ZWIĄZEK RZEMIOSŁA POLSKIEGO
PREZES
prof. Jan Klimek

Warszawa, 05.11.2026

Pan Dariusz Standerski

Sekretarz Stanu

Ministerstwo Cyfryzacji

Szanowny Panie Ministrze

nawiązując do Ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w brzmieniu nadanym Ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, w załączeniu przesyłam opinię Związku Rzemiosła Polskiego do ewentualnego wykorzystania przez Pana Ministra przy jej doskonaleniu.

Załączona opinia powstała w ramach projektu, pt. „Monitorowanie prawa przez organizacje rzemiosła w zakresie zatrudnienia i umiejętności" współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus 2021-2027 w ramach Programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (nr umowy: FERS.04.03-IP.06-0001/24) i jest efektem konsultacji przeprowadzonych z izbami rzemieślniczymi i cechami rzemiosła zrzeszonymi w Związku Rzemiosła Polskiego.

Z szacunkiem

Jan Klimek

Załącznik:

Opinia Związku Rzemiosła Polskiego.

Warszawa, 05.11.2026 r.

OPINIA

Związku Rzemiosła Polskiego

dot. ustawy o krajowym systemie cyberbezpieczeństwa

Związek Rzemiosła Polskiego do Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: „ustawa KSC"), w brzmieniu nadanym Ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz. U. z 2026 r. poz. 252), która wdrożyła do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS 2), podchodzi z perspektywy mikro, małych i średnich przedsiębiorstw. Nowelizacja dzieli podmioty na kluczowe i ważne, rozszerza katalog sektorów objętych obowiązkami cyberbezpieczeństwa, ustanawia prowadzony w systemie teleinformatycznym wykaz podmiotów oraz określa obowiązki zarządcze, dokumentacyjne i incydentowe, a także zasady nadzoru i sankcji. Choć samorząd rzemieślniczy co do zasady pozostaje poza bezpośrednim zasięgiem tych obowiązków, nie pozostaje wobec nich obojętny: wymogi spływają kaskadowo przez umowy z większymi kontrahentami, a świadomość nowych reguł przesądza o bezpieczeństwie tysięcy firm. Stąd niniejsze stanowisko – praktyczne spojrzenie na obowiązki i ryzyka, jakie nowe prawo przynosi naszym organizacjom członkowskim i całemu środowisku rzemieślniczemu.

Wdrożenie dyrektywy (UE) 2022/2555 (NIS 2) do polskiego porządku prawnego zostało, w ocenie ZRP, przeprowadzone ze starannością, jakiej wymaga materia tak wrażliwa jak bezpieczeństwo sieci i systemów informacyjnych. Nowelizacja z 23 stycznia 2026 r. buduje spójną architekturę krajowego systemu cyberbezpieczeństwa, porządkując obowiązki podmiotów od systemu zarządzania bezpieczeństwem informacji, przez dokumentację, aż po obsługę incydentów, i koncentrując się na sektorach naprawdę newralgicznych dla funkcjonowania państwa

Opinia powstała w ramach projektu „Monitorowanie prawa przez organizacje rzemiosła w zakresie zatrudnienia i umiejętności" współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus 2021-2027 w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (nr umowy FERS.04.03-IP.06-0001/24)

i gospodarki. Analiza ekspercka przeprowadzona na zlecenie Związku Rzemiosła Polskiego nie zidentyfikowała przy tym rozwiązań, które budziłyby wątpliwości konstytucyjne. Formułowane niżej postulaty nie podważają tej zgodności - dotyczą wyłącznie proporcjonalności poszczególnych obowiązków wobec najmniejszych uczestników rynku.

Ustawa KSC co do zasady nie obejmuje swoim zakresem organizacji samorządu gospodarczego rzemiosła. Cechy, izby rzemieślnicze oraz Związek Rzemiosła Polskiego nie mieszczą się w kategorii „podmiotów publicznych", którą ustawa definiuje. Rzemiosło nie zostało ujęte w żadnym z dziewiętnastu sektorów objętych załącznikami do ustawy, a edukacja zawodowa nie stanowi odrębnego sektora (załącznik nr 2 wymienia wyłącznie „badania naukowe"). Jedynym obszarem, w którym organizacja rzemieślnicza mogłaby potencjalnie zostać zakwalifikowana jako podmiot ważny, pozostaje „produkcja wyrobów optycznych" wskazana w załączniku nr 2, przy czym kwalifikacja ta może dotyczyć wyłącznie organizacji spełniających kryteria średniego przedsiębiorstwa. Na typowej izbie rzemieślniczej lub cechu – prowadzących ewidencję kwalifikacji zawodowych, egzaminy czeladnicze i mistrzowskie oraz obsługę administracyjną członków – nie ciążą zatem bezpośrednie obowiązki wynikające z Ustawy KSC.

Obowiązki, których ustawa wprost nie nakłada, mogą zostać na MŚP przeniesione zapisami umów z kontrahentami, których ustawa już obejmuje. Podmioty kluczowe i ważne muszą w ramach systemu zarządzania bezpieczeństwem informacji (SZBI) zapewnić bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT, „z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym" (art. 8 ust. 1 pkt 2 lit. e ustawy KSC). W praktyce rzemieślnik lub izba współpracujący z takim podmiotem mogą w treści umowy lub aneksu do niej zostać zobowiązani do przestrzegania wymogów w zakresie cyberbezpieczeństwa, których wcześniej nie negocjowali i których nie mają jak audytować. Przykładowo chmura do wymiany dokumentacji, KSeF przy fakturowaniu, wspólny dysk z zamawiającym – każda z tych funkcjonalności może stać się pretekstem do objęcia umowy reżimem NIS 2 dla usług ICT i wygenerować koszty audytów i certyfikacji nieproporcjonalne do skali mikroprzedsiębiorcy lub stać się powodem jego wykluczenia z postępowań przetargowych.

Opinia powstała w ramach projektu „Monitorowanie prawa przez organizacje rzemiosła w zakresie zatrudnienia i umiejętności" współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus 2021-2027 w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (nr umowy FERS.04.03-IP.06-0001/24)

Zgodnie z art. 73b ust. 1 pkt 3 ustawy KSC kara pieniężna może dotknąć nie tylko podmiot kluczowy lub ważny, lecz także producenta albo dostawcę, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NASK lub CSIRT GOV. Odpowiedzialność sięga więc poza krąg podmiotów, którym ustawa cokolwiek nakazuje.

Jednym z postulatów legislacyjnych Związku Rzemiosła Polskiego jest usunięcie w art. 8 ust. 1 pkt 2 lit. e ustawy KSC fragmentu „z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym" – obowiązek dbałości o łańcuch dostaw powinien spoczywać na podmiocie, na który ustawa go nakłada, a nie spływać umowami na jego najmniejszych kontrahentów. Drugim postulatem legislacyjnym jest usunięcie pkt 3 w art. 73b ust. 1 ustawy KSC, obejmującego „producenta lub dostawcę, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NASK lub CSIRT GOV". Żadna z tych zmian nie osłabia w naszej ocenie cyberodporności usług kluczowych - obie jednak zdejmują ciężary, które najmniejsi uczestnicy rynku dźwigają dziś bez rzeczywistego zysku dla bezpieczeństwa systemu.

Odrębnej uwagi wymaga kwestia świadomości prawnej przedsiębiorców. Identyfikacja statusu podmiotu kluczowego lub ważnego opiera się przede wszystkim na samorejestracji – podmiot zobowiązany jest samodzielnie rozpoznać, że spełnia ustawowe przesłanki, i wystąpić z wnioskiem o wpis do wykazu. Do 3 kwietnia 2027 r. podmioty objęte ustawą zobowiązane zostały do wdrożenia systemu zarządzania bezpieczeństwem informacji oraz procedury zgłaszania incydentów. Na 3 kwietnia 2028 r. przypada pierwszy obowiązkowy audyt podmiotów kluczowych. Podmiot pozbawiony wiedzy o objęciu go zakresem ustawy nie będzie miał realnej możliwości dochowania tych terminów. Z tego względu Związek Rzemiosła Polskiego postuluje przeprowadzenie kampanii informacyjnej adresowanej do przedsiębiorców oraz opracowanie przystępnych wyjaśnień dotyczących kryteriów kwalifikacji i konsekwencji braku wpisu do wykazu, deklarując jednocześnie własne wsparcie w upowszechnianiu tych materiałów poprzez izby rzemieślnicze, cechy oraz kanały szkoleniowe samorządu gospodarczego rzemiosła. Świadomość obowiązków powinna być kształtowana przede wszystkim przez działania informacyjne, a nie przez praktykę sankcyjną – takie podejście służy również skuteczności samego nadzoru.

Opinia powstała w ramach projektu „Monitorowanie prawa przez organizacje rzemiosła w zakresie zatrudnienia i umiejętności" współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus 2021-2027 w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (nr umowy FERS.04.03-IP.06-0001/24)

Związek Rzemiosła Polskiego wyraża gotowość dalszego uczestnictwa w Państwa pracach, deklarując wsparcie merytoryczne w zakresie specyfiki funkcjonowania organizacji rzemieślniczych i ich członków oraz chęć współpracy przy testowaniu wytycznych, kodeksów dobrych praktyk i rozwiązań wspierających cyberodporność MŚP.

Wierzymy, że wspólne działania Państwa i samorządu gospodarczego rzemiosła pozwolą pogodzić wysoki poziom cyberbezpieczeństwa z zachowaniem konkurencyjności mikro, małych i średnich przedsiębiorstw.

Opinia powstała w ramach projektu „Monitorowanie prawa przez organizacje rzemiosła w zakresie zatrudnienia i umiejętności" współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus 2021-2027 w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 (nr umowy FERS.04.03-IP.06-0001/24)