Warszawa, dnia 23 czerwca 2025 r.

Poz. 810

ROZPORZĄDZENIE RADY MINISTRÓW

z dnia 6 czerwca 2025 r.

w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa

Na podstawie art. 32a ust. 14 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, z późn. zm.[1)]) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) warunki i tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 32a ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, zwanej dalej „ustawą”;

2) czynności niezbędne do przeprowadzania oceny bezpieczeństwa;

3) warunki i tryb dokonywania uzgodnień ramowych warunków przeprowadzania oceny bezpieczeństwa z organami administracji publicznej, właścicielami, posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122 oraz z 2024 r. poz. 834, 1222, 1473, 1572 i 1907).

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) ocena bezpieczeństwa – ocenę, o której mowa w art. 32a ust. 1 ustawy;

2) system – systemy teleinformatyczne i sieci teleinformatyczne, o których mowa w art. 32a ust. 1 ustawy, podlegające ocenie bezpieczeństwa;

3) architektura systemu – opis składników systemu teleinformatycznego lub sieci teleinformatycznej oraz powiązań i relacji między tymi składnikami;

4) usługa sieciowa – właściwość systemu teleinformatycznego polegającą na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze;

5) podmiot zarządzający systemem – podmiot, o którym mowa w art. 32a ust. 3 ustawy;

6) roczny plan – roczny plan przeprowadzania oceny bezpieczeństwa, o którym mowa w art. 32a ust. 2 ustawy.

§ 3. 1. W ramach oceny bezpieczeństwa przeprowadza się następujące czynności:

1) pasywne zbieranie informacji – zbieranie w sieci Internet informacji związanych z funkcjonowaniem systemu, wpływających na jego bezpieczeństwo;

2) półpasywne zbieranie informacji – zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, na zasadach właściwych dla użytkownika tego systemu, z wyłączeniem uprawnień wymagających uwierzytelnienia w tym systemie; czynności te mogą być uzupełnione zbieraniem informacji wynikających z analizy architektury systemu;

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1222, 1562, 1684 i 1871 oraz z 2025 r. poz. 179 i 718.

3) aktywne zbieranie informacji – zbieranie w systemie informacji związanych z funkcjonowaniem tego systemu, wpływających na jego bezpieczeństwo, w sposób przekraczający uprawnienia użytkownika systemu, w tym wymagających uwierzytelnienia w systemie, w szczególności polegających na enumeracji usług, portów, wykrywaniu urządzeń pośredniczących, wykrywaniu systemów IDS/IPS oraz zapór ogniowych;

4) identyfikacja podatności architektury systemu i usług sieciowych – podejmowanie czynności mających na celu identyfikację podatności, o której mowa w art. 32a ust. 4 ustawy, dokonywanych na podstawie informacji uzyskanych w ramach czynności, o których mowa w pkt 1–3, oraz na podstawie informacji na temat architektury systemu udostępnionych przez podmiot zarządzający systemem.

2. W ramach oceny bezpieczeństwa poza czynnościami, o których mowa w ust. 1, mogą być również przeprowadzane, za zgodą podmiotu zarządzającego systemem, następujące czynności:

1) wykorzystanie podatności – podejmowanie w systemie czynności nakierowanych na użycie podatności zidentyfikowanych w ramach czynności, o której mowa w ust. 1 pkt 4, w celu ominięcia zabezpieczeń systemu oraz identyfikacji podatności, których identyfikacja jest niemożliwa w ramach czynności, o której mowa w ust. 1 pkt 4;

2) analiza wpływu wykorzystania czynników inżynierii społecznej – wykorzystanie ogólnych metod inżynierii społecznej, które mają na celu uzyskanie informacji na temat zachowania użytkowników systemu, w celu weryfikacji procedur bezpieczeństwa badanego systemu realizowanych przez tych użytkowników; czynności mogą być wykonywane z zastosowaniem narzędzi, o których mowa w art. 32a ust. 7 ustawy;

3) analiza odporności systemu na działania narzędzi, o których mowa w art. 32a ust. 7 ustawy – zaplanowane zastosowanie narzędzi, o których mowa w art. 32a ust. 7 ustawy, w celu zbadania możliwości wykorzystania luk w zabezpieczeniach systemu, polegające na badaniu odporności systemu na możliwość wykorzystania go do popełniania przestępstw, o których mowa w art. 32a ust. 7 ustawy.

§ 4. 1. Przed przeprowadzeniem oceny bezpieczeństwa Agencja Bezpieczeństwa Wewnętrznego, zwana dalej „ABW”, zwraca się do podmiotu zarządzającego systemem o przekazanie informacji dotyczących systemu, które mogą obejmować:

1) architekturę systemu, w tym informacje o urządzeniach wchodzących w skład infrastruktury systemu;

2) adresację sieciowej infrastruktury systemu;

3) informację o posiadaniu aktualnej kopii bezpieczeństwa systemu i zasad jej aktualizacji;

4) określenie czasu wymaganego do przywrócenia systemu z kopii bezpieczeństwa systemu;

5) informację o posiadaniu środowiska testowego i o jego zakresie;

6) zabezpieczenia teleinformatyczne systemu;

7) procedury bezpieczeństwa systemu;

8) dane osoby wyznaczonej przez kierownika podmiotu zarządzającego systemem do bieżącego kontaktu z ABW w czasie przeprowadzania oceny bezpieczeństwa, zwanej dalej „osobą wyznaczoną”;

9) dane osoby upoważnionej przez kierownika podmiotu zarządzającego systemem do reprezentowania tego podmiotu w ramach oceny bezpieczeństwa, zwanej dalej „osobą upoważnioną”.

2. Podmiot zarządzający systemem przekazuje informacje, o których mowa w ust. 1, w terminie:

1) 14 dni od dnia otrzymania wystąpienia ABW – w przypadku systemu ujętego w rocznym planie;

2) 7 dni od dnia otrzymania wystąpienia ABW – w przypadku systemu nieujętego w rocznym planie.

§ 5. 1. ABW dokonuje analizy informacji, o których mowa w § 4 ust. 1, w celu przygotowania propozycji oceny bezpieczeństwa.

2. ABW w terminie 30 dni od dnia otrzymania informacji, o których mowa w § 4 ust. 1, przekazuje podmiotowi zarządzającemu systemem projekt porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa, obejmujące w szczególności:

1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;

2) zakres przeprowadzanych testów, w tym czynności, o których mowa w § 3;

3) rodzaj przeprowadzanych testów, o których mowa w przepisach wydanych na podstawie art. 32a ust. 12 ustawy.

§ 6. 1. Podmiot zarządzający systemem w terminie 14 dni od dnia otrzymania projektu porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa może wnieść zastrzeżenia do treści tego projektu wraz z uzasadnieniem tych zastrzeżeń.

2. Zastrzeżenia do treści projektu porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa mogą obejmować w szczególności rodzaj i zakres przeprowadzanych testów z uwzględnieniem konieczności minimalizacji zakłócenia pracy systemu lub ograniczenia jego dostępności bądź nieodwracalnego zniszczenia danych przetwarzanych w systemie.

§ 7. 1. ABW odnosi się do zastrzeżeń do treści projektu porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa w terminie 14 dni od dnia ich otrzymania.

2. W przypadku gdy uwzględnienie zastrzeżeń do treści projektu porozumienia zawierającego ramowe warunki przeprowadzenia oceny bezpieczeństwa może spowodować, że ocena bezpieczeństwa stanie się niekompletna lub zwiększy możliwość wystąpienia zakłócenia pracy systemu lub ograniczenia jego dostępności bądź nieodwracalnego zniszczenia danych przetwarzanych w systemie, ABW odstępuje od przeprowadzenia tej oceny.

3. Podmiot zarządzający systemem w terminie 7 dni od dnia otrzymania informacji o odstąpieniu od przeprowadzenia oceny bezpieczeństwa może zwrócić się z pisemnym wnioskiem do ABW o przeprowadzenie tej oceny w przypadkach, o których mowa w ust. 2, akceptując niekompletność oceny bezpieczeństwa lub możliwość wystąpienia negatywnych następstw oceny bezpieczeństwa związanych z zakłóceniem pracy systemu lub ograniczeniem jego dostępności.

§ 8. 1. ABW odstępuje od przeprowadzenia oceny bezpieczeństwa, w sytuacji gdy:

1) podmiot zarządzający systemem przekaże informację o tym, że nie posiada aktualnej kopii bezpieczeństwa systemu;

2) z analizy, o której mowa w § 5 ust. 1, wynika, że:
   a) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie, który będzie podlegał ocenie bezpieczeństwa,
   b) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność,
   c) podczas przeprowadzania oceny bezpieczeństwa może dojść do uszkodzenia urządzeń wchodzących w skład infrastruktury tego systemu oraz innych systemów teleinformatycznych podmiotu zarządzającego systemem,
   d) istnieje zagrożenie ograniczenia dostępności usług świadczonych drogą elektroniczną przez podmiot zarządzający systemem.

2. ABW informuje podmiot zarządzający systemem o odstąpieniu od przeprowadzenia oceny bezpieczeństwa oraz o okolicznościach i przyczynach tego odstąpienia.

3. Podmiot zarządzający systemem w terminie 7 dni od dnia otrzymania informacji o odstąpieniu od przeprowadzenia oceny bezpieczeństwa może zwrócić się z pisemnym wnioskiem do ABW o przeprowadzenie tej oceny mimo zaistnienia zagrożeń, o których mowa w ust. 1 pkt 2 lit. b–d, akceptując możliwość wystąpienia tych zagrożeń i ich negatywnych następstw.

§ 9. W przypadku gdy z analizy, o której mowa w § 5 ust. 1, wynika konieczność udostępnienia pomieszczeń lub urządzeń wchodzących w skład infrastruktury systemu funkcjonariuszowi ABW lub pracownikowi ABW przeprowadzającemu ocenę bezpieczeństwa, ABW uzgadnia z podmiotem zarządzającym systemem sposób udostępniania tych pomieszczeń lub urządzeń.

§ 10. 1. Po przeprowadzeniu uzgodnień, o których mowa w § 4–9, Szef ABW i kierownik podmiotu zarządzającego systemem zawierają porozumienie o przeprowadzeniu oceny bezpieczeństwa.

2. Porozumienie o przeprowadzeniu oceny bezpieczeństwa zawiera w szczególności:

1) harmonogram oceny bezpieczeństwa, w tym datę jej rozpoczęcia i zakończenia;

2) zakres przeprowadzanych testów, w tym czynności, o których mowa w § 3;

3) rodzaj przeprowadzanych testów, o których mowa w przepisach wydanych na podstawie art. 32a ust. 12 ustawy;

4) zgodę podmiotu zarządzającego systemem na przeprowadzenie oceny bezpieczeństwa w sytuacji, o której mowa w § 7 ust. 3 lub § 8 ust. 3;

5) sposób udostępniania pomieszczeń lub urządzeń wchodzących w skład infrastruktury tego systemu;

6) dane osoby wyznaczonej;

7) dane osoby upoważnionej.

3. Wzór porozumienia o przeprowadzeniu oceny bezpieczeństwa jest określony w załączniku do rozporządzenia.

§ 11. Podmiot zarządzający systemem utrzymuje za pośrednictwem osoby wyznaczonej stały kontakt z funkcjonariuszem ABW lub pracownikiem ABW przeprowadzającym ocenę bezpieczeństwa, w celu bieżącej konsultacji związanej z przebiegiem przeprowadzanej oceny bezpieczeństwa, w tym przekazywania informacji o zidentyfikowanych w systemie zakłóceniach wywołanych przeprowadzaną oceną bezpieczeństwa.

§ 12. 1. Funkcjonariusz ABW lub pracownik ABW przeprowadzający ocenę bezpieczeństwa wstrzymuje prowadzenie czynności, jeżeli:

1) otrzymał od osoby wyznaczonej informację o zakłóceniach w prawidłowym funkcjonowaniu systemu, które mogą skutkować zagrożeniami, o których mowa w § 8 ust. 1 pkt 1 lub pkt 2 lit. a, c lub d;

2) pojawiło się jedno z zagrożeń, o których mowa w § 8 ust. 1 pkt 1 lub pkt 2 lit. a, c lub d, albo uzasadnione podejrzenie ich wystąpienia.

2. ABW informuje podmiot zarządzający systemem o wstrzymaniu prowadzenia czynności w przypadkach, o których mowa w ust. 1, oraz o okolicznościach i przyczynach tego wstrzymania.

3. Podmiot zarządzający systemem w terminie 2 dni roboczych od daty poinformowania o wstrzymaniu prowadzenia czynności w przypadkach, o których mowa w ust. 1, może zwrócić się z pisemnym wnioskiem do ABW o dalsze prowadzenie czynności w ramach oceny bezpieczeństwa mimo zaistnienia zagrożeń, o których mowa w § 8 ust. 1 pkt 2 lit. c lub d, akceptując możliwość wystąpienia tych zagrożeń lub ich negatywnych następstw.

4. W przypadku nieotrzymania wniosku, o którym mowa w ust. 3, ABW odstępuje od dalszego przeprowadzania oceny bezpieczeństwa.

§ 13. 1. Po przeprowadzeniu oceny bezpieczeństwa ABW opracowuje raport z przeprowadzonej oceny bezpieczeństwa w terminie 60 dni od dnia jej zakończenia.

2. Raport z przeprowadzonej oceny bezpieczeństwa zawiera w szczególności:

1) datę rozpoczęcia i zakończenia oceny bezpieczeństwa oraz jej harmonogram;

2) zakres przeprowadzonych testów, w tym czynności, o których mowa w § 3;

3) rodzaj przeprowadzonych testów, o których mowa w przepisach wydanych na podstawie art. 32a ust. 12 ustawy;

4) informację o zgodzie podmiotu zarządzającego systemem na przeprowadzenie oceny bezpieczeństwa w sytuacji, o której mowa w § 7 ust. 3 lub § 8 ust. 3, lub o braku tej zgody;

5) informację o zaistnieniu okoliczności, o których mowa w § 12 ust. 1, oraz informację o otrzymaniu wniosku, o którym mowa w § 12 ust. 3, lub informację o odstąpieniu od przeprowadzania oceny bezpieczeństwa, o którym mowa w § 12 ust. 4;

6) informację o aktualności wyników przeprowadzonej oceny bezpieczeństwa w odniesieniu do czasu jej przeprowadzenia i zakończenia;

7) wyniki przeprowadzonej oceny bezpieczeństwa zawierające wykaz zidentyfikowanych podatności oraz poziom ich zagrożenia dla ocenianego systemu;

8) zalecenia i rekomendacje.

§ 14. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.[2)]

Prezes Rady Ministrów: *D. Tusk*

[2)] Niniejsze rozporządzenie było poprzedzone rozporządzeniem Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym (Dz. U. poz. 1076), które traci moc z dniem wejścia w życie niniejszego rozporządzenia zgodnie z art. 11 ust. 2 ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 1834).

Załącznik do rozporządzenia Rady Ministrów
z dnia 6 czerwca 2025 r. (Dz. U. poz. 810)

WZÓR

.....
(klauzula tajności – po wypełnieniu)

.....
(sygnatura literowo-cyfrowa)

Egz. nr .....

POROZUMIENIE

zawarte w dniu ..... w Warszawie

o przeprowadzeniu oceny bezpieczeństwa

§ 1

1. Przedmiotem porozumienia o przeprowadzeniu oceny bezpieczeństwa, zwanego dalej „porozumieniem”, jest przeprowadzenie przez ABW oceny bezpieczeństwa, w rozumieniu art. 32a ust. 1 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2024 r. poz. 812, z późn. zm.), zwanej dalej „ustawą”, następujących systemów teleinformatycznych lub sieci teleinformatycznych podmiotu zarządzającego systemem:
   .....
   .....
   .....
   ..... ,
   zwanych dalej „systemem”.
2. Stronami porozumienia są:
   Szef Agencji Bezpieczeństwa Wewnętrznego: .....
   (stopień, imię i nazwisko)
   kierownik podmiotu zarządzającego systemem: .....
   (stanowisko i nazwa podmiotu)
3. Ocena bezpieczeństwa rozpocznie się z dniem ..... r.

§ 2

1. W celu realizacji przedmiotu porozumienia ABW wykona czynności określone w § 3 ust. 1 rozporządzenia Rady Ministrów z dnia 6 czerwca 2025 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym lub uprawdopodabniającym popełnienie przestępstwa szpiegostwa (Dz. U. poz. 810), zwanego dalej „rozporządzeniem”.

.....
(klauzula tajności – po wypełnieniu)

.....
(klauzula tajności – po wypełnieniu)

.....
(sygnatura literowo-cyfrowa)

Egz. nr .....

2.* Podmiot zarządzający systemem, działając w trybie § 3 ust. 2 rozporządzenia, wyraża zgodę na dokonanie przez ABW, w ramach oceny bezpieczeństwa, następujących czynności:

.....
.....
.....
.....
.....
.....
.....
.....
.....

3.* Podmiot zarządzający systemem wyraża zgodę na przeprowadzenie przez ABW, w ramach oceny bezpieczeństwa, następujących testów bezpieczeństwa[1)]:

.....
.....
.....
.....

4. ABW po przeprowadzeniu oceny bezpieczeństwa sporządza i przekazuje w terminie, o którym mowa w § 13 ust. 1 rozporządzenia, podmiotowi zarządzającemu systemem raport, o którym mowa w art. 32a ust. 10 ustawy, spełniający wymagania określone w § 13 ust. 2 rozporządzenia.

§ 3

Podmiot zarządzający systemem oświadcza, że systemy teleinformatyczne wskazane do przeprowadzenia oceny bezpieczeństwa pozostają w jego faktycznej oraz prawnej dyspozycji oraz że posiada on wszelkie prawa do wdrożenia we wskazanych systemach takich testów w zakresie określonym w porozumieniu oraz na zasadach w nim określonych.

§ 4

1. Podmiot zarządzający systemem przekazuje ABW w terminie, o którym mowa w § 4 ust. 2 pkt 1 / § 4 ust. 2 pkt 2* rozporządzenia, informacje, o których mowa w § 4 ust. 1 rozporządzenia.
2. Podmiot zarządzający systemem może zwrócić się do ABW, w trybie § 7 ust. 3 lub § 8 ust. 3 rozporządzenia, z pisemnym wnioskiem o przeprowadzenie oceny bezpieczeństwa mimo wystąpienia jednej z przesłanek, o których mowa w § 7 ust. 2 lub § 8 ust. 1 pkt 2 lit. b–d rozporządzenia.

[1)] Rodzaje testów bezpieczeństwa przeprowadzanych przez ABW są określone w zarządzeniu Szefa ABW wydanym na podstawie art. 32a ust. 12 ustawy i ogłoszonym przez Szefa ABW w Dzienniku Urzędowym Agencji Bezpieczeństwa Wewnętrznego.

.....
(klauzula tajności – po wypełnieniu)

.....
(klauzula tajności – po wypełnieniu)

.....
(sygnatura literowo-cyfrowa)

Egz. nr .....

§ 5

W przypadku wyrażenia zgody na przeprowadzenie przez ABW czynności i testów, o których mowa odpowiednio w § 2 ust. 2 i 3 porozumienia, lub w przypadku przeprowadzenia przez ABW oceny bezpieczeństwa, o której mowa w § 4 ust. 2 porozumienia, odpowiedzialność za ewentualne skutki ich przeprowadzenia przez ABW ponosi podmiot zarządzający systemem.

§ 6

Ustanawia się następujący harmonogram oceny bezpieczeństwa:

.....
.....
.....
.....

§ 7

* Ustanawia się następujący sposób udostępniania pomieszczeń lub urządzeń wchodzących w skład infrastruktury systemu podmiotu zarządzającego systemem:

.....
.....

§ 8

W celu zapewnienia sprawnej realizacji porozumienia kierownik podmiotu zarządzającego systemem:

1) upoważnia Panią/Pana* ..... ,
dane kontaktowe: ..... ,
do reprezentowania go przed ABW w ramach oceny bezpieczeństwa;
2) wyznacza Panią/Pana* ..... ,
dane kontaktowe: ..... ,
do bieżącego kontaktu oraz udzielania wyjaśnień i przekazywania ABW informacji dotyczących funkcjonowania systemu.

§ 9

Podmiot zarządzający systemem oświadcza, że jeżeli przeprowadzenie oceny bezpieczeństwa systemów teleinformatycznych przez ABW wymaga podjęcia jakichkolwiek dodatkowych czynności formalnoprawnych lub organizacyjnych, w szczególności uzyskania stosownych zgód właściwych podmiotów czy też poinformowania tych podmiotów o prowadzonych działaniach, podmiot zarządzający systemem ponosi odpowiedzialność za właściwą realizację takich czynności.

.....
(klauzula tajności – po wypełnieniu)

.....
(klauzula tajności – po wypełnieniu)

.....
(sygnatura literowo-cyfrowa)

Egz. nr .....

§ 10

1. Porozumienie zawiera się na czas przeprowadzenia oceny bezpieczeństwa.
2. Wszelkie zmiany porozumienia mogą być dokonywane wyłącznie za zgodną wolą stron, z zachowaniem formy pisemnej pod rygorem nieważności.

§ 11

Porozumienie sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla ABW i podmiotu zarządzającego systemem.

§ 12

Porozumienie wchodzi w życie z dniem podpisania.

.....	.....
(podpis Szefa ABW albo osoby upoważnionej)	(podpis kierownika podmiotu zarządzającego systemem albo osoby upoważnionej)

* Niepotrzebne skreślić.