

Warszawa, dnia 4 czerwca 2018 r.

Poz. 1069

**ROZPORZĄDZENIE
MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI¹⁾**

z dnia 18 maja 2018 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, 650 i 730) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

- 1) tryb gromadzenia i sposoby przetwarzania w zbiorach danych informacji, danych osobowych, w tym danych osobowych uzyskanych lub przetwarzanych przez organy innych państw lub organizacje międzynarodowe, służących rozpoznawaniu, zapobieganiu lub wykrywaniu przestępstw;
- 2) sposób oceny danych pod kątem ich przydatności do realizacji zadań Służby Ochrony Państwa;
- 3) wzór protokołu usunięcia danych osobowych ze zbioru danych.

§ 2. Użyte w rozporządzeniu określenia 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.

§ 3. 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.

§ 4. Zbiory danych tworzy w drodze decyzji Komendant, który ustala ich zakres informacyjny i rzeczowy, odpowiada za ich wewnętrzną strukturę i przeznaczenie, a także dostosowuje procedury przetwarzania w nich informacji, w tym danych osobowych, do rodzaju zadań wykonywanych przez Służbę Ochrony Państwa.

§ 5. 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.

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 i 225).

3. W przypadku dokonania oceny, że informacje, w tym dane osobowe, są nieprzydatne lub nieadekwatne do realizacji celów określonych w art. 3 ustawy albo że ich gromadzenie byłoby nadmierne z punktu widzenia realizacji tych celów, funkcjonariusze lub pracownicy Służby Ochrony Państwa odpuszczają od wprowadzenia do zbioru takich informacji.

§ 6. 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 zbiorze danych, a także z przepisami dotyczącymi ochrony informacji, w tym danych osobowych, w nim zgromadzonych.

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

2. Dla każdego użytkownika systemu teleinformatycznego, po zweryfikowaniu jego uprawnień do dostępu do danego systemu, ustala się odrębny identyfikator i hasło użytkownika.

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

§ 8. Operacje 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) niezbędnych danych identyfikacyjnych oraz uprawnień dostępu do zbioru danych posiadanego przez funkcjonariusza lub pracownika Służby Ochrony Państwa, wykonującego operację przetwarzania,
- 3) daty pierwszego wprowadzenia informacji, w tym danych osobowych, do zbioru danych,
- 4) źródła informacji, w przypadku uzyskania danych osobowych od innej osoby niż ta, której dane dotyczą,
- 5) przyczyny, zakresu i celu modyfikacji informacji, w tym danych osobowych, która nastąpiła w wyniku wykonanej operacji ich przetwarzania,
- 6) danych identyfikujących osobę zlecającą wykonanie operacji przetwarzania informacji, w tym danych osobowych,
- 7) wskazania celu lub powodu wykonania operacji przetwarzania informacji, w tym danych osobowych,
- 8) 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 (Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723)

– podlegają rejestracji w formie odpowiedniej do właściwości danego zbioru danych.

§ 9. 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.

§ 10. Informacje, w tym dane osobowe, przetwarza się przy użyciu wprowadzonych przez administratora danych formularzy rejestracyjnych, jeżeli wymagają tego właściwości zbioru danych.

§ 11. 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 popełnienia lub popełniła w przeszłości przestępstwa, o których mowa w art. 3 pkt 2 lub 3 ustawy,
 - b) czyni przygotowania do popełnienia przestępstw, o których mowa w art. 3 pkt 2 lub 3 ustawy,
 - c) podlega lub udziela pomocy w popełnieniu przestępstw, o których mowa w art. 3 pkt 2 lub 3 ustawy,
- 3) znaczenie informacji dla rozpoznawania przestępstw, o których mowa w art. 3 pkt 2 lub 3 ustawy;

- 4) inne zgromadzone lub dostępne informacje o osobie, której informacja dotyczy, lub innych osobach;
- 5) ustanie okoliczności albo ziszczenie się celu uzasadniającego wprowadzenie danych do zbioru danych.

§ 12. 1. Oceny, o której mowa w § 11, 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. z 2018 r. poz. 452, 650 i 730), Komendant lub osoba przez niego upoważniona może zwrócić się do organów, które przekazały dane osób, o aktualizację tych danych.

§ 13. 1. Komendant lub osoba przez niego upoważniona wyznacza komisję do usunięcia ze zbioru danych uznanych za nieprzydatne lub zbędne w wyniku oceny, o której mowa w § 12. Komisja sporządza protokół usunięcia danych ze zbioru danych.

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

§ 14. 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 § 11–13.

§ 15. Dane osobowe znajdujące się w systemach teleinformatycznych lub na informatycznych nośnikach danych usuwa się:

- 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

– w sposób uniemożliwiający odtworzenie usuniętych danych.

§ 16. Rozporządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

Minister Spraw Wewnętrznych i Administracji: *wz. K. Kozłowski*

Załącznik do rozporządzenia Ministra Spraw Wewnętrznych
i Administracji z dnia 18 maja 2018 r. (poz. 1069)

WZÓR

PROTOKÓŁ USUNIĘCIA DANYCH OSOBOWYCH ZE ZBIORU DANYCH

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

Komisja w składzie:

1.
2.
3.
(dane członków komisji; w przypadku funkcjonariusza Służby Ochrony Państwa – stopień, imię i nazwisko oraz stanowisko służbowe;
w przypadku pracownika Służby Ochrony Państwa – imię i nazwisko oraz stanowisko służbowe)

wyznaczona przez w dniu r.
(wskazanie 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)

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.