę kluczową;

b. podmiot prowadzi działalność na terytorium tego państwa członkowskiego i jego infrastruktura krytyczna znajduje się na terytorium tego państwa członkowskiego; oraz
c. ustalono, że incydent miałby **istotne skutki zakłócające** dla świadczenia przez podmiot co najmniej jednej usługi kluczowej lub dla świadczenia innych usług kluczowych w sektorach określonych w załączniku, które zależą od tej usługi kluczowej lub tych usług kluczowych.

Nadto, należy mieć na uwadze regulację art. 7l ust.1 Ustawy, zgodnie z którą **organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, może uznać** osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej **za podmiot kluczowy lub podmiot ważny**, która nie spełnia przesłanek określonych w art. 5 ust. 1 pkt 1-3, pkt 4 lit. a-d oraz g-j, ust. 2 pkt 1-5 oraz 7 i 8, ust. 3-11 Ustawy, jeżeli:

1. jest podmiotem określonym w załączniku nr 1 lub 2 do ustawy;
2. spełnia co najmniej jedną z poniższych przesłanek:
   a) jako jedyna świadczy usługę, za pomocą systemu informacyjnego, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
   b) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego,
   c) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
   d) świadczenie przez nią, za pomocą systemu informacyjnego, usługi ma istotne znaczenie na poziomie wojewódzkim lub krajowym lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

Przez wzgląd na powyższe, podmioty sektora ochrony zdrowia, pomimo negatywnej samoidentyfikacji jako podmiot kluczowy lub ważny, muszą liczyć się z tym, że mogą zostać zakwalifikowane do krajowego systemu cyberbezpieczeństwa przez właściwe organy, a w konsekwencji, że będą podlegać obowiązkom wynikającym z Ustawy, za których wdrożenie będą rozliczane pod sankcją nałożenia znacznych kar finansowych. Ustawa co prawda przewiduje dla takich podmiotów czas na dostosowanie się i spełnienie obowiązków ustawowych, jednakże, wobec faktu, że obowiązki te wiążą się ze zmianą w strategii zarządzania, istotnymi wydatkami na dostosowanie systemów bezpieczeństwa, wprowadzenie zabezpieczeń IT, okres na dostosowanie może okazać się bardzo rygorystyczny w porównaniu do tego, który mają inne podmioty, znające konkretne przesłanki kwalifikacji wynikające z Ustawy.

Dlatego też, zwracamy się do Ministerstwa Zdrowia z prośbą o wskazanie, jakie kategorie podmiotów sektora zdrowia będą kwalifikowane jako podmioty krytyczne, a jakie jako kluczowe lub ważne na podstawie decyzji właściwego organu, w związku z uznaniem ich za istotne dla bezpieczeństwa zdrowia publicznego, czy z punktu widzenia istotności dla systemu. W szczególności, prosimy o doprecyzowanie jakie przesłanki będą brane pod uwagę, według jakich szczegółowych kryteriów owa istotność dla systemu/istotność skutków zakłócających świadczenia będzie oznaczana.

Jednocześnie, mając na uwadze cel regulacji wynikający z Dyrektywy NIS2 oraz ustawy o krajowym systemie cyberbezpieczeństwa, polegający na zapewnieniu ciągłości świadczenia usług kluczowych oraz ograniczeniu skutków incydentów dla społeczeństwa, pozwalamy sobie przedstawić następujące uwagi i postulaty interpretacyjne.

W naszej ocenie, przy dokonywaniu kwalifikacji podmiotów leczniczych do krajowego systemu cyberbezpieczeństwa w trybie uznaniowym, zasadnym jest uwzględnienie jako jednego z

OGÓLNOPOLSKIE STOWARZYSZENIE
SZPITALI PRYWATNYCH

81-350 Gdynia
Plac Kaszubski 1
www.ossp.pl

podstawowych kryteriów udzielanie przez dany podmiot świadczeń zdrowotnych finansowanych ze środków publicznych na podstawie umów zawartych z Narodowym Funduszem Zdrowia.

Podmioty realizujące świadczenia w ramach systemu publicznego stanowią bowiem integralną część systemu zabezpieczenia zdrowotnego państwa, a ich działalność pozostaje bezpośrednio związana z realizacją konstytucyjnego prawa do ochrony zdrowia, o którym mowa w art. 68 Konstytucja RP. Zakłócenie ich funkcjonowania, w tym w wyniku incydentu cyberbezpieczeństwa, może prowadzić do istotnego ograniczenia dostępności świadczeń gwarantowanych dla szerokiej grupy pacjentów.

Kryterium posiadania umowy z Narodowym Funduszem Zdrowia może jednocześnie stanowić obiektywny i weryfikowalny wskaźnik znaczenia danego podmiotu dla systemu ochrony zdrowia, pozwalający na ograniczenie uznaniowości decyzji organu oraz zapewnienie transparentności procesu kwalifikacji. Jednocześnie kryterium to pozostaje w zgodzie z logiką oceny wpływu incydentu na ciągłość świadczenia usług, wynikającą z dyrektywy NIS2, gdyż podmioty realizujące świadczenia finansowane ze środków publicznych mają bezpośredni wpływ na bezpieczeństwo zdrowia publicznego.

Zastrzegamy przy tym, że wskazane kryterium nie powinno mieć charakteru wyłącznego, lecz stanowić istotny element szerszej oceny, uwzględniającej również inne czynniki, takie jak zakres udzielanych świadczeń, ich znaczenie dla systemu ochrony zdrowia, liczba obsługiwanych pacjentów czy rola danego podmiotu w zabezpieczeniu potrzeb zdrowotnych na poziomie regionalnym lub krajowym.

W związku z powyższym, będziemy wdzięczni za przedstawienie stanowiska Ministerstwa Zdrowia w zakresie:

- planowanych lub stosowanych kryteriów kwalifikacji podmiotów sektora ochrony zdrowia w trybie uznaniowym,
- ewentualnego uwzględniania faktu realizacji świadczeń finansowanych ze środków publicznych jako jednego z kluczowych elementów tej kwalifikacji,
- a także przewidywanych wytycznych lub rekomendacji w tym zakresie.

W naszej ocenie, nawet ogólne i kierunkowe wytyczne będą nieocenionym wsparciem dla podmiotów, które odpowiedzialnie podchodzą do kwestii cyberbezpieczeństwa i zapewnienia ciągłości świadczonych usług, a także pomogą zrealizować cel ustawy i wzmocnić strategię państwa w zakresie systemu cyberbezpieczeństwa.

Z wyrazami szacunku

Andrzej Sokołowski

prezes zarządu
Ogólnopolskiego Stowarzyszenia
Szpitali Prywatnych