Projekt z dnia 19 stycznia 2018 r.

ROZPORZĄDZENIE

MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI[1)]

z dnia <data wydania aktu> r.

w sprawie przetwarzania informacji przez Służbę Ochrony Państwa

Na podstawie art. 56 ust. 13 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138) zarządza się, co następuje:

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) tryb gromadzenia, przekazywania, sposoby przetwarzania w zbiorach danych informacji, danych osobowych, w tym danych osobowych uzyskanych lub przetwarzanych przez organy innych państw lub organizacje międzynarodowe, służących zapobieganiu lub zwalczaniu przestępczości;
2) sposób oceny danych pod kątem ich przydatności przy realizacji zadań formacji;
3) wzory dokumentów obowiązujących przy przetwarzaniu danych.

§ 2. Użyte w rozporządzeniu określenia i skróty oznaczają:

1) Komendant – Komendanta Służby Ochrony Państwa;
2) funkcjonariusz – funkcjonariusza Służby Ochrony Państwa;
3) ustawa – ustawę z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138);
4) zestaw zbiorów danych – kilka zbiorów danych prowadzonych na podstawie wspólnych dla tych zbiorów systemów teleinformatycznych, zintegrowanych wspólnymi środkami dostępu oraz zawierających powiązane ze sobą informacje, w tym dane osobowe.

§ 3. 1. Administratorem informacji, o których mowa w § 1 pkt 1, w tym danych osobowych, oraz zbiorów danych, w których są przetwarzane te informacje, jest Komendant.

[1)] Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej - sprawy wewnętrzne, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 10 stycznia 2018 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. poz. 97).

2. W odniesieniu do danych osobowych uzyskanych od organów władzy publicznej, organów innych państw, a następnie przetwarzanych przez Służbę Ochrony Państwa w celu realizacji jej zadań ustawowych, Komendant posiada uprawnienia i wykonuje zadania administratora danych, określone w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922).

§ 4. Sposób przetwarzania informacji, w tym danych osobowych, w zbiorach danych obejmuje:

1) tworzenie zbiorów danych w Służbie Ochrony Państwa;
2) wprowadzanie informacji, w tym danych osobowych, do zbiorów danych;
3) procedury zapewniające:
   a) pobieranie, gromadzenie i uzyskiwanie informacji, w tym danych osobowych,
   b) organizację dostępu do zbiorów danych i przetwarzania informacji, w tym danych osobowych, w sposób umożliwiający kontrolę dostępu do zbiorów danych i nadzór nad przetwarzaniem tych informacji,
   c) usuwanie informacji ze zbiorów danych.

Rozdział 2

Zbiory danych i ich zestawy

§ 5. 1. Zbiory danych, w których Służba Ochrony Państwa gromadzi lub przetwarza informacje, w tym dane osobowe, są prowadzone w systemach teleinformatycznych lub w formie sporządzanych ręcznie kartotek, skorowidzów, ksiąg, teczek, wykazów, registratur, rejestrów, albumów lub innych ewidencji.

2. Zbiór danych może być utworzony, gdy gromadzenie lub przetwarzanie informacji, w tym danych osobowych, w zbiorze danych pozwoli skuteczniej wykonywać zadania ustawowe Służby Ochrony Państwa lub zapewni lepszą kontrolę lub ochronę informacji lub lepszy nadzór nad nimi, niż w przypadku ich gromadzenia lub przetwarzania poza zbiorem danych, w szczególności mając na względzie cele prowadzenia danego zbioru, jego zakres rzeczowy lub terytorialny oraz sposoby przetwarzania w nim informacji.

3. Zestaw zbiorów danych może być utworzony, gdy jest celowe zintegrowanie, skoordynowanie i usprawnienie przetwarzania informacji, w tym danych osobowych, zgromadzonych w odrębnych zbiorach danych.

§ 6. 1. Zbiory danych oraz zestawy zbiorów danych tworzy, w drodze decyzji, Komendant, który ustala ich zakres informacyjny, rzeczowy i terytorialny, odpowiada za ich

wewnętrzną strukturę, przeznaczenie oraz funkcjonowanie w Służbie Ochrony Państwa, a także dostosowuje właściwości tych zbiorów lub zestawów oraz procedury przetwarzania w nich informacji, w tym danych osobowych, do rodzaju zadań wykonywanych przez Służbę Ochrony Państwa, zakresu informacji niezbędnych do wykonania określonego zadania, a także do celów przetwarzania informacji w tych zbiorach lub zestawach.

2. Komendant może zezwolić na wykonanie repliki całości lub części zbioru danych lub całości lub części zestawu zbiorów danych, w celu usprawnienia dostępu określonej komórki organizacyjnej Służby Ochrony Państwa do przetwarzanych informacji, w tym danych osobowych.

§ 7. 1. Komendant prowadzi rejestr zbiorów danych oraz zestawów zbiorów danych utworzonych w Służbie Ochrony Państwa.

2. Rejestr, o którym mowa w ust. 1, zawiera w szczególności:

1) oznaczenie rodzaju, formy prowadzenia i nazwy zbioru danych lub zestawu zbiorów danych oraz wskazanie daty wpisu do rejestru;
2) wskazanie osób odpowiedzialnych w imieniu administratora zbiorów danych w ramach struktury organizacyjnej Służby Ochrony Państwa za administrowanie zbiorem danych lub zestawem zbiorów danych i uprawnionych do korzystania ze zbioru danych lub zestawu zbiorów danych;
3) wskazanie daty utworzenia i podstawy prawnej prowadzenia zbioru danych lub zestawu zbiorów danych;
4) oznaczenie celu prowadzenia, zakresu informacyjnego, rzeczowego i terytorialnego zbioru danych lub zestawu zbiorów danych;
5) datę likwidacji zbioru danych lub zestawu zbiorów danych oraz numer ewidencyjny i datę sporządzenia protokołu likwidacji zbioru danych lub zestawu zbiorów danych;
6) określenie liczby utworzonych replik całości lub części zbioru danych lub liczby utworzonych replik całości lub części zestawu zbiorów danych wraz ze wskazaniem komórek organizacyjnych Służby Ochrony Państwa, dla których repliki utworzono, oraz wskazaniem dla każdej repliki informacji, o których mowa w pkt 2, 3 i 5.

3. Komendant prowadzi zbiór dokumentów zawierający, odrębnie dla każdego zbioru danych lub zestawu zbiorów danych, kopie:

1) aktów prawnych dotyczących utworzenia zbioru danych lub zestawu zbiorów danych;
2) dokumentów dotyczących zmian danych objętych rejestrem;
3) protokołu likwidacji zbioru danych lub zestawu zbiorów danych.

§ 8. 1. Zbiór danych lub zestaw zbiorów danych likwiduje się łącznie z wykonanymi replikami na podstawie decyzji Komendanta określającej datę likwidacji zbioru lub zestawu, skład osobowy komisji likwidacyjnej oraz sposób usunięcia informacji, w tym danych osobowych, zgromadzonych w tym zbiorze lub zestawie.

2. Z likwidacji zbioru danych lub zestawu zbiorów danych sporządza się protokół.

3. Wzór protokołu likwidacji zbioru danych albo zestawu zbiorów danych jest określony w załączniku nr 1 do rozporządzenia.

§ 9. 1. Zbiór danych oraz zestaw zbiorów danych może być przetwarzany przy użyciu kilku systemów teleinformatycznych, jeżeli wymagają tego cele przetwarzania.

2. W zestawach zbiorów danych zapewnia się zróżnicowanie dostępu do zbiorów danych w zależności od ich przeznaczenia oraz przydatności lub niezbędności określonych informacji, w tym danych osobowych, do wykonywania poszczególnych zadań Służby Ochrony Państwa.

Rozdział 3

Wprowadzanie informacji, w tym danych osobowych, do zbiorów danych, sposoby ich przetwarzania oraz kontrola dostępu do zbiorów danych i nadzór nad ich przetwarzaniem

§ 10. 1. Funkcjonariusze lub pracownicy Służby Ochrony Państwa wprowadzają informacje, w tym dane osobowe, do utworzonego zbioru danych, jeżeli w toku wykonywania czynności służbowych zaistniały okoliczności uzasadniające pobranie, uzyskanie lub zgromadzenie tych informacji i informacje te odpowiadają zakresowi rzeczowemu danego zbioru.

2. Funkcjonariusze lub pracownicy Służby Ochrony Państwa uprawnieni do przetwarzania informacji, w tym danych osobowych, w zbiorze danych, przed wykonaniem każdej operacji przetwarzania, sprawdzają, czy informacja podlegająca wprowadzeniu do zbioru danych nie została już do niego wprowadzona.

3. Funkcjonariusze lub pracownicy Służby Ochrony Państwa korzystają z informacji, w tym danych osobowych, przetwarzanych w zbiorach danych wyłącznie wtedy, gdy jest to przydatne lub niezbędne do prawidłowego wykonania czynności służbowych oraz podczas ich wykonywania.

§ 11. 1. Do przetwarzania informacji, w tym danych osobowych, oraz do użytkowania systemów teleinformatycznych, w których są przetwarzane informacje, o których mowa w § 1 pkt 1 i 2, a także informacje, o których mowa w art. 56 ust. 8 ustawy, udostępnione Służbie

Ochrony Państwa w sposób określony w art. 41 ust. 4 tej ustawy, dopuszcza się wyłącznie funkcjonariuszy lub pracowników Służby Ochrony Państwa upoważnionych przez Komendanta, zwanych dalej „osobami uprawnionymi".

2. Komendant określa, indywidualnie dla każdego zbioru danych, w trybie określonym w § 6, procedury nadawania, zmiany, cofania lub utraty uprawnień osobom uprawnionym. W tym samym trybie Komendant określa osoby upoważnione w jego imieniu do nadawania, zmiany i cofania uprawnień osobom uprawnionym.

§ 12. Przed dopuszczeniem do pracy przy przetwarzaniu informacji, w tym danych osobowych, w zbiorze danych, osobę uprawnioną zaznajamia się z przepisami dotyczącymi zbioru danych oraz przetwarzania informacji, w tym danych osobowych, w tym zbiorze danych, a także z przepisami dotyczącymi ochrony informacji, w tym danych osobowych, w nim zgromadzonych.

§ 13. 1. Systemy teleinformatyczne, w których są zgromadzone dane osobowe, wyposaża się w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do przetwarzanych danych.

2. Dla każdej osoby uprawnionej będącej użytkownikiem systemu teleinformatycznego ustala się odrębny identyfikator i hasło użytkownika.

3. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie teleinformatycznym może mieć miejsce wyłącznie po podaniu identyfikatora i właściwego hasła użytkownika.

§ 14. 1. Uzyskanie danych i informacji, w tym danych osobowych, na podstawie art. 40 ust. 3 ustawy, którymi dysponują organy władzy publicznej lub inne podmioty, odbywa się na podstawie pisemnego wniosku o ich przekazanie lub udostępnienie, którym komórki organizacyjne Służby Ochrony Państwa zwracają się do organu lub podmiotu dysponującego tymi informacjami.

2. Wniosek, o którym mowa w ust. 1, zawiera:

1) oznaczenie sprawy;
2) określenie zbioru danych, z którego informacje mają zostać udostępnione;
3) wskazanie informacji, których wniosek dotyczy;
4) wskazanie wnioskodawcy;
5) wskazanie podstawy prawnej udostępnienia informacji;
6) oznaczenie formy przekazania lub udostępnienia informacji;

7) imię, nazwisko, stopień służbowy lub zajmowane stanowisko osoby uprawnionej.

3. W przypadkach niecierpiących zwłoki, a w szczególności podczas wykonywania czynności mających na celu realizację zadań, o których mowa w art. 3 pkt 2 i 3 ustawy, funkcjonariusz, o ile przepisy odrębne nie wykluczają takiej możliwości, może uzyskiwać informacje, w tym dane osobowe, ze zbiorów danych, o których mowa w ust. 1, na podstawie ustnego wniosku, podając informacje, o których mowa w ust. 2.

4. Uzyskanie informacji, w tym danych osobowych, w formie ustnej potwierdza się po ustaniu okoliczności, o których mowa w ust. 3, w pisemnym wniosku zawierającym informacje, o których mowa w ust. 2, skierowanym do organu władzy publicznej lub podmiotu, od którego uzyskano informacje.

5. Przepisów ust. 1–4 nie stosuje się do informacji, w tym danych osobowych, zawartych w zbiorach danych udostępnionych Służbie Ochrony Państwa w drodze teletransmisji danych zgodnie z art. 41 ust. 4 ustawy.

6. W przypadku gdy osoba uprawniona pobrała dokumenty zawierające informacje, w tym dane osobowe, albo uzyskała wgląd w ich treść, na podstawie wniosku, o którym mowa w ust. 1, potwierdza na piśmie pobranie tych dokumentów albo uzyskanie wglądu w ich treść.

§ 15. 1. Udokumentowaniem zgromadzenia informacji, w tym danych osobowych, oraz potwierdzeniem ich zarejestrowania w zbiorze danych lub potwierdzeniem wykonania innej operacji ich przetwarzania w systemie teleinformatycznym jest wydruk lub raport zawierający zestawienie zakresu, treści lub graficznej formy przetwarzanych informacji, formularz rejestracyjny z identyfikatorem określonego zbioru danych lub inna forma zapisu przetwarzanych informacji w postaci papierowej, w tym odwzorowanej cyfrowo, lub elektronicznej.

2. Operacja przetwarzania informacji, w tym danych osobowych, w systemie teleinformatycznym, której wykonywanie jest niezbędne dla realizacji czynności służbowych lub stanowi integralną część tych czynności, może być dokumentowana lub potwierdzona przez wykonanie i udokumentowanie tej czynności w formie i w sposób właściwy dla zrealizowanej czynności służbowej.

§ 16. Stosuje się następujące sposoby przetwarzania informacji, w tym danych osobowych, zawartych w zbiorach danych:

1) rejestrowanie – polegające na wprowadzaniu informacji, w tym danych osobowych, po raz pierwszy do zbioru danych;

2) sprawdzanie – polegające na zapoznaniu się z informacjami, w tym danymi osobowymi, znajdującymi się w zbiorach danych;
3) klasyfikowanie – polegające na porządkowaniu zawartości zbiorów danych według określonych kryteriów;
4) weryfikowanie – polegające na sprawdzaniu poprawności, kompletności i prawidłowości zarejestrowanych informacji, w tym danych osobowych, lub na dokonywaniu oceny przydatności lub niezbędności tych informacji do dalszego ich przetwarzania;
5) modyfikowanie – polegające na zmianie zawartości informacji, w tym danych osobowych, znajdujących się w zbiorze danych, w tym zmianie zarejestrowanych informacji lub ich uzupełnieniu;
6) typowanie – polegające na wyszukaniu i identyfikacji w zbiorach danych informacji, w tym danych osobowych, o cechach odpowiadających określonym kryteriom selekcyjnym;
7) analizowanie – polegające na poszukiwaniu związków zachodzących między poszczególnymi informacjami, w tym danymi osobowymi, znajdującymi się w zbiorze danych;
8) przekazywanie – polegające na udostępnieniu informacji, w tym danych osobowych, ze zbioru danych innemu uprawnionemu podmiotowi, bez względu na formę tej czynności;
9) usuwanie – polegające na zniszczeniu lub deformacji informacji, w tym danych osobowych, w sposób uniemożliwiający dalsze ich odczytywanie;
10) wykorzystywanie.

§ 17. Administrator zbioru danych zapewnia rejestrację, w formie odpowiedniej do właściwości danego zbioru danych, każdej operacji przetwarzania informacji, w tym danych osobowych, w zakresie:

1) daty, godziny i minuty rozpoczęcia i zakończenia pracy w systemie teleinformatycznym lub w ręcznie sporządzanej ewidencji;
2) identyfikatora kadrowego, niezbędnych danych identyfikacyjnych oraz uprawnienia dostępu do zbioru danych posiadanego przez funkcjonariusza lub pracownika Służby Ochrony Państwa, wykonującego operację przetwarzania;
3) informacji, w tym danych osobowych, do których funkcjonariusz lub pracownik Służby Ochrony Państwa miał dostęp w związku z wykonywaną operacją ich przetwarzania;
4) daty pierwszego wprowadzenia informacji, w tym danych osobowych, do zbioru danych;

5) źródła informacji, w przypadku uzyskania danych osobowych od innej osoby niż ta, której dane dotyczą;
6) przyczyny, zakresu i celu modyfikacji informacji, w tym danych osobowych, która nastąpiła w wyniku wykonanej operacji ich przetwarzania;
7) danych identyfikujących osobę zlecającą wykonanie operacji przetwarzania informacji, w tym danych osobowych;
8) wskazania celu lub powodu wykonania operacji przetwarzania informacji, w tym danych osobowych;
9) wniosków składanych w związku z realizacją praw określonych w art. 32 ust. 1 pkt 6 i art. 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§ 18. 1. Operacje przetwarzania informacji, w tym danych osobowych, mogą być wykonywane również na zlecenie osób uprawnionych, niemających bezpośredniego dostępu do systemu teleinformatycznego, w którym jest prowadzony dany zbiór danych. Do zlecającego stosuje się odpowiednio przepisy § 12 i § 13.

2. Do przetwarzania, o którym mowa w ust. 1, stosuje się formularze rejestracyjne.

3. Za prawidłowe i poprawne wykonanie operacji przetwarzania informacji, w tym danych osobowych, odpowiadają osoby uprawnione, bezpośrednio przetwarzające informacje w zbiorze danych, a za prawidłowe i poprawne wypełnienie formularza rejestracyjnego – zlecający wykonanie operacji przetwarzania informacji.

4. Komendant może wyznaczyć komórki organizacyjne właściwe w sprawach wykonywania operacji przetwarzania informacji, w tym danych osobowych, w zbiorach danych.

§ 19. 1. Informacjom, w tym danym osobowym, wprowadzanym po raz pierwszy do systemu teleinformatycznego, w którym jest prowadzony określony zbiór danych, nadaje się indywidualny identyfikator tego zbioru.

2. W przypadku gdy ta sama informacja, w tym dane osobowe, podlega rejestracji w więcej niż jednym zbiorze danych lub w kilku odrębnych kategoriach informacji wydzielonych w jednym zbiorze, przy każdej rejestracji tej informacji nadaje się odrębny identyfikator danego zbioru lub kategorii oraz wskazuje się jej powiązanie z rejestracjami dokonanymi w pozostałych zbiorach danych lub kategoriach.

§ 20. Informacje, w tym dane osobowe przetwarza się w sposób, o którym mowa w § 16, a także przy użyciu wprowadzonych przez administratora zbioru danych formularzy rejestracyjnych, jeżeli wymagają tego właściwości zbioru danych.

§ 21. Gromadzone przez Służbę Ochrony Państwa informacje w formie zdjęć osób, w tym zdjęć sygnalitycznych, można wykorzystywać do tworzenia albumów fotograficznych okazywanych w celach identyfikacyjnych, wykrywczych lub zapobiegawczych.

§ 22. 1. W odniesieniu do informacji, w tym danych osobowych, gromadzonych w zbiorach danych i przetwarzanych w systemach teleinformatycznych, w celu zabezpieczenia informacji przed nieuprawnionym dostępem oraz zapewnienia zgodności trybu gromadzenia informacji z celem ich przetwarzania, administrator bezpieczeństwa informacji, o którym mowa w art. 60 ustawy, administrator zbiorów danych lub osoba przez niego upoważniona może kontrolować i nadzorować:

1) dostęp do zbiorów danych prowadzonych w Służby Ochrony Państwa oraz do informacji, w tym danych osobowych, w nich przetwarzanych;
2) dostęp do informacji, w tym danych osobowych, przetwarzanych w zbiorach danych udostępnianych Służbie Ochrony Państwa w drodze teletransmisji danych na podstawie art. 41 ust. 4 ustawy;
3) przetwarzanie informacji, w tym danych osobowych, w zbiorach danych, o których mowa w pkt 1 i 2;
4) uprawnienia do przetwarzania informacji, w tym danych osobowych, w zbiorach danych, o których mowa w pkt 1 i 2.

2. Czynności, o których mowa w ust. 1, realizuje się w szczególności przez:

1) weryfikację, typowanie i analizę informacji, w tym danych osobowych, przetwarzanych w zbiorach danych;
2) sprawdzanie zakresu dostępu do zbiorów danych, zakresu i rodzaju operacji przetwarzania wykonanych na informacjach, w tym danych osobowych, oraz ocenę, analizę lub weryfikację wyników tego sprawdzenia;
3) kontrolę rejestrów czynności (logowań) odnotowywanych w systemie teleinformatycznym;
4) kontrolę i ocenę legalności, poprawności, kompletności i celowości przetwarzania informacji, w tym danych osobowych, a także przeprowadzenie analizy w tym zakresie;

5) sprawdzanie dokumentacji stanowiącej podstawę do wprowadzenia informacji, w tym danych osobowych, do zbioru danych, a także stanowiącej podstawę ich sprawdzenia, wykorzystania, modyfikacji lub usunięcia, jeżeli czynności tych dokonywano w oparciu o dokumenty;
6) usuwanie informacji, w tym danych osobowych, wobec których stwierdzono brak przesłanek ich przetwarzania przez Służbę Ochrony Państwa.

3. Administrator bezpieczeństwa informacji, administrator zbiorów danych lub osoba przez niego upoważniona może wydawać polecenia, zalecenia lub wytyczne w celu usunięcia stwierdzonych uchybień w przetwarzaniu informacji, w tym danych osobowych, a w przypadku naruszenia przepisów prawa – skierować sprawę do właściwego przełożonego dyscyplinarnego.

Rozdział 4

Sposób oceny danych pod kątem ich przydatności, przesłanki zaniechania zbierania określonych rodzajów informacji oraz sposoby usuwania danych

§ 23. Oceniając dane zgromadzone pod kątem ich przydatności uwzględnia się w szczególności:

1) znaczenie informacji dla realizacji zadania polegającego na ochronie osób i obiektów określonych w art. 3 pkt 1 ustawy;
2) znaczenie informacji dla oceny, czy osoba, której informacja dotyczy:
   a) zmierza do dokonania lub popełniła w przeszłości przestępstwa, o którym mowa w art. 3 pkt 2–3 ustawy,
   b) czyni przygotowania do popełnienia przestępstwa, o którym mowa w art. 3 pkt 2–3 ustawy,
   c) podżega lub udziela pomocy w popełnieniu przestępstwa, o którym mowa w art. 3 pkt 2 – 3 ustawy,
2) znaczenie informacji dla rozpoznawania przestępstw, o których mowa w art. 3 pkt 2–3 ustawy;
3) inne zgromadzone lub dostępne informacje o osobie, której informacja dotyczy lub innych osobach;
4) ustanie okoliczności albo ziszczenie się celu uzasadniającego wprowadzenie danych do zbioru danych.

§ 24. 1. Oceny, o której mowa w § 23, dokonuje się z wykorzystaniem informacji, w tym danych osobowych:

1) zgromadzonych w zbiorach danych prowadzonych w Służbie Ochrony Państwa, powiązanych z danymi wytypowanymi do oceny;
2) zawartych we wnioskach osób, których dane dotyczą, złożonych w trybie art. 32 ust. 1 pkt 1 – 6 i art. 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
3) uzyskanych od innych organów, służb lub instytucji państwowych.

2. Przy ocenie danych, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904 i 1948), administrator danych lub osoba przez niego upoważniona może zwrócić się do organów, które przekazały dane osób, o aktualizację tych danych.

§ 25. 1. W celu realizacji ustawowych zadań, Służba Ochrony Państwa nie gromadzi informacji, o których mowa w art. 56 ust. 7 ustawy.

2. Gromadzeniu nie podlegają informacje, które znajdują się w powszechnie udostępnianych publicznych rejestrach, prowadzonych przez instytucje krajowe.

§ 26. 1. Administrator danych lub osoba przez niego upoważniona wyznacza komisję do usunięcia ze zbioru danych uznanych za nieprzydatne lub zbędne w wyniku oceny, o której mowa w § 24. Komisja sporządza protokół usunięcia danych ze zbioru danych.

2. Wzór protokołu usunięcia danych osobowych ze zbioru danych jest określony w załączniku nr 2 do rozporządzenia.

§ 27. Dane pobrane, uzyskane lub zgromadzone od organów innych państw ocenia się i usuwa w sposób określony przez organ przekazujący te dane, a w przypadku gdy nie został on określony – w sposób wskazany w § 23–24 i § 26.

§ 28. Dane osobowe znajdujące się w systemach teleinformatycznych lub na informatycznych nośnikach danych usuwa się w sposób uniemożliwiający odtworzenie usuniętych danych:

1) przy użyciu technik programowych;
2) przez zniszczenie nośników zawierających dane osobowe przeznaczone do usunięcia, jeżeli ich usunięcie w sposób określony w pkt 1 nie jest możliwe.

Rozdział 5

Przepis końcowy

§ 29. Rozporządzenie wchodzi w życie z dniem 1 lutego 2018 r.

MINISTER SPRAW
WEWNĘTRZNYCH
I ADMINISTRACJI

Za zgodność
pod względem prawnym,
redakcyjnym i redakcyjnym

ZASTĘPCA DYREKTORA
Departamentu Prawnego MSWiA
Radosław BALCER

Załączniki do rozporządzenia
Ministra Spraw Wewnętrznych i
Administracji z dnia … (poz. …)

Załącznik nr 1

WZÓR PROTOKOŁU LIKWIDACJI ZBIORU DANYCH ALBO ZESTAWU ZBIORÓW DANYCH

Protokół likwidacji zbioru danych/zestawu zbiorów danych*)

....
(numer ewidencyjny) (miejsce i data sporządzenia)

Komisja likwidacyjna w składzie:

1. .....

2. .....

3. .....

(dane członków komisji likwidacyjnej; w przypadku funkcjonariusz – stopień, imię i nazwisko oraz stanowisko służbowe; w przypadku pracownika – imię i nazwisko oraz stanowisko służbowe)

działająca na podstawie decyzji nr .....
(oznaczenie decyzji Komendanta Służby Ochrony Państwa w sprawie likwidacji zbioru danych/zestawu zbiorów danych*))

w dniu ..... r. przeprowadziła likwidację zbioru danych/zestawu zbiorów danych*) .....
(rodzaj i nazwa likwidowanego zbioru danych/zestawu zbiorów danych*))

.....

przez .....
(opis sposobu likwidacji zbioru danych/zestawu zbiorów danych*)

.....

1. .....

2. .....

3. .....
(podpisy członków komisji likwidacyjnej)

*) - niepotrzebne skreślić.

Uwaga do wzoru:

Dopuszcza się sporządzenie protokołu przy zastosowaniu procesora tekstu z zachowaniem zawartości protokołu, przy czym można pominąć te elementy, które służą jedynie wskazaniu miejsca i sposobu wypełnienia protokołu, oraz te, które podlegają skreśleniu jako niepotrzebne.

Załącznik nr 2

WZÓR PROTOKOŁU USUNIĘCIA DANYCH OSOBOWYCH ZE ZBIORU DANYCH

Protokół usunięcia danych osobowych ze zbioru danych

....

(numer ewidencyjny) (miejsce i data sporządzenia)

Komisja w składzie:

1. .....

2. .....

3. .....

(dane członków komisji likwidacyjnej; w przypadku funkcjonariusz – stopień, imię i nazwisko oraz stanowisko służbowe; w przypadku pracownika – imię i nazwisko oraz stanowisko służbowe)

wyznaczona przez .....w dniu ..... r.

(nazwa administratora danych lub osoby przez niego upoważnionej)

na podstawie .....

(podstawa prawna usunięcia danych)

usunęła ze zbioru danych .....

(nazwa zbioru danych)

dane osobowe .....

.....

.....

.....

(opis usuniętych danych osobowych)

przez .....

.....

(wykaz zniszczonych dokumentów lub nośników informatycznych zawierających dane osobowe oraz sposób zniszczenia tych danych)

1. .....

2. .....

3. .....

(podpisy członków komisji likwidacyjnej)

Uwaga do wzoru:

Dopuszcza się sporządzenie protokołu przy zastosowaniu procesora tekstu z zachowaniem zawartości protokołu, przy czym można pominąć te elementy, które służą jedynie wskazaniu miejsca i sposobu wypełnienia protokołu.

UZASADNIENIE

Przedłożony projekt rozporządzenia stanowi wykonanie upoważnienia zawartego w art. 56 ust. 13 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz 138) zwanej dalej „ustawą".

Przywołany akt normatywny określa szczegółowy tryb gromadzenia, sposoby przetwarzania informacji, w tym danych osobowych, o których mowa w art. 56 ust. 2–5 ustawy, w zbiorach danych, wzory dokumentów obowiązujących przy przetwarzaniu danych oraz sposób oceny danych pod kątem ich przydatności w prowadzonych postępowaniach, uwzględniając potrzebę ochrony danych przed nieuprawnionym dostępem i przesłanki zaniechania zbierania określonych rodzajów informacji, a w przypadku informacji, o których mowa w art. 56 ust. 3 ustawy, uwzględniając konieczność dostosowania się do wymogów określonych przez organy innych państw – od których uzyskiwane są dane.

W pierwszej kolejności w projekcie określono, że administratorem informacji, w tym danych osobowych, oraz zbiorów danych, w których są przetwarzane te informacje jest Komendant Służby Ochrony Państwa. W odniesieniu do danych osobowych uzyskanych od organów władzy publicznej i organów innych państw, a następnie przetwarzanych przez Służbę Ochrony Państwa, Komendant posiada uprawnienia i wykonuje zadania administratora danych określone w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

W rozdziale drugim projekt wyszczególnia sposoby prowadzenia zbiorów danych, tworzenia zestawów zbiorów, w tym podmioty uprawnione do ich tworzenia, formy i zakres prowadzenia zbiorów, możliwości tworzenia replik. Określono, kto prowadzi i co zawiera rejestr zbiorów danych. Ponadto wskazano podstawę i sposób oraz określono dokumentację związaną z likwidacją zbiorów lub zestawów zbiorów.

W rozdziale trzecim określono podstawy wprowadzania informacji, w tym danych osobowych, do zbiorów danych, sposoby ich przetwarzania oraz kontrolę dostępu do zbiorów danych i nadzór nad ich przetwarzaniem.

W rozdziale czwartym wyszczególniono sposób oceny danych pod kątem ich przydatności dla zadań formacji określonych w art. 3 ustawy. Wskazano przy tym, iż oceny tej należy dokonywać także z uwzględnieniem znaczenia danej informacji w zestawieniu z innymi dostępnymi danymi. W dalszej kolejności uregulowano tryb i sposób usuwania nieprzydatnych danych oraz wskazano przesłanki zaniechania zbierania określonych rodzajów informacji.

Do problematyki uregulowanej w projekcie rozporządzenia odnoszą się przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz

uchylająca decyzję ramową Rady 2008/977/WSISW. Państwa członkowskie są zobowiązane do przyjęcia i publikacji przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania do wykonania ww. dyrektywy – do dnia 6 maja 2018 r.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projekt rozporządzenia nie wymaga notyfikacji, ponieważ nie zawiera przepisów technicznych, o których mowa w § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2007 r. poz. 248) w związku 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.), projekt rozporządzenia z chwilą przekazania go do uzgodnień z członkami Rady Ministrów został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacji.

Projekt został przekazany, zgodnie z § 32 ust. 2 uchwały nr 190 z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2016 r. poz. 1006 i 1204), do koordynatora oceny skutków regulacji w Kancelarii Prezesa Rady Ministrów z prośbą o zaopiniowanie w tym zakresie.

Nazwa projektu Projekt rozporządzenia w sprawie przetwarzania informacji przez Służbę Ochrony Państwa **Ministerstwo wiodące i Ministerstwa współpracujące:** Minister Spraw Wewnętrznych i Administracji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Jarosław Zieliński Sekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji **Kontakt do opiekuna merytorycznego projektu** Pan Mariusz Cichomski, Zastępca Dyrektora Departamentu Porządku Publicznego MSWiA tel. 22 601 40 70 e-mail dpp.koordynacja@mswia.gov.pl	**Data sporządzenia** 18.01.2018 r. **Źródło:** art. 56 ust. 13 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz. U. z 2018 r. poz. 138) **Nr w wykazie prac** 279

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Proponowany projekt stanowi realizację delegacji z art. 56 ust. 13 ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa i określa wymogi odnoszące się do uzyskiwania informacji, w tym także niejawnie, gromadzenia ich, sprawdzania oraz przetwarzania.

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

Rozporządzenie określa tryb gromadzenia oraz sposoby przetwarzania w zbiorach danych informacji, w tym danych osobowych, w ramach realizacji zadań tej służby.

Oczekiwanym efektem regulacji jest określenie zasad przetwarzania danych osobowych, tak aby następowało ono w zgodności zarówno z ustawą o ochronie danych, jak i z przepisami szczególnymi, tj. art. 56 ust. 1-13 ustawy o Służbie Ochrony Państwa. Jednocześnie celem regulacji jest zapewnienie Służbie Ochrony Państwa możliwości przewarzania danych osobowych w zakresie umożliwiającym realizację ustawowych zadań tej formacji.

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

Do problematyki uregulowanej w projekcie rozporządzenia odnoszą się przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSISW. W polskim porządku prawnym implementacja ww. dyrektywy będzie polegała w szczególności na uchwaleniu ustawy o przetwarzaniu danych osobowych w związku z zapobieganiem i zwalczeniem przestępczości. Ponieważ prace nad ww. ustawą są na początkowym etapie, a ponadto równolegle trwają zaawansowane prace legislacyjne nad nową ustawą o ochronie danych osobowych, kształt ostatecznych rozwiązań w tym zakresie nie jest jeszcze znany. Państwa członkowskie są zobowiązane do przyjęcia i publikacji przepisów ustawowych, wykonawczych i administracyjnych niezbędnych do wykonania do wykonania ww. dyrektywy – do dnia 6 maja 2018 r.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Funkcjonariusze Służby Ochrony Państwa	3000	dane dotyczące zakładanej w procesie legislacji liczby	Obowiązek stosowania szczegółowo uregulowanych zasad

		funkcjonariuszy Służby Ochrony Państwa	przetwarzania informacji przez Służbę Ochrony Państwa.
Osoby fizyczne, których dane Służba Ochrony Państwa może przetwarzać.	Nie do oszacowania		Dodatkowa ochrona praw osób fizycznych, których dane będą przetwarzane przez Służbę Ochrony Państwa

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

Projekt rozporządzenia został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Spraw Wewnętrznych i Administracji, stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz 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 i 1204) projekt został udostępniony w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji. Projektowana regulacja nie spowoduje skutków dla budżetów jednostek samorządu terytorialnego, tym samym projekt nie wymaga konsultacji z Komisją Wspólną Rządu i Samorządu Terytorialnego.

6. Wpływ na sektor finansów publicznych

Wejście w życie projektowanego rozporządzenia nie spowoduje skutków finansowych w rozumieniu art. 50 ustawy z dnia 27 sierpnia 2009 r. o finansach 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	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa	-	-	-	-	-	-	-	-	-	-	-	-
JST	-	-	-	-	-	-	-	-	-	-	-	-
pozostałe jednostki (oddzielnie)	-	-	-	-	-	-	-	-	-	-	-	-

Źródła finansowania	Budżet Państwa w części 42 - Sprawy wewnętrzne" w zakresie budżetu Służby Ochrony Państwa
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowana regulacja nie będzie miała wpływu na sektor finansów publicznych, w tym budżet państwa oraz budżety jednostek samorządu terytorialnego. Wydatki tego sektora będą bowiem spowodowane nie tyle przyjęciem rozporządzenia, co wejściem w życie ustawy z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa.

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	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa	-						
	sektor mikro-, małych i średnich przedsiębiorstw	-						
	rodzina, obywatele oraz gospodarstwa domowe	-						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Nie przewiduje się wpływu projektowanej regulacji na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

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

X nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	tak nie X 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 X nie dotyczy

Nie przewiduje się wpływu projektowanego rozporządzenia na ww. obszary.

9. Wpływ na rynek pracy

Nie przewiduje się wpływu projektowanej ustawy na rynek pracy.

10. Wpływ na pozostałe obszary

środowisko naturalne sytuacja i rozwój regionalny inne:	demografia mienie państwowe	informatyzacja zdrowie

Omówienie wpływu	Nie przewiduje się wpływu projektowanej regulacji na ww. obszary.

11. Planowane wykonanie przepisów aktu prawnego

Wejście w życie rozporządzenia planowane jest na dzień 1 lutego 2018 r.

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

Z uwagi na zakres przedmiotowy projektu, ewaluacja efektów projektu jest niezasadna.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak.