Projekt z dnia 07.06.2019

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I

z dnia ……. 2019 r.

w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo

Na podstawie art. 14 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) zarządza się, co następuje:

§ 1. 1. Podmiot świadczący usługi z zakresu cyberbezpieczeństwa w zakresie warunków organizacyjnych jest obowiązany:

1) posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN-EN ISO/IEC 27001;
2) zapewnić ciągłość działania usłudze obsługi incydentu, polegającej na podejmowaniu działań w zakresie rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo systemów informacyjnych zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
3) posiadać i udostępniać w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF);
4) zapewnić wsparcie operatorowi usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej;
5) dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:
   a) identyfikowania zagrożeń w odniesieniu do systemów informacyjnych operatora usługi kluczowej oraz proponowania rozwiązań ograniczających ryzyko wynikające z tych zagrożeń,
   b) analizowania oprogramowania szkodliwego i określania jego wpływu na system informacyjny operatora usługi kluczowej,
   c) wykrywania przełamywania lub omijania zabezpieczeń systemu informacyjnego operatora usługi kluczowej, prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego,

d) zabezpieczania informacji potrzebnych do analizy powłamaniowej pozwalające na określenie charakteru, zakresu i czasu trwania incydentu na potrzeby postępowań prowadzonych przez organy ścigania.

2. Wewnętrzna struktura organizacyjna operatora usługi kluczowej jest obowiązana spełniać warunki, o których mowa w ust. 1 pkt 1, 2, 4 i 5.

§ 2. 1. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo, które wykonują czynności związane z realizacją obowiązków, o których mowa w art. 8 pkt 3, 4 i 6, art. 11 ust. 1 pkt 1-5 oraz art. 12-13 ustawy o krajowym systemie cyberbezpieczeństwa są obowiązane dysponować prawem do wyłącznego korzystania z pomieszczeń, które wyposażone są w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej w:

1) system sygnalizacji włamania i napadu stopnia 2 według Polskiej Normy PN-EN 50131-1 z transmisją alarmu do alarmowego centrum odbiorczego, zapewniający identyfikację użytkowników włączających i wyłączających system lub jego część;
2) system kontroli dostępu stopnia 2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia przez co najmniej rzecz posiadaną przez tą osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem, wyposażony w rezerwowe źródło zasilania, podtrzymujące działanie systemu po zaniku napięcia zasilania z sieci energetycznej przez okres wynikający z szacowania ryzyka;
3) system wykrywania i sygnalizacji pożaru z powiadamianiem do centrum odbiorczego alarmów pożarowych;
4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych o istotnym znaczeniu dla prowadzonej działalności, klasy S1 spełniającymi wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy lub okoliczności wymagają zastosowania dla szaf wyższej klasy odporności na włamanie lub odporności pożarowej;
5) zabezpieczenia zewnętrznych drzwi wejściowych do pomieszczeń rozwiązaniem o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627;
6) otwory okienne zabezpieczone w klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia;

7) ściany zewnętrzne o odporności na włamanie o klasie odporności RC3 według wymagań Polskiej Normy PN-EN 1627.

2. W przypadku, gdy obiekt, w którym znajdują się pomieszczenia wskazane w ust. 1, nie jest wyposażony w system, o którym mowa w ust. 1 pkt 3, dopuszcza się, po wykonaniu szacowania ryzyka i gdy brak jest przeciwwskazań wynikających z innych przepisów, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania i napadu, o ile alarmowe centrum odbiorcze monitorujące alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów.

§ 3. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo w zakresie spełnienia warunków technicznych dysponują:

1) sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:
   a) automatyczne rejestrowanie zgłoszeń incydentów,
   b) analizę kodu oprogramowania uznanego za szkodliwe,
   c) badanie odporności systemów informacyjnych na przełamanie zabezpieczeń,
   d) zabezpieczania informacji potrzebnych do analizy powłamaniowej pozwalające na określenie charakteru, zakresu i czasu trwania incydentu na potrzeby postępowań prowadzonych przez organy ścigania;
2) środkami łączności umożliwiającymi wymianę informacji z podmiotami, dla których świadczą usługi, oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

§ 4. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo realizujące inne obowiązki niż wymienione w § 2 ust. 1 zobowiązane są wprowadzić zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji zgodnie z oszacowanym ryzykiem.

§ 5. W przypadku wykonywania czynności związanych z realizacją obowiązków, o których mowa w art. 8 pkt 3, 4 i 6, art. 11 ust. 1 pkt 1-5 oraz art. 12-13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, poza pomieszczeniami wyposażonymi w zabezpieczenia opisane w § 2 ust. 1, podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych

odpowiedzialne za cyberbezpieczeństwo zapewniają bezpieczeństwo pracy zdalnej, przez co najmniej:

1) ustalenie zasad świadczenia pracy zdalnej;

2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;

3) minimalizację przechowywanych danych poza bezpiecznym środowiskiem.

§ 6. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo, w terminie 30 dni od dnia wejścia w życie niniejszego rozporządzenia, dostosują pomieszczenia do wymogów określonych w § 2.

§ 7. Traci moc rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 1780).

§ 8. Rozporządzenie wchodzi w życie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

Za zgodność pod względem prawnym, redakcyjnym i legislacyjnym
Katarzyna Prusak - Górniak
Dyrektor
Departamentu Prawnego
Ministerstwa Cyfryzacji
/-podpisano elektronicznie/

U Z A S A D N I E N I E

Na mocy art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) na operatorów usług kluczowych nałożono obowiązki związane z wdrożeniem i zapewnieniem właściwego funkcjonowania systemu zarządzania bezpieczeństwem w systemach informacyjnych, wykorzystywanych do świadczenia usług kluczowych. Dla wykonania tych zadań każdy operator winien powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z tego zakresu.

Po wejściu w życie obecnie obowiązującego rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 1780), podmioty zobowiązane skierowały do Ministerstwa Cyfryzacji uwagi dotyczące zagadnień związanych z wdrażaniem wymagań wynikających z tego aktu wykonawczego. Powyższe kwestie omawiane były również na spotkaniach roboczych w Ministerstwie Cyfryzacji.

Omawiano potrzebę wprowadzenia następujących zmian:

- proporcjonalność wymogów (wymogi dostosowane do realizowanych obowiązków);
- usprawnienie istniejących wymogów;
- doprecyzowanie „miękkich zapisów” (np. rozbicie obowiązków typu „czynności z zakresu informatyki śledczej” na poszczególne obowiązki).

Doprecyzowano przepisy dotyczące zabezpieczeń technicznych zgodnie ze wskazówkami Polskiej Izby Systemów Alarmowych oraz uwagami przedsiębiorców, dopuszczono pracę zdalną (z odrębnymi zabezpieczeniami), rozróżniono rodzaje zabezpieczeń w zależności od realizowanych czynności (podział na czynności techniczne i organizacyjne).

Projektowany § 1 wskazuje warunki organizacyjne, jakie musi spełniać podmiot świadczący usługi z zakresu cyberbezpieczeństwa oraz wewnętrzna struktura organizacyjna operatora usługi kluczowej. Doprecyzowano warunki dotyczące personelu.

Projektowany § 2 określa wymogi dotyczące pomieszczeń. Istotną zmianą w tym paragrafie jest wskazanie, że pomieszczenia mają służyć bezpiecznemu realizowaniu następujących czynności:

- art. 8 pkt 3,4 i 6 (zbieranie informacji o zagrożeniach, cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zarządzanie incydentami oraz stosowanie bezpiecznej łączności na potrzeby krajowego systemu cyberbezpieczeństwa);
- art. 11 ust. 1 pkt 1-5 (działania związane z incydentami) oraz
- art. 12-13 (zgłaszanie incydentów i innych informacji do zespołów CSIRT).

Pozostałe obowiązki, takie jak art. 8 pkt 1-2 (prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem oraz wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych), art. 9 (wyznaczanie osób kontaktowych), art. 10 (postępowanie z dokumentacją) oraz art. 11 ust. 1 pkt 6 (usuwanie podatności) powinny być realizowane po wprowadzeniu zabezpieczeń zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych informacji zgodnie z oszacowanym ryzykiem w danej organizacji. Usunięto wymogi dotyczące ścian wewnętrznych.

W projektowanym § 5 wprowadza się możliwość pracy zdalnej. Jest ona dopuszczalna, pod warunkiem zapewnienia bezpieczeństwa pracy zdalnej, przez co najmniej:

1) ustalenie zasad świadczenia pracy zdalnej;

2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;

3) minimalizację przechowywanych danych poza bezpiecznym środowiskiem.

Rozporządzenie będzie dopuszczać dzięki temu możliwość np. konsultacji z ekspertami czy zlecenie analizy zewnętrznej firmie. Wyżej wymienione środki ostrożności pozwolą zmniejszyć ryzyko wycieku danych dotyczących incydentu oraz wpływu na referencyjność próbek. Zasadą ma być świadczenie usług „certowych” w bezpiecznym środowisku, pozwalającym na ochronę informacji operatora usługi kluczowej.

W projektowanym § 6 zawarto przepis przejściowy, zgodnie z którym podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury organizacyjne operatorów usług kluczowych odpowiedzialne za cyberbezpieczeństwo, które wykonują czynności związane z realizacją obowiązków, o których mowa w art. 8 pkt 3, 4 i 6, art. 11 ust.

1 pkt 1-5 oraz art. 12-13 ustawy o krajowym systemie cyberbezpieczeństwa, w terminie 30 dni od dnia wejścia w życie niniejszego rozporządzenia, dostosują pomieszczenia do wymogów określonych w § 2.

Zawarte w projekcie regulacje nie stanowią przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039, z późn. zm.), dlatego też projekt rozporządzenia nie podlega procedurze notyfikacji.

Projektowane rozporządzenie nie wymaga przedstawiania organom i instytucjom Unii Europejskiej w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt zostanie udostępniony w Biuletynie Informacji Publicznej. Ponadto zgodnie z § 52 ust. 1 uchwały Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006, z późn. zm.), zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Zawarte w projekcie regulacje będą miały wpływ na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. 2018 poz. 646, z późn. zm.).

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Nazwa projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Sekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa tel. (22) 245 59 22, e-mail: sekretariat.dc@mc.gov.pl Jakub Dysarz, Departament Cyberbezpieczeństwa tel. (22) 245 58 38, e-mail: jakub.dysarz@mc.gov.pl	**Data sporządzenia** 03.06.2019 **Źródło:** art. 14 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) **Nr w wykazie prac MC**: **132**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Na mocy art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) na operatorów usług kluczowych nałożono obowiązki związane z wdrożeniem i zapewnieniem właściwego funkcjonowania systemu zarządzania bezpieczeństwem w systemach informacyjnych, wykorzystywanych do świadczenia usług kluczowych.
Dla wykonania tych zadań każdy operator winien powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z tego zakresu.
Obecnie obowiązujące rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz. U. poz. 1780) okazało się być trudne we wdrożeniu, nie dopuszczając niektórych form współpracy z ekspertami z zakresu cyberbezpieczeństwa. Wobec uzyskanych informacji z rynku, Ministerstwo Cyfryzacji zorganizowało spotkanie z przedsiębiorcami, podczas którego omówiono możliwości zmiany ww. rozporządzenia. Ponadto, swoje uwagi zgłosiła Polska Izba Systemów Alarmowych, wskazując konieczność doprecyzowania niektórych zapisów, które wynikały z odniesień do norm technicznych.
Zgłoszono potrzebę wprowadzenia następujących zmian:
- proporcjonalność wymogów (wymogi dostosowane do realizowanych obowiązków);
- usprawnienie istniejących wymogów;
- doprecyzowanie „miękkich zapisów” (np. rozbicie obowiązków typu „czynności z zakresu informatyki śledczej” na poszczególne obowiązki).
Niniejszy projekt jest wynikiem ww. spotkania.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Doprecyzowano przepisy dotyczące zabezpieczeń technicznych zgodnie ze wskazówkami Polskiej Izby Systemów Alarmowych oraz uwagami przedsiębiorców, dopuszczono pracę zdalną (z odrębnymi zabezpieczeniami), rozróżniono rodzaje zabezpieczeń w zależności od realizowanych czynności (podział na czynności techniczne i organizacyjne).

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	64	Wykaz operatorów usług kluczowych (stan na 31 maja 2019 r.).	Wprowadzenie zabezpieczeń określonych w rozporządzeniu bądź nawiązanie współpracy z firmami, które świadczą usługi zgodnie z rozporządzeniem.
Podmioty świadczące usługi z zakresu cyberbezpieczeństwa	ok. 20	Szacunki oparte na danych własnych	Dostosowanie się do wymogów
Eksperci z zakresu cyberbezpieczeństwa	n/a	n/a	Umożliwienie ekspertom tzw. trzeciej linii współpracy z podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach harmonogramu prac nad projektem rozporządzenia przewidziane jest przeprowadzenie uzgodnień międzyresortowych, opiniowania oraz konsultacji publicznych z partnerami społecznymi, a także zorganizowanie konferencji uzgodnieniowej z udziałem podmiotów biorących udział w uzgodnieniach międzyresortowych oraz opiniowaniu.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt zostanie udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej MC oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0

pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	n/a

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu. Pojawi się możliwość zasięgania opinii ekspertów (często działających na zasadach zlecenia dla jednoosobowej działalności gospodarczej) co do konkretnego przypadku.						
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje zamieszczone w rozporządzeniu przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele.						
Niemierzalne	-	Nie dotyczy						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Projekt rozporządzenia nie ma wpływu na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na sytuację ekonomiczną i społeczną rodziny, a także osób niepełnosprawnych oraz osób starszych, a także na obywateli i gospodarstwa domowe.						

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy	
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

Pozytywny – przepisy przyczynią się do wzrostu zatrudnienia w obszarze cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Przepisy rozporządzenia przyczynią się do zwiększenia poziomu cyberbezpieczeństwa, co będzie miało pozytywny wpływ na przedsiębiorców i obywateli.	

11. Planowane wykonanie przepisów aktu prawnego

Po upływie okresów przewidzianych na wprowadzenie odpowiednich rozwiązań (vacatio legis) bądź dostosowanie istniejących przez adresatów aktu.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

100% operatorów ma wdrożone odpowiednie rozwiązania, po roku od wejścia w życie przepisów.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak