Blisko milion złotych może ponieść jeden przedsiębiorca za wymianę serwerów, komputerów czy kosztów licencji oprogramowania

Czy Ministerstwo Cyfryzacji zna koszty wprowadzenia w życie zmian w ustawie o krajowym systemie cyberbezpieczeństwa, jakie będą, musieli ponieść przedsiębiorcy w tym z sektora MŚP?
Takie pytanie zadaje p. Robert Składowski – Prezes Federacji Panu Krzysztofowi Gawkowskiemu Wicepremierowi, Ministrowi Cyfryzacji.
Jednocześnie Federacja przygotowała raport w zakresie znajomości projektowanych przepisów przez przedsiębiorców. Raport obejmuje także zagadnienia dotyczące kosztów wprowadzenia w życie zmian w ustawie o krajowym systemie cyberbezpieczeństwa odnoszący się do sektora gospodarowania odpadami.

Cel proponowanych zmian

W kwietniu 2024 r. na stronie Rządowego Centrum Legislacji został opublikowany projekt nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa. Wnioskodawcą projektu jest Minister Cyfryzacji. Natomiast wersja po konsultacjach jest datowana na 3 października 2024 r.

Projekt ustawy nowelizującej dyrektywę NIS2 ma na celu dostosowanie polskiego systemu cyberbezpieczeństwa do nowych, bardziej rygorystycznych standardów unijnych. Główne cele i potrzeby, które napędza ta nowelizacja, to:

- **Wypełnienie obowiązku transpozycji:** Polska, podobnie jak inne państwa członkowskie UE, powinna wdrożyć przepisy dyrektywy NIS2 do swojego porządku prawnego w określonym terminie.
- **Adaptacja do zmieniającego się krajobrazu cyberzagrożeń:** Szybki rozwój technologii, zwiększona liczba i złożoność ataków cybernetycznych wymagają bardziej kompleksowych i skutecznych środków ochronnych. Pytanie tylko czyim kosztem.
- **Wzmocnienie współpracy między różnymi podmiotami:** Nowe przepisy mają na celu usprawnić współpracę między organami administracji publicznej, przedsiębiorstwami i innymi podmiotami zaangażowanymi w zapewnienie cyberbezpieczeństwa.
- **Usprawnienie zarządzania ryzykiem:** Podmioty kluczowe i ważne będą zobowiązane do wdrożenia bardziej zaawansowanych systemów zarządzania ryzykiem cybernetycznym.
- **Wzmocnienie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa:** Pełnomocnik otrzyma szersze uprawnienia.
- **Rozwój infrastruktury CSIRT:** Planowane jest utworzenie nowych sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Zgodnie z ogólnie dostępnymi stanowiskami i opiniami prawnymi, projekt dokonuje transpozycji postanowień NIS2 w szerszym zakresie, niż wymaga tego sama dyrektywa. Przede wszystkim rozszerzono katalog sektorów objęty regulacjami ustawy (m.in. poprzez objęcie jednostek samorządu terytorialnego, jednostek budżetowych w tym przedszkoli, szkół i placówek publicznych zakładanych i prowadzonych przez ministrów i jednostki samorządu terytorialnego, samorządowych zakładów budżetowych oraz uczelni, a także podmiotów wchodzących w skład systemu szkolnictwa wyższego i nauki).

Należy także wskazać, że za podmiot kluczowy i ważny co do zasady mogą być uznane firmy będące co najmniej średnim przedsiębiorstwem. Projekt przewiduje jednak wyjątki. Chodzi m.in. o sytuację, gdy zakłócenie świadczonej usługi mogłoby mieć znaczący wpływ na porządek, bezpieczeństwo lub zdrowie publiczne. W takim przypadku regulacje ustawowe będą dotyczyć także małych i mikro przedsiębiorców. W zależność od poszczególnych decyzji, liczba podmiotów, która zostanie objęta obowiązkami regulacyjnymi, wynosi ok. 38 000.

Wnioski z raportu kosztowego wprowadzenia w życie zmian w ustawie o krajowym systemie cyberbezpieczeństwa odnoszącego się do sektora gospodarowania odpadami.

Odnosząc się do sektora gospodarowania odpadami, to opracowana przez Ministerstwo Cyfryzacji Ocena Skutków Regulacji wskazuje, że nowelizacja ustawy będzie miała wpływ jedynie na 276 podmiotów z tej branży. Jednocześnie z danych znajdujących się w posiadaniu Ogólnopolskiej Federacji Przedsiębiorców i Pracodawców – Przedsiębiorcy.pl wynika, że w Polsce działa łącznie ponad 8865 firm, z których ponad 1500 zatrudnia więcej niż 50 pracowników.

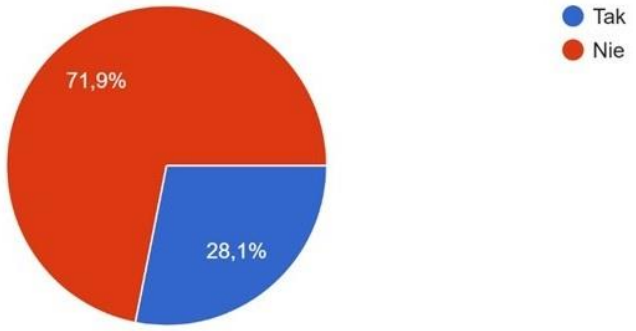
W Ocenie Skutków Regulacji – w kontekście skutków finansowych – zaprezentowano precyzyjnie jedynie wpływ na sektor finansów publicznych. W sekcji pn. „Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe" tabela dotycząca skutków w ujęciu pieniężnym nie została wypełniona, ale jednocześnie projektodawca przyznaje, że wejście przepisów w życie będzie się wiązać ze wzrostem nakładów finansowych. Celem dostosowania się do wymogów projektu przedsiębiorstwa będą musiały wdrożyć środki zarządzania cyberbezpieczeństwem. W przypadku dużych przedsiębiorstw może to zająć pewien czas. Niezbędne będzie dokonanie inwentaryzacji infrastruktury, przeglądu procesów i wewnętrznych procedur, przeprowadzenie wewnętrznych szkoleń.

Projektodawca wskazał, że koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka są niemierzalne. Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, co zdaniem Ministerstwa Cyfryzacji, prowadzi do niemożności wskazania kosztów, jakie poniosą podmioty kluczowe i podmioty ważne.

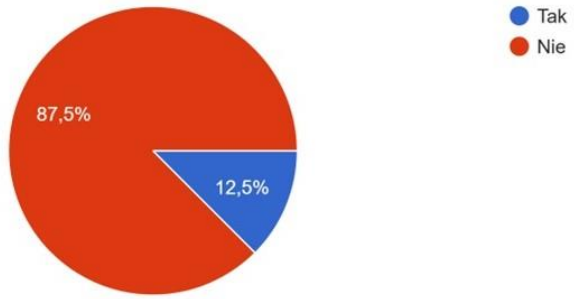
W ujęciu niepieniężnym dla sektora mikro-, małych i średnich przedsiębiorstw, jak wskazało Ministerstwo Cyfryzacji: „Na tym etapie nie jest możliwe oszacowanie kosztów dostosowawczych po stronie przedsiębiorców w zależności od ich rodzajów z uwagi na brak danych. Projekt oddziałuje na podmioty o zróżnicowanej wielkości – od małych do dużych. Koszty audytów bezpieczeństwa, zatrudnienia specjalistów z zakresu cyberbezpieczeństwa, wdrożenia systemu zarządzania bezpieczeństwem informacji itd., będą się znacząco różnić od wielkości i charakteru usług świadczonych przez podmiot. Projekt może być uzupełniony w tym zakresie, jeżeli w toku konsultacji publicznych zostaną przedstawione dane dotyczące kosztów wdrożenia".

Wiedza przedsiębiorców odnośnie znajomości projektowanych zmian i skutków finansowych.

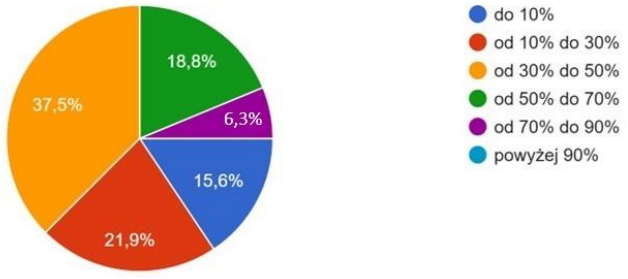
Wykres nr 1 – Odpowiedzi udzielone na pytanie: Czy znane są Pani/Panu konsekwencje dla przedsiębiorców wprowadzenia ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa przedstawionego przez Ministerstwo Cyfryzacji?



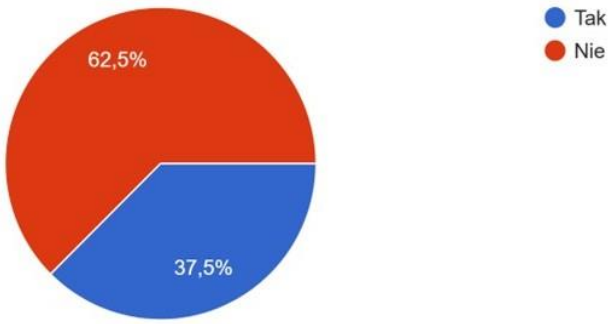
Wykres nr 2 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem istnieje realna możliwość wymiany sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn i zastąpienie ich wyłącznie urządzeniami produkowanymi przez firmy z państw Unii Europejskiej i NATO?



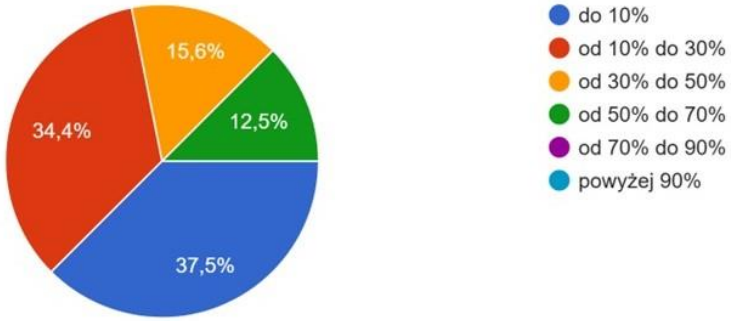
Wykres nr 3 – Odpowiedzi udzielone na pytanie: Ile w zasobach Pani/Pana firmy znajduje się sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (urządzenia pokładowe typu OBU, panele sterujące, sterowniki zabudowy śmieciarki, wyposażenie śmieciarki, taśmy do segregacji odpadów, urządzenia sortujące, komputery, serwery, dyski twarde, telefony, routery, drukarki, skanery, monitory, kamery itp.) pochodzenia spoza państw Unii Europejskiej i NATO?



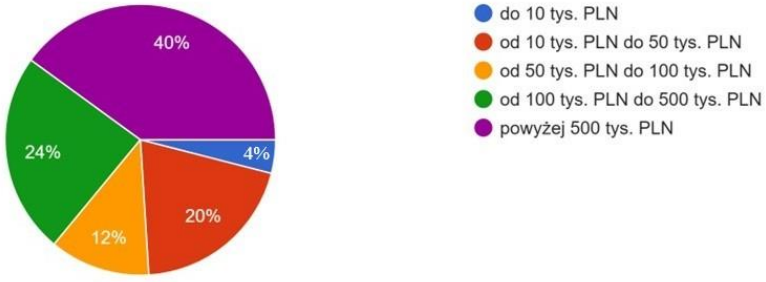
Wykres nr 4 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem istnieje realna możliwość wymiany powyższego oprogramowania i zastąpienie go wyłącznie oprogramowaniem firm z państw Unii Europejskiej i NATO?



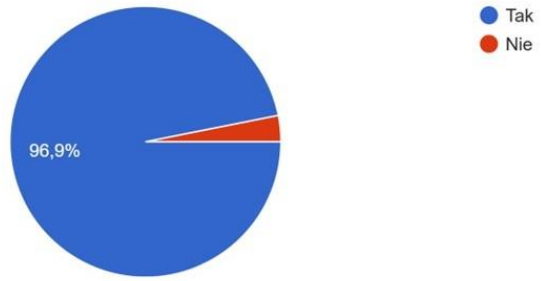
Wykres nr 5 – Odpowiedzi udzielone na pytanie: Jaka jest procentowa wartość wykorzystywanego oprogramowania (w tym programów komputerowych, aplikacji, sterowników, silników bazodanowych etc., niezależenie od formy posiadania – własność produktów, licencje, subskrypcje itp.) pochodzącego z państw spoza Unii Europejskiej i NATO w stosunku do całego posiadanego oprogramowania?



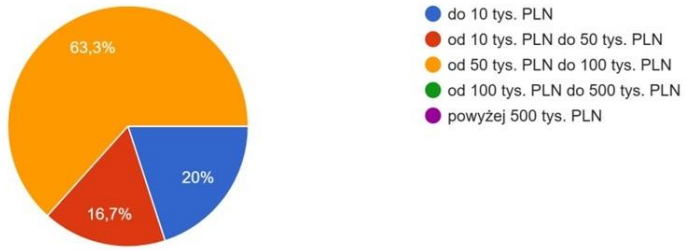
Wykres nr 6 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: czy Pani/Pana zdaniem koszt netto wymiany sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn (koszt wymiany jest rozumiany jako zakup nowych urządzeń, utylizacja wymienianych oraz usługa demontażu i instalacji nowych urządzeń) będzie na poziomie?



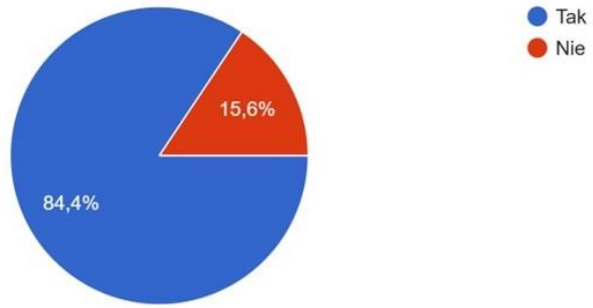
Wykres nr 7 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem wymiana posiadanego sprzętu teleinformatycznego, urządzeń elektronicznych, maszyn na sprzęt pochodzący wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?



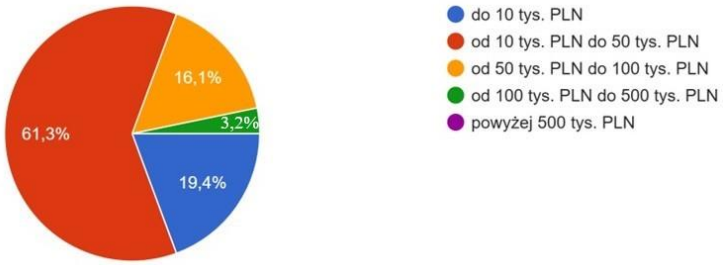
Wykres nr 8 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: będzie to kwota netto na poziomie?



Wykres nr 9 – Odpowiedzi udzielone na pytanie: Czy Pani/Pana zdaniem wymiana posiadanego oprogramowania (w tym programów komputerowych, aplikacji, sterowników, silników bazodanowych etc., niezależenie od formy posiadania – własność produktów, licencje, subskrypcje itp.) na oprogramowanie pochodzące wyłącznie z państw Unii Europejskiej i NATO będzie wiązała się z większymi kosztami serwisu i wsparcia technicznego?



Wykres nr 10 – Odpowiedzi udzielone na pytanie: Jeżeli TAK to: będzie to kwota netto na poziomie?



Podsumowanie, wnioski i rekomendacje Federacji Przedsiębiorcy.pl po przeprowadzonej ankiecie wśród przedsiębiorców

- **Nadmierna regulacja:** Nowe przepisy wprowadzają znacznie więcej ograniczeń niż wymaga tego dyrektywa NIS2.
- **Brak precyzji:** Niejasne kryteria dotyczące uznania podmiotów za kluczowe lub ważne, a także za dostawców wysokiego ryzyka.
- **Wysokie koszty:** Szacunkowe koszty dostosowania się do nowych przepisów są znaczne i mogą prowadzić do problemów finansowych przedsiębiorców.
- **Brak świadomości:** Większość przedsiębiorców nie jest świadoma nowych obowiązków i ich konsekwencji.

Wnioski i propozycje:

1. **Konieczność korekt legislacyjnych:**
    - **Doprecyzowanie kryteriów:** Należy jasno określić, które podmioty będą uznawane za kluczowe lub ważne, a także jakie czynniki będą brane pod uwagę przy ocenie dostawców wysokiego ryzyka.
    - **Zharmonizowanie z dyrektywą NIS2:** Przepisy krajowe powinny być dostosowane do wymagań dyrektywy, unikając nadmiernej regulacji.
    - **Ocena skutków finansowych:** Należy przeprowadzić rzetelną ocenę skutków finansowych nowych przepisów dla różnych sektorów gospodarki.
2. **Wsparcie dla przedsiębiorców:**
    - **Kampanie informacyjne:** Należy prowadzić szeroko zakrojone kampanie informacyjne, aby przedsiębiorcy byli świadomi nowych obowiązków i mieli możliwość przygotowania się do zmian.
    - **Konsultacje:** Należy zapewnić przedsiębiorcom możliwość konsultacji z ekspertami w zakresie cyberbezpieczeństwa.
    - **Wsparcie finansowe:** Można rozważyć wprowadzenie instrumentów wsparcia finansowego dla przedsiębiorców, którzy będą musieli ponieść znaczne koszty dostosowania się do nowych przepisów.
3. **Monitorowanie i ewaluacja:**
    - **Regularna ocena skuteczności przepisów:** Należy regularnie oceniać, czy nowe przepisy przynoszą oczekiwane efekty i czy nie powodują niepożądanych skutków ubocznych.

- **Dostosowanie przepisów do zmieniających się warunków:** W razie potrzeby należy wprowadzać niezbędne zmiany legislacyjne.

Propozycje działań:

- **Zorganizowanie debaty publicznej:** Zaproszenie przedstawicieli rządu, przedsiębiorców, ekspertów ds. cyberbezpieczeństwa i organizacji pozarządowych do dyskusji na temat nowych przepisów.
- **Współpraca z organizacjami przedsiębiorców:** Współpraca z organizacjami takimi jak Ogólnopolska Federacja Przedsiębiorców i Pracodawców – Przedsiębiorcy.pl w celu zbierania informacji zwrotnej od przedsiębiorców i reprezentowania ich interesów.

Wnioski końcowe:

Przedstawione wnioski i propozycje mają na celu przyczynić się do stworzenia bardziej efektywnego i zrównoważonego systemu cyberbezpieczeństwa w Polsce. Konieczna jest ścisła współpraca między rządem, przedsiębiorcami i ekspertami, aby znaleźć rozwiązania, które będą zarówno skuteczne w zapewnieniu bezpieczeństwa, jak i nie będą nadmiernie obciążały przedsiębiorców.

Autor: Dr n. pr. Marek Woch
Ekspert Centrum Legislacji Federacji Przedsiebiorcy.pl