

Załącznik nr 1 do Uchwały nr ZF-2/III/2019 z dnia 23.05.2019r.



FEDERACJA STOWARZYSZEŃ SŁUŻB MUNDUROWYCH  
RZECZYPOSPOLITEJ POLSKIEJ

**POLITYKA OCHRONY DANYCH OSOBOWYCH  
w FEDERACJI STOWARZYSZEŃ SŁUŻB MUNDUROWYCH RP**

Podstawa:

Art. 24 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

## I. Postanowienia ogólne

Polityka ochrony danych jest dokumentem mającym na celu określenie podstawowych reguł dotyczących zasad przetwarzania danych osobowych oraz środków bezpieczeństwa stosowanych przez Administratora danych osobowych.

Polityka ochrony danych została opracowana na podstawie europejskich i krajowych przepisów dotyczących ochrony danych osobowych, w szczególności:

- 1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako RODO);
- 2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako Ustawa).

Administrator danych osobowych, realizując Politykę ochrony danych, zobowiązuje się do dołożenia szczególnej staranności w zakresie ochrony przetwarzanych przez niego danych osobowych zapewniając w szczególności, aby:

- 1) dane osobowe przetwarzane były zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- 2) dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- 3) zbierane dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
- 4) dane osobowe były prawidłowe i w razie potrzeby uaktualniane;
- 5) dane osobowe były przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
- 6) dane osobowe były przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Zasady określone w Polityce ochrony danych stosowane są do:

- 1) wszystkich danych osobowych przetwarzanych przez Administratora danych osobowych,

- 2) wszystkich miejsc (lokali, pomieszczeń), w których są przetwarzane dane osobowe,
- 3) wszystkich osób upoważnionych przez Administratora do przetwarzania danych osobowych,
- 4) wszelkiej dokumentacji zawierającej dane osobowe oraz wszystkich nośników danych, na których znajdują się dane osobowe,
- 5) wszystkich systemów informatycznych, za pomocą których przetwarzane są dane osobowe.

Przetwarzanie danych osobowych przez Administratora danych osobowych następuje jedynie po spełnieniu jednej z przesłanek wymienionych w art. 6 ust. 1 RODO, tj.:

- a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze danych osobowych;
- d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi danych osobowych;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora danych osobowych lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Przetwarzanie szczególnych kategorii danych osobowych (tj. danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących stanu zdrowia, seksualności lub orientacji seksualnej tej osoby) jest możliwe tylko w przypadkach wskazanych w art. 9 ust. 2 RODO.

Za wdrożenie i monitorowanie stosowania Polityki ochrony danych odpowiedzialny jest Administrator danych osobowych, a w ramach struktury wewnętrznej Administratora danych

osobowych, Prezydent Federacji lub osoba, której powierzono nadzór nad obszarem ochrony danych osobowych oraz zapewnienia zgodności z ochroną danych osobowych.

Do stosowania zasad wynikających z Polityki ochrony danych zobowiązani są wszyscy pracownicy i współpracownicy Administratora danych osobowych, którzy przetwarzają dane osobowe w jego imieniu.

## II. Stosowane pojęcia.

Na potrzeby Polityki ochrony danych przyjmuje się następujące definicje:

- 1) **polityka ochrony danych (dokument)** – polityka bezpieczeństwa w zakresie ochrony danych osobowych w Federacji Stowarzyszeń Służb Mundurowych RP,
- 2) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
- 3) **osoba możliwa do zidentyfikowania** - to osoba fizyczna, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
- 4) **szczególne kategorie danych osobowych (tzw. „dane wrażliwe”)** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
- 5) **zbiór danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
- 6) **administrator danych osobowych lub ADO** – osoba fizyczną lub prawną, organ publiczny, jednostka lub inny podmiot, który ustala cele i sposoby przetwarzania danych osobowych, w tym przypadku:

**Federacja Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie,**  
ul. Krochmalna 32 lok. 35, 00-864 Warszawa, zarejestrowana przez Sąd Rejonowy w Warszawie XII Wydział Gospodarczy KRS pod numerem: 0000342738, NIP: 1132826105, REGON: 14228871, kierowana przez Zarząd Federacji i reprezentowana przez Prezydenta Federacji,

- 7) **Prezydent Federacji** – osoba funkcyjna wybierana ze swego grona przez Zarząd Federacji,
- 8) **osoba upoważniona** – członek zarządu oraz inna osoba upoważniona przez Administratora danych osobowych (lub osobę przez niego upoważnioną) do przetwarzania danych osobowych na jego polecenie w zakresie wynikającym z upoważnienia,
- 9) **przetwarzanie danych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
- 10) **system informatyczny** – komputery stacjonarne lub przenośne, a także zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- 11) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- 12) **naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
- 13) **usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- 14) **zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
- 15) **podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
- 16) **odbiorca danych** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, (organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi

zastosowanie stosownie do celów przetwarzania), a więc każdy, komu udostępnia się dane osobowe, z wyłączeniem:

- a) osoby, której dane dotyczą,
- b) osoby upoważnionej do przetwarzania danych,
- c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

- 17) ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. Nr 1000 z późn. zm.),
- 18) nośnik danych** – wszelkie nośniki, na których zapisywane są w postaci elektronicznej, w tym w szczególności dyski twarde, płyty CD lub DVD, karty magnetyczne, pamięci przenośne,
- 19) rozliczalność** - zdolność jednoznacznego zidentyfikowania osoby, która jest odpowiedzialna za określone działania, a także możliwość wykazania, iż przetwarzanie danych osobowych odbywa się zgodnie ze wszystkimi zasadami wynikającymi z obowiązujących przepisów prawa z zakresu ochrony danych osobowych,
- 20) poufność** - zapewnienie dostępu do danych osobowych tylko osobom upoważnionym,
- 21) Integralność** - właściwość zapewniająca, że dane osobowe nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.

### **III. Podstawowe obowiązki Administratora Danych Osobowych (ADO).**

Administrator danych osobowych wypełnia obowiązki z zakresu ochrony danych osobowych, w szczególności:

- 1) spełnia obowiązek informacyjny wobec osób, których dane osobowe są przetwarzane przez Administratora danych osobowych;
- 2) zachowuje staranność przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane osobowe są przetwarzane;
- 3) stosuje środki techniczne i organizacyjne zapewniające odpowiednią ochronę przetwarzanych danych osobowych;
- 4) respektuje prawa osób, których dane osobowe dotyczą w zakresie żądania uzupełnienia, uaktualnienia, sprostowania, przeniesienia danych osobowych oraz zaprzestania ich przetwarzania;
- 5) spełnia obowiązek udzielenia informacji o zakresie przetwarzanych danych osobowych;
- 6) prowadzi dokumentację związaną z bezpieczeństwem przetwarzanych danych osobowych, w szczególności politykę ochrony danych osobowych;

- 7) zgłasza naruszenia ochrony danych osobowych w przypadkach przewidzianych przepisami prawa;
- 8) weryfikuje, czy ma miejsce przekazanie danych do państw trzecich lub organizacji międzynarodowych oraz, jeżeli ma ono miejsce, zapewnia zgodność z prawem takiego przekazywania;
- 9) przetwarza dane jedynie w oparciu o podstawy prawne przewidziane w przepisach prawa oraz posiada wiedzę na temat podstaw prawnych, na jakich dokonywane są konkretne czynności przetwarzania danych osobowych, a jeżeli podstawą przetwarzania określonych danych jest uzasadniony interes Administratora ochrony danych, wiedzę na temat konkretnego realizowanego przetwarzaniem prawnie uzasadnionego interesu.

#### **IV. Sposoby przetwarzania danych osobowych.**

1. Administrator danych osobowych przetwarza dane osobowe w siedzibie Federacji Stowarzyszeń Służb Mundurowych RP, w formie papierowej oraz sporadycznie elektronicznej, przy użyciu edytora tekstu (MS Word), arkusza kalkulacyjnego (MS Excel) lub innych dostępnych programów do tworzenia baz danych.
2. Przetwarzanie danych osobowych w formie papierowej i systemach informatycznych następuje przy zachowaniu zasad ochrony tych danych osobowych obowiązujących u Administratora danych osobowych opisanych w dalszej części Polityki ochrony danych.
3. Administrator danych osobowych lub osoba przez niego wyznaczona prowadzi wykaz systemów informatycznych, w których przetwarzane są dane osobowe według wzoru stanowiącego **załącznik nr 1**.

#### **V. Zasady dostępu do danych osobowych.**

##### **1. Upoważnienia do przetwarzania danych osobowych:**

- 1) Przetwarzanie danych osobowych możliwe jest wyłącznie przez osoby upoważnione do ich przetwarzania, tj. członków funkcyjnych Zarządu Federacji, którymi są:
  - Prezydent Federacji,
  - Wiceprezydenci Federacji,
  - Sekretarz Generalny Federacji,

- Skarbnik Federacji,  
oraz inne osoby na podstawie specjalnego upoważnienia określającego osobę upoważnioną oraz zakres i termin upoważnienia, wydawanego według wzoru stanowiącego **załącznik nr 2**;
- 2) Specjalne upoważnienia, o których mowa w ust. 1 nadaje Prezydent Federacji lub osoba przez niego wyznaczona;
- 3) Administrator danych osobowych lub osoba przez niego wyznaczona prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych według wzoru stanowiącego **załącznik nr 3**;
- 4) Upoważnienie, o którym mowa w ust. 1 powinno zostać nadane przed uzyskaniem przez osobę, której upoważnienie ma zostać wydane, dostępu do danych osobowych przetwarzanych przez Administratora danych osobowych;
- 5) Upoważnione do przetwarzania danych osoby są zapoznawane z obowiązującymi u ADO procedurami związanymi z ochroną danych osobowych oraz zobligowane do ich przestrzegania;
- 6) Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do zachowania w tajemnicy danych osobowych, z którymi ma styczność oraz sposobów ich zabezpieczenia u ADO.

## **2. Zasady dostępu do systemów informatycznych:**

- 1) Dostęp do komputera, przez który następuje dostęp do danych osobowych przetwarzanych za pomocą Systemów:
  - a) dostęp do komputera należącego do Administratora danych osobowych przekazanego do użytku osobom upoważnionym przez Administratora danych osobowych do przetwarzania danych osobowych w Systemach możliwy jest po zalogowaniu;
  - b) zalogowanie się jest możliwe po wpisaniu hasła, które znane jest jedynie osobom upoważnionym przez Administratora danych osobowych do korzystania z komputera;
  - c) rejestracja Użytkownika systemu polega na nadaniu Użytkownikowi systemu unikalnego identyfikatora, przydzieleniu hasła oraz wprowadzeniu tych danych do bazy Użytkowników systemu;
- 2) Wyrejestrowanie Użytkownika systemu:
  - a) wyrejestrowania Użytkownika systemu z Systemu dokonuje Administrator danych osobowych lub osoba przez niego wyznaczona;



- b) wyrejestrowanie z Systemu polega na zablokowaniu konta osoby, która utraciła uprawnienia do przetwarzania danych osobowych za pośrednictwem Systemu oraz unieważnieniu przydzielonego jej loginu;
  - c) identyfikator Użytkownika systemu, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie;
- 3) Osobą odpowiedzialną za realizację procedury nadawania uprawnień i rejestrowania Użytkownika w Systemie jest Prezydent Federacji lub osoba przez niego wyznaczona.

## **VI. Rejestr czynności przetwarzania.**

1. W Federacji przetwarzane są dane:

- 1) członków władz Federacji, a w tym:
  - a) członków Zarządu Federacji,
  - b) członków Komisji Rewizyjnej Federacji,
  - c) delegatów na kongres Federacji,
- 2) członków Komisji Zarządu Federacji,
- 3) pracowników oraz osób zatrudnionych na podstawie umów cywilno-prawnych,
- 4) wolontariuszy,
- 5) darczyńców,
- 6) osób zwracających się do Federacji w prośbami, wnioskami i zażaleniami.

2. Dane członków Zarządu i Komisji Rewizyjnej przetwarzane są w formie papierowej oraz sporadycznie elektronicznej i obejmują w szczególności:

- 1) imię, nazwisko,
- 2) datę i miejsce urodzenia,
- 3) pełny adres zamieszkania (miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
- 4) numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej.

Podstawą prawną przetwarzania tych danych jest prawny obowiązek Federacji w odniesieniu do art. 6 ust. 1 lit. c RODO w związku z wymogami ustawy z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach ( Dz. U. z 1989 r., nr. 20, poz. 104 ze zm.).

3. Dane delegatów na Kongres Federacji oraz członków Komisji Zarządu Federacji przetwarzane są w formie papierowej oraz sporadycznie elektronicznej i obejmują w szczególności:

- 1) Imię i nazwisko,
- 2) funkcja w Stowarzyszeniu – członku Federacji,

- 3) praca w Komisji/Zespole Stowarzyszenia – członku Federacji,
- 4) numer telefonu komórkowego,
- 5) adres e-mail,
- 6) wykształcenie/kwalifikacje.

Podstawą prawną przetwarzania tych danych jest prawnie uzasadniony interes Federacji w odniesieniu do art. 6 ust. 1 lit. f RODO w związku ze statutem Federacji.

4. Dane pracowników oraz osób zatrudnionych na podstawie umów cywilno-prawnych przetwarzane w są formie papierowej oraz elektronicznej i obejmują w szczególności:
  - 1) imię, nazwisko,
  - 2) numer ewidencyjny PESEL,
  - 3) datę i miejsce urodzenia,
  - 4) pełny adres zamieszkania (miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
  - 5) wykształcenie i doświadczenie zawodowe,
  - 6) numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej,
  - 7) numer rachunku bankowego.

Podstawą prawną przetwarzania tych danych jest umowa o pracę lub umowa zlecenie w odniesieniu do art. 6 ust. 1 lit. b RODO oraz prawny obowiązek Federacji w odniesieniu do art. 6 ust. 1 lit. c RODO w związku z wymogami ustawy z dnia 26 czerwca 1974 r. Kodeks pracy.

5. Dane osobowe wolontariuszy współpracujących ze Federacją przetwarzane są w formie papierowej oraz sporadycznie elektronicznej i obejmują następujący zakres:
  - 1) imiona i nazwiska,
  - 2) adres zamieszkania (miejscowość wraz z kodem pocztowym, ulica, numer domu, numer mieszkania),
  - 3) serię i numer dowodu osobistego, numer ewidencyjny PESEL i/lub NIP,
  - 4) ramy graniczne obowiązywania porozumienia o wolontariacie,
  - 5) dane kontaktowe (telefon komórkowy/stacjonarny oraz adres poczty elektronicznej).

Podstawą prawną przetwarzania tych danych jest prawny obowiązek Federacji zawarcia porozumienia w odniesieniu do art. 6 ust. 1 lit. b RODO w związku z postanowieniami art. 44 ustawy z dnia 24 kwietnia 2003 r. o działalności pożytku publicznego i o wolontariacie (Dz. U. z 2003 r., nr 96, poz. 873).

6. Dane osobowe darczyńców Federacji przetwarzane są w formie papierowej oraz elektronicznej i obejmują następujący zakres:

- 1) imię i nazwisko,
- 2) pełny adres lub oznaczenie samej tylko miejscowości,
- 3) serię i numer dowodu osobistego,
- 4) numer ewidencyjny PESEL i/lub NIP,
- 5) numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej,
- 6) datę wpływu/przekazania darowizny,
- 7) przedmiot darowizny (pieniężna i/lub rzeczowa),
- 8) nazwę banku i numer rachunku bankowego (w przypadku darowizny pieniężnej).

Podstawą prawną przetwarzania tych danych jest prawny obowiązek Federacji w odniesieniu do art. 6 ust. 1 lit. c RODO w związku z postanowieniami ustawy z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (Dz. U. z 1983 r., nr 45, poz. 207) oraz ustawy z dnia 15 lutego 1992 r. o podatku dochodowym od osób prawnych (Dz. U. z 1992 r., nr 21, poz. 86).

7. Dane osobowe w niezbędnym zakresie przekazywane są do:

- 1) Zakładu Ubezpieczeń Społecznych,
- 2) Narodowego Instytutu Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego – w razie realizacji Programów Operacyjnych Funduszu Inicjatyw Obywatelskich,
- 3) Ministerstwa Obrony Narodowej – w razie udziału w otwartych konkursach ofert,
- 4) Urzędu ds. Kombatantów i Osób Represjonowanych – w razie udziału w otwartych konkursach ofert,
- 5) Ministerstwa Spraw Wewnętrznych i Administracji – w razie organizowania zbiórek publicznych,
- 6) organów administracji rządowej i samorządowej – w razie ubiegania się o dotacje
- 7) innych organów państwowych upoważnionych do dostępu do danych osobowych na mocy odrębnych przepisów.

8. Dane z podmiotami wymienionymi w ppkt. 1 – 7 przesyłane są teletransmisyjnie za pośrednictwem Internetu oraz w formie papierowej.

9. Przelewy bankowe realizowane są za pośrednictwem Internetu lub przekazów pocztowych.

10. Administrator danych osobowych jest zobowiązany do prowadzenia rejestru czynności przetwarzania danych osobowych, za który odpowiada;

11. W rejestrze czynności przetwarzania należy zamieścić następujące informacje:

- a) nazwę oraz dane kontaktowe Administratora danych osobowych;

- b) nazwę czynności przetwarzania (procesu/zbioru);
  - c) cele przetwarzania;
  - d) podstawę prawną przetwarzania danych osobowych;
  - e) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
  - f) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
  - g) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a także dokumentacja odpowiednich zabezpieczeń;
  - h) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
  - i) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa ochrony danych osobowych;
12. Obowiązki, o których mowa w pkt. 10 i 11, nie mają zastosowania do Administratora danych zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonuje, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych (tzw. dane wrażliwe), o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

## **VII. Przeprowadzanie oceny ryzyka dla ochrony danych.**

1. Administrator danych osobowych powinien systematycznie przeprowadzać analizę ryzyka dla ochrony danych osobowych, które przetwarza;
2. Celem procesu analizy ryzyka jest zapewnienie ochrony danych osobowych na wszystkich etapach procesu przetwarzania danych, tj. od momentu zebrania danych osobowych do momentu ich usunięcia.
3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:
  - a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
  - b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
  - c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

## **VIII. Powierzenie przetwarzania danych osobowych.**

Jeżeli Administrator danych osobowych zamierza przetwarzać dane osobowe przy pomocy innego podmiotu, to:

- 1) zobowiązany jest do korzystania z usług wyłącznie takich przetwarzających, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przewidziane w przepisach prawa, w szczególności RODO i chroniło prawa osób, których dane dotyczą;
- 2) zobowiązany jest do zawarcia pisemnej umowy powierzenia przetwarzania danych osobowych, w której określa się przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Umowa powinna wskazywać w szczególności, że Podmiot przetwarzający:
  - a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora danych osobowych;
  - b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
  - c) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora danych osobowych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
  - d) udostępnia Administratorowi danych osobowych wszelkie informacje niezbędne do wykazania spełnienia w/w obowiązków oraz umożliwia Administratorowi danych osobowych lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;
- 3) Administrator danych osobowych lub osoba przez niego wyznaczona prowadzi wykaz Podmiotów przetwarzających, z którymi Administrator danych osobowych zawarł umowę powierzenia przetwarzania danych osobowych.

## **IX. Zasady realizacji praw osób, których dane dotyczą.**

1. Administrator danych osobowych dokłada wszelkich starań, aby osoby, których dane dotyczą, mogły w pełni korzystać z praw, które związane są z przetwarzaniem ich danych osobowych, w szczególności:

- 1) prawa do poinformowania (art.13 RODO);
  - 2) prawa dostępu do danych osobowych (art. 15 RODO);
  - 3) prawa do sprostowania danych osobowych (art. 16 RODO);
  - 4) prawa do usunięcia danych osobowych (art. 17 RODO);
  - 5) prawa do ograniczenia przetwarzania (art. 18 RODO);
  - 6) prawa do wniesienia sprzeciwu (art.21 RODO).
2. Wykonywanie praw przez osoby, których dane dotyczą odbywa się przy uwzględnieniu następujących zasad:
- 1) W przypadku pozyskania przez Administratora danych osobowych danych od osoby, której dane dotyczą, spełnia on przy zbieraniu danych obowiązek informacyjny według wzoru stanowiącego **załącznik nr 4**;
  - 2) W przypadku, gdy Administrator danych osobowych pozyskał dane nie bezpośrednio od osoby, której dane dotyczą (z innego źródła), spełnia on wobec tej osoby obowiązek informacyjny według wzoru stanowiącego **załącznik nr 5**.
  - 3) Administrator danych osobowych podejmuje odpowiednie środki, aby w związku, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem, udzielić osobie, której dane dotyczą wszelkich informacji oraz prowadzić z nią wszelką komunikację w sprawie przetwarzania;
  - 4) Administrator danych osobowych bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania, udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z wykonywaniem przez nią praw z zakresu ochrony danych osobowych;
  - 5) Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie w zakresie wykonywania przez nią przysługujących jej praw, może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą;
  - 6) Administrator danych osobowych informuje osobę o planowanej zmianie celu przetwarzania danych;
  - 7) Administrator danych osobowych uzupełnia i aktualizuje dane na żądanie osoby;
  - 8) Na żądanie osoby, Administrator danych osobowych usuwa dane, gdy:
    - dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,
    - zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
    - osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
    - dane były przetwarzane niezgodnie z prawem,
    - konieczność usunięcia wynika z obowiązku prawnego,

Administrator danych osobowych informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

## **X. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.**

Administrator danych osobowych wprowadził środki techniczne i organizacyjne konieczne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.

### **1. Zabezpieczenia fizyczne:**

- 1) Pomieszczenia i lokale, w których przetwarzane są dane osobowe zabezpieczone są kluczem, alarmem i monitoringiem video;
- 2) W oknach pomieszczeń, w których przetwarzane są dane osobowe zamontowano kraty/rolety/folię antywłamaniową;
- 3) Klucze do pomieszczeń, w których przetwarzane są dane osobowe przechowywane są w zabezpieczonym miejscu, a dostęp do nich mają jedynie osoby upoważnione;
- 4) W czasie godzin pracy pomieszczenia nadzorowane są przez pracowników upoważnionych do przetwarzania danych osobowych;
- 5) Osoby postronne mogą przebywać w pomieszczeniach, w których przetwarzane są dane osobowe wyłącznie w obecności osób upoważnionych do przetwarzania danych osobowych;
- 6) W sytuacji, gdy w miejscu przetwarzania danych osobowych przyjmowane są osoby postronne, osoby upoważnione do przetwarzania danych osobowych są zobowiązane do zwrócenia szczególnej uwagi na zabezpieczenie stanowiska pracy tak, aby osoby postronne nie miały dostępu do danych osobowych, w szczególności należy:
  - a) ograniczyć do niezbędnego minimum ilość dokumentów zawierających dane osobowe, na których się pracuje;
  - b) ograniczyć możliwość niekontrolowanego dostępu do przetwarzanych danych osobowych, w szczególności poprzez zamykanie teczek zawierających dane osobowe, odwrócenie tych dokumentów stroną zawierającą dane osobowe do dołu, wyłączenie monitora, włączenie wygaszacza ekranu;
- 7) Dokumentacja papierowa jest przechowywana w szafkach metalowych oraz niemetalowych zamykanych na klucz;



- 8) Stosowana jest zasada „czystego biurka”, która oznacza, że po zakończeniu pracy każdy pracownik powinien schować dokumentację papierową zawierającą dane osobowe do wyznaczonej do tego szafy;
- 9) Po ustaniu przydatności dokumentacja papierowa zawierająca dane osobowe jest niszczone za pomocą niszczarki do papieru;

## **2. Zabezpieczenia związane z systemami informatycznymi:**

- 1) Dostęp do systemów informatycznych, za pomocą których przetwarzane są dane osobowe wymaga nadania i zarejestrowania uprawnień do przetwarzania danych osobowych oraz ich uwierzytelniania za pomocą loginu i hasła z zachowaniem następujących zasad:
- 2) Systemy informatyczne zostały zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego poprzez zainstalowanie programu antywirusowego;
- 3) Systemy informatyczne/serwery zostały zabezpieczone przed utratą danych w razie awarii zasilania lub zakłóceniami w sieci zasilającej poprzez urządzenia UPS/listwy antyprzebieciowe;
- 4) Urządzenia/dyski twarde komputerów, drukarek, kserokopiarek oddawane mogą być do serwisu po usunięciu danych osobowych lub zaszyfrowaniu;
- 5) Monitory ustawiane są w sposób uniemożliwiający wgląd osobom postronnym;
- 6) Pliki zawierające dane osobowe przesyłane za pośrednictwem poczty elektronicznej są hasłowane;
- 7) Administrator danych osobowych oraz upoważnione przez niego osoby korzystają z mobilnych urządzeń i nośników danych z zachowaniem następujących zasad:
  - a) mobilne urządzenia i nośniki danych powinny być szyfrowane;
  - b) mobilne urządzenia i nośniki danych nie są wynoszone poza siedzibę Administratora danych osobowych;
  - c) mobilne urządzenia i nośniki danych po zakończeniu ich używania zamykane są w zamykanych szafach;
- 8) Urządzenia, dyski lub inne nośniki informatyczne, na których zgromadzone są dane osobowe, przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych lub uszkadza w sposób uniemożliwiający odczytanie danych osobowych.

## **3. Zabezpieczenia organizacyjne:**



- 1) W niniejszej Polityce ochrony danych określono zasady mające na celu zabezpieczenie organizacyjne przetwarzanych danych osobowych, w szczególności określono:
  - a) zasady przebywania osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe;
  - b) zasady zarządzania incydentami dotyczącymi naruszeń ochrony danych osobowych;
  - c) zasady udostępnienia danych osobowych.
- 2) Przeprowadzane są wrywkowe, okresowe kontrole zabezpieczeń fizycznych po zakończonej pracy przez osoby upoważnione do przetwarzania danych osobowych.

#### **4. Zabezpieczenia personalne:**

- 1) Dostęp do danych osobowych mają tylko osoby posiadające upoważnienie do przetwarzania danych osobowych;
- 2) Osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania w tajemnicy danych osobowych, do których mają dostęp oraz stosowanych środków bezpieczeństwa;
- 3) Prowadzona jest ewidencja osób upoważnionych mających dostęp do zbiorów danych osobowych przetwarzanych u Administratora danych osobowych;
- 4) Zostały przyjęte jasne procedury przetwarzania danych osobowych;
- 5) Wprowadzono zasady bezpieczeństwa danych osobowych na stanowiskach pracy, w tym obowiązek wylogowywania się z systemów informatycznych, stosowania zasady „czystego biurka”, niezapisywanie prywatnych dokumentów zawierających dane osobowe na komputerach pracowniczych;
- 6) Wszystkie osoby, które mają do czynienia z przetwarzaniem danych osobowych zostały odpowiednio przeszkolone i poinformowane o zagrożeniach oraz konsekwencjach wynikających z niezastosowania się, złamania lub pominięcia przyjętych procedur;
- 7) Zostały wyznaczone osoby odpowiedzialne za systemy, procesy, zasoby związane z danymi osobowymi, w szczególności:
  - a) wyznaczono osobę odpowiedzialną za systemy informatyczne, przy pomocy których Administrator danych osobowych przetwarza te dane;
  - b) wprowadzono monitorowanie działań osób upoważnionych do przetwarzania danych osobowych ze strony kierownictwa;

- 8) Ustalono reguły postępowania w przypadku nieobecności pracowników przetwarzających dane osobowe.

#### **5. Procedura przeprowadzania kontroli stanu zabezpieczeń danych osobowych:**

- 1) Administrator danych osobowych lub osoba przez niego upoważniona przeprowadza ocenę skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania, które mają się odbywać co najmniej raz na rok;
- 2) Osoba zobowiązana do przeprowadzania czynności, o których mowa powyżej, zobowiązana jest do ustalenia, czy wprowadzone zabezpieczenia są wystarczające dla ochrony przetwarzanych danych osobowych, w szczególności uwzględniając w szczególności stan wiedzy technicznej, koszt wdrożenia oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia dla przetwarzanych danych.

### **XI. Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.**

#### **1. Postępowanie w przypadku ujawnienia incydentu ochrony danych osobowych:**

- 1) Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do niezwłocznego poinformowania Administratora danych osobowych, przede wszystkim Prezydenta Federacji o każdym podejrzeniu naruszenia bezpieczeństwa danych osobowych;
- 2) Po otrzymaniu informacji o incydencie, Administrator danych osobowych podejmuje czynności mające na celu ustalenie, czy doszło do naruszenia bezpieczeństwa danych osobowych, w tym w szczególności sprawdza stan wszelkich urządzeń służących do przetwarzania danych osobowych, sposób działania wprowadzonych zabezpieczeń oraz metody pracy osób upoważnionych do przetwarzania danych osobowych;
- 3) Po ustaleniu, iż doszło do naruszenia zabezpieczeń danych osobowych Administrator danych osobowych podejmuje w szczególności czynności mające na celu:
  - a) uniemożliwienie dalszego naruszenia bezpieczeństwa danych osobowych;
  - b) powstrzymanie lub ograniczenie dostępu do danych osobowych nieupoważnionej osobie;

- c) przywrócenie prawidłowego działania zabezpieczeń;
  - d) ustalenie, w jaki sposób doszło do naruszenia bezpieczeństwa;
  - e) inne czynności niezbędne do ustalenia przyczyn naruszeń oraz podjęcia działań mających na celu wyeliminowanie naruszeń w przyszłości;
- 4) Administrator danych osobowych lub osoba przez niego wyznaczona prowadzi rejestr naruszeń ochrony danych osobowych według wzoru stanowiącego **załącznik nr 6**;
- 5) Prezydent Federacji lub osoba przez niego wyznaczona, podejmuje działania mające na celu wyciągnięcie konsekwencji wobec osoby odpowiedzialnej za naruszenie (o ile przyczyną naruszenia jest działanie jakiegokolwiek osoby) oraz wyeliminowanie jakichkolwiek naruszeń zabezpieczeń danych osobowych w przyszłości.

## **2. Zgłoszenie do organu nadzorczego naruszenia ochrony danych osobowych:**

- 1) Administrator danych osobowych jest zobowiązany bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić je organowi nadzorczemu według wzoru stanowiącego **załącznik nr 7**, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku, gdy zgłoszenie przekazano organowi nadzorczemu po upływie 72 godzin, należy dołączyć do niego wyjaśnienie przyczyn opóźnienia;
- 2) Zgłoszenie, o którym mowa powyżej, powinno co najmniej:
- a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
  - b) zawierać imię i nazwisko oraz dane kontaktowe osoby, od którego można uzyskać więcej informacji;
  - c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
  - d) opisywać środki zastosowane lub proponowane przez Administratora danych osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

## **3. Zawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą:**

- 1) Administrator danych osobowych jest zobowiązany bez zbędnej zwłoki, zawiadomić osobę, której dane dotyczą o naruszeniu jej danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności tych osób;
- 2) Zawiadomienia dokonuje się według wzoru stanowiącego **załącznik nr 8**;
- 3) Nie trzeba dokonywać zawiadomienia o którym mowa powyżej w przypadku, gdy:
  - a) zostały przez Administratora danych osobowych wdrożone odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczyło naruszenie;
  - b) zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
  - c) wymagałoby to niewspółmiernie dużego wysiłku; w takim przypadku wydaje się publiczny komunikat lub stosuje się podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób.

## **XII. Postanowienia końcowe**

1. Wdrożenie „Polityki ochrony danych” odbywa się poprzez zapoznanie wszystkich osób upoważnionych do przetwarzania danych osobowych z treścią „Polityki ochrony danych” oraz systematyczne szkolenia ich z zakresu ochrony danych osobowych.
2. „Polityka ochrony danych” wchodzi w życie z dniem podjęcia uchwały przez Zarząd Federacji lub w terminie określonym w treści tej uchwały.
3. Zmiany w „Polityce ochrony danych” będą wchodzić w życie w terminach określonych w uchwałach Prezydium Zarządu Federacji dotyczących wprowadzenia zmian w dokumencie.

## **XIII. WYKAZ ZAŁĄCZNIKÓW**

Do Polityki ochrony danych zostały załączone następujące wzory dokumentów:

1. Wykaz systemów informatycznych służących do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych.
3. Ewidencja osób upoważnionych do przetwarzania danych osobowych z ramienia Federacji.
4. Wzór ogólny obowiązku informacyjnego w przypadku osób, których dane pozyskano bezpośrednio od nich.
- 4a. Wzór obowiązku informacyjnego w przypadku osób, których dane pozyskano bezpośrednio od nich.

5. Wzór obowiązku informacyjnego wobec osób, których dane zostały pozyskane z innego źródła (nie od osoby, której dane dotyczą).
6. Rejestr naruszeń ochrony danych osobowych prowadzony przez Federację.
7. Zawiadomienie o naruszeniu ochrony danych osobowych przez Federację.
8. Zawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą.
9. Zgoda na przetwarzanie danych osobowych.
10. Zgoda na rozpowszechnianie wizerunku.

**ZAŁĄCZNIKI:**

**Załącznik nr 1**  
**do Polityki ochrony danych osobowych obowiązującej**  
**w Federacji Stowarzyszeń Służb Mundurowych RP**

**WYKAZ SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO  
 PRZETWARZANIA  
 DANYCH OSOBOWYCH**

Nazwa systemu informatycznego	Opis systemu informatycznego (do czego system informatyczny służy)	Kategorie przetwarzanych danych (np. członkowie władz Federacji itd. )

**Załącznik nr 2**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

Warszawa, dnia .....

**UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH**

**UPOWAŻNIENIE NR .....**

**Federacja Stowarzyszeń Służb Mundurowych RP** z siedzibą w Warszawie, ul. Krochmalna 32, jako Administrator Danych Osobowych, z dniem .....

**upoważnia Panią/Pana** .....

członka władz Federacji, członka komisji/ zespołu problemowego ....., zatrudnionego na podstawie umowy o pracę/wykonującą/-ego obowiązki wynikające z umowy zlecenia/umowy o dzieło,

**do przetwarzania danych osobowych** (w systemach informatycznych i w formie papierowej) **w zakresie niezbędnym do wykonywania obowiązków** wynikających z pełnionej funkcji lub w/w umowy.

Niniejsze **upoważnienie jest ważne do ustania** pełnienia funkcji lub stosunku wynikającego z w/w umowy.

Jednocześnie informuję, iż zgodnie z europejskimi i krajowymi przepisami dotyczącymi ochrony danych osobowych, **osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia.**

.....  
Podpis Administratora danych

.....  
Podpis osoby upoważnionej

### **OŚWIADCZENIE OSOBY UPOWAŻNIONEJ DO PRZETWARZANIA DANYCH OSOBOWYCH**

Ja, niżej podpisana/y:

1. Oświadczam, że zostałam(em) przeszkolona(y) w zakresie ochrony danych osobowych, w tym obowiązujących przepisów prawa europejskiego i krajowego dotyczącego ochrony danych osobowych oraz zapisów dokumentów wewnętrznych obowiązujących u Administratora danych osobowych, tj. Federacji Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, ul. Krochmalna32), w szczególności Polityki ochrony danych oraz instrukcjach i procedurach dotyczących ochrony danych osobowych.
2. Oświadczam, że zobowiązuję się do:
  - a) ochrony danych osobowych przed dostępem do nich osób nieupoważnionych oraz do zabezpieczenia danych osobowych przed zniszczeniem i nielegalnym ujawnieniem, w tym zgodnie z procedurami przewidzianymi w obowiązującej u Administratora danych osobowych Polityce ochrony danych oraz instrukcjach i procedurach dotyczących ochrony danych osobowych;
  - b) zachowania w tajemnicy danych osobowych, z którymi zetknęłam/zatknąłem się w trakcie wykonywania swoich obowiązków wynikających z pełnionej funkcji lub umowy zawartej z Administratorem danych osobowych oraz środków bezpieczeństwa stosowanych przez Administratora danych osobowych;
  - c) zostałam (em) zapoznana (y) z przepisami dotyczącymi odpowiedzialności prawnej za naruszenie przepisów o ochronie danych osobowych.

.....  
Podpis Administratora danych osobowych

.....  
Podpis osoby upoważnionej

**Załącznik nr 3**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

**EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH  
Z RAMIENIA  
FEDERACJI STOWARZYSZEŃ SŁUŻB MUNDUROWYCH RP Z SIEDZIBĄ  
W WARSZAWIE**

Nr	Imię i nazwisko użytkownika	Zakres przydzielonych uprawnień oraz identyfikator w systemie informatycznym	Data nadania uprawnień	Data odebrania uprawnień
1.				
2.				
3.				
4.				
5.				
6.				
7.				



Załącznik nr 4

do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP

**Wzór ogólny obowiązku informacyjnego w przypadku osób, których dane pozyskano bezpośrednio od nich:**

**INFORMACJA**

1. Administratorem Pani/Pana danych osobowych jest Federacja Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32 lok. 35, 00 864 Warszawa, email: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl), tel. ...., dalej jako ADO;
2. Pani/Pana dane osobowe będą przetwarzane w celu .....
3. Podstawą przetwarzania Pani/Pana danych osobowych jest .....
4. Odbiorcami Pani/Pana danych osobowych są/będą .....
5. ADO nie zamierza przekazywać Pani/Pana danych osobowych do państwa trzeciego/organizacji międzynarodowej;
6. Pani/Pana dane osobowe będą przechowywane przez okres .....
7. Przysługuje Pani/Panu prawo żądania dostępu do treści swoich danych osobowych oraz prawo ich sprostowania.
8. W przypadkach określonych przepisami prawa przysługuje Pani/Panu prawo żądania usunięcia danych osobowych, żądania ograniczenia przetwarzania danych osobowych, prawo do przeniesienia danych osobowych, prawo sprzeciwu wobec przetwarzania danych osobowych.
9. Przysługuje Pani/Panu prawo cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
10. Przysługuje Pani/Panu prawo wniesienia skargi do organu zajmującego się ochroną danych osobowych, gdy uzna Pani/Pan, że ADO naruszył przepisy dotyczące ochrony danych osobowych.
11. Podanie przez Panią/Pana danych osobowych jest *wymogiem ustawowym/umownym/ jest warunkiem zawarcia umowy*. Podanie danych *jest/nie jest* obowiązkowe. Brak podania danych będzie skutkowało .....

12. Pana/Pani dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji względem Pana/Pani, w tym do profilowania.

Zapoznałem/am się z treścią powyższej  
Informacji:

.....  
Data i czytelny podpis

**Załącznik nr 4a**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

**Wzór obowiązku informacyjnego w przypadku osób, których dane pozyskano  
pośrednio od nich:**

### **Informacje dotyczące przetwarzania danych osobowych**

#### **Administrator danych osobowych.**

Administratorem Państwa danych osobowych będzie Federacja Stowarzyszeń Służb Mundurowych RP (dalej Federacja) z siedzibą w Warszawie, przy ul. Krochmalnej 32.  
Z Federacją można skontaktować się poprzez adres email: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl), telefonicznie pod nr tel. .... lub pisemnie na adres: ul. Krochmalna 32 lok. 35, 00-864 Warszawa.

#### **Cel i podstawa przetwarzania.**

Będziemy przetwarzać Państwa dane osobowe w celu realizacji statutu Federacji Stowarzyszeń Służb Mundurowych RP, zgodnie z art. 6 ust. 1 lit. c RODO<sup>1</sup> w związku z ustawą z dnia 7 kwietnia 1989 r. Prawo o stowarzyszeniach ( Dz. U. z 1989 r., nr. 20, poz. 104 ze zm.).

Podanie danych jest nieobowiązkowe, ale niezbędne do realizacji powyżej podanego celu przetwarzania.

#### **Odbiorcy danych osobowych.**

---

<sup>1</sup> Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U. UE L 119 z 4 maja 2016 r. oraz Dz.U. UE L 127 z 23 maja 2018 r.) – nazywanego RODO

Dane osobowe będą mogły być powierzane przez Federację do przetwarzania podmiotom przetwarzającym dane w jej imieniu, w tym w zakresie obsługi systemów informatycznych, obsługi finansowo-księgowej lub prawnej - przy czym takie podmioty przetwarzają dane jako podwykonawcy, na podstawie umowy ze Federacją i wyłącznie zgodnie z jej poleceniami.

#### **Okres przechowywania danych.**

Będziemy przechowywać Państwa dane osobowe w okresie udziału w działalności Federacji, dla której zostały one zebrane, a następnie - w przypadkach, w których wymagają tego przepisy ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2018 r., poz. 217 ze zm.) – przez czas określony w tych przepisach.

#### **Prawa osób, których dane dotyczą**

Zgodnie z RODO przysługuje Państwu:

- a. prawo dostępu do swoich danych oraz otrzymania ich kopii;
- b. prawo do sprostowania (poprawiania) swoich danych, jeśli są błędne lub nieaktualne, a także prawo do ich usunięcia, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa;
- c. prawo do ograniczenia lub wniesienia sprzeciwu wobec przetwarzania danych;
- d. prawo do wniesienia skargi do Prezesa UODO (na adres Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa)

Zapoznałem/am się z treścią powyższej  
Informacji:

.....  
Data i czytelny podpis

Załącznik nr 5

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

**Wzór ogólny obowiązku informacyjnego wobec osób, których dane zostały pozyskane z innego źródła (nie od osoby, której dane dotyczą):**

Warszawa, dnia .....

.....

Imię i nazwisko adresata

**INFORMACJA**

1. Administratorem Pani/Pana danych osobowych w postaci ..... jest Federacja Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32 lok. 35, 00 864 Warszawa, email: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl), tel. ...., dalej jako ADO.
2. ADO pozyskał Pani/Pana dane osobowe od/z .....
3. Pani/Pana dane osobowe będą przetwarzane w celu .....
4. Podstawą przetwarzania Pani/Pana danych osobowych jest .....
5. Odbiorcami Pani/Pana danych osobowych są/będą .....
6. ADO nie zamierza przekazywać Pani/Pana danych osobowych do państwa trzeciego/organizacji międzynarodowej;
7. Pani/Pana dane osobowe będą przechowywane przez okres .....
8. Przysługuje Pani/Panu prawo żądania dostępu do treści swoich danych osobowych oraz prawo ich sprostowania.
9. W przypadkach określonych przepisami prawa przysługuje Pani/Panu prawo żądania usunięcia danych osobowych, żądania ograniczenia przetwarzania danych osobowych, prawo do przeniesienia danych osobowych, prawo wniesienia sprzeciwu wobec przetwarzania danych osobowych.
10. Przysługuje Pani/Panu prawo cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
11. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, gdy uzna Pani/Pan, że ADO naruszył przepisy dotyczące ochrony danych osobowych;

12. Pana/Pani dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji względem Pana/Pani, w tym do profilowania

Zapoznałem/am się z treścią powyższej  
Informacji:

.....  
Data i czytelny podpis

**Załącznik nr 6**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

**REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH  
PROWADZONY PRZEZ FEDERACJĘ STOWARZYSZEŃ  
SŁUŻB MUNDUROWYCH RP**

L.p.	Rodzaj naruszenia <sup>2</sup>	Data i godzina naruszenia	Kategoria i ilość osób, których dotyczy naruszenie <sup>3</sup>	Kategorie danych (zakres danych), których dotyczy naruszenie <sup>4</sup>	Okoliczności naruszenia – opis, analiza zdarzenia, przyczyny wystąpienia naruszenia <sup>5</sup>	Opis skutków naruszenia/możliwych konsekwencji naruszenia ochrony danych osobowych <sup>6</sup>	zarac zasto prop zarac ochr podj zmin nega
------	--------------------------------	---------------------------	---	---	--	---	---

<sup>2</sup> Za naruszenie ochrony danych osobowych rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, np. wyciek danych z systemu, kradzież laptopa z danymi osobowymi.

<sup>3</sup> Należy wskazać, jakiej kategorii osób/jakich osób dotyczy naruszenie oraz przybliżoną liczbę osób, których dotyczy naruszenie, np. Pracownicy, osoby z władz FEDERACJI itd. oraz przybliżoną ilość osób, których dotyczy naruszenie wyrażoną liczbowo, np. ok. 10 osób.

<sup>4</sup> Należy wskazać, jakich konkretnie danych osób dotyczy naruszenie, np. imię, nazwisko, PESEL itd.

<sup>5</sup> Należy wskazać okoliczności naruszenia ochrony danych osobowych, tj. w jaki sposób doszło do naruszenia, przyczyny wystąpienia naruszenia ochrony danych osobowych.

<sup>6</sup> Należy wskazać, jakie skutki lub możliwe konsekwencje może nieść za sobą naruszenie ochrony danych osobowych wobec osób, których dane osobowe dotyczą, np. kradzież tożsamości, naruszenie dobrego imienia/ naruszenie dóbr osobistych itd.

<sup>7</sup> Należy wskazać, jakie działania zaradcze zostały podjęte w związku z dokonanym naruszeniem ochrony danych osobowych, np. zastosowanie dodatkowego oprogramowania, alarm, karty dostępu do pomieszczeń, wprowadzenie dodatkowych procedur itd.

<sup>8</sup> Zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego jest wymagane, chyba że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, których dane osobowe dotyczą.

<sup>9</sup> Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych jest wymagane, jeżeli to naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

1.							
2.							

Załącznik nr 7

do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP

Warszawa, dnia .....

Nazwa podmiotu zgłaszającego:

**Federacja Stowarzyszeń Służb Mundurowych RP**

ul. Krochmalna 32 lok. 35, 00 864 Warszawa,

email: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl)

dalej jako *Podmiot zgłaszający*

Adresat zgłoszenia:

**Urząd Ochrony Danych Osobowych**

**ul. Stawki 2**

**00-193 Warszawa**

**ZGŁOSZENIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH**

Działając w imieniu Podmiotu zgłaszającego, wypełniając obowiązek wynikający z przepisu art. 33 Rozporządzenia UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych z dnia 27 kwietnia 2016 r. niniejszym zgłaszam, że:

1. W okresie ..... doszło do naruszenia ochrony danych osobowych polegającego na .....
2. Możliwymi konsekwencjami naruszenia ochrony danych osobowych opisanego w pkt 1 powyżej są .....
3. Podmiot zgłaszający *zastosował/proponuje* zastosować następujące środki w celu zaradzenia naruszeniu ochrony danych osobowych opisanemu w pkt 1 powyżej, w tym środki mające na celu zminimalizowanie ewentualnych negatywnych skutków naruszenia:
  - 1) .....
  - 2) .....
4. Zgłoszenie następuje z opóźnieniem z uwagi na .....

Poniżej podaję dane osoby, z którą można kontaktować się w przedmiotowej sprawie:

Imię i nazwisko: .....

Adres: .....

Telefon kontaktowy: .....

Adres e-mail: .....

**Załącznik nr 8**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

Warszawa, dnia .....

**Nazwa podmiotu zawiadamiającego:**

**Federacja Stowarzyszeń Służb Mundurowych RP**

**ul. Krochmalna 32 lok. 35, 00 864 Warszawa,**

email: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl)

dalej jako *Podmiot zawiadamiający*

**Adresat zawiadomienia:**

.....

### **ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH**

Działając w imieniu Podmiotu zawiadamiającego, wypełniając obowiązek wynikający z przepisu art. 34 Rozporządzenia UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych z dnia 27 kwietnia 2016 r. niniejszym zawiadamiam, że:

1. W okresie ..... doszło do naruszenia ochrony *Pani/Pana* danych osobowych polegającego na .....
2. Możliwymi konsekwencjami naruszenia ochrony danych osobowych opisanego w pkt 1 powyżej są .....
3. Podmiot zawiadamiający *zastosował/proponuje* zastosować następujące środki w celu zaradzenia naruszeniu ochrony danych osobowych opisanemu w pkt 1 powyżej, w tym środki mające na celu zminimalizowanie ewentualnych negatywnych skutków naruszenia:
  - 1) .....
  - 2) .....
4. ....

Poniżej podaję dane Inspektora Ochrony Danych Osobowych/osoby, z którą można kontaktować się w przedmiotowej sprawie:

Imię i nazwisko: .....

Adres: .....

Telefon kontaktowy: .....

Adres e-mail: .....

**Załącznik nr 9**

**do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP**

**ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH**

Ja, niżej podpisana/y, ..... (imię i nazwisko),  
PESEL ....., niniejszym wyrażam zgodę na przetwarzanie moich danych  
osobowych w postaci ...../wskazanych w ..... przez Federację  
Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32  
lok. 35, 00-864 Warszawa, w celu .....

.....  
Data i czytelny podpis

Oświadczam, że zostałem/-am poinformowany/-a o tym, że:

1. Administratorem moich w/w danych osobowych (dalej jako: dane osobowe) jest Federacja Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32 lok. 35, 00-864 Warszawa, e-mail: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl), nr telefonu: ....., dalej jako ADO.
2. Dane osobowe będą przetwarzane w celu, na jakim wyraziłem/am zgodę powyżej.
3. Podstawą prawną przetwarzania danych osobowych jest wyrażona powyżej zgoda (tj. art. 6 ust. 1 lit. a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej jako RODO).
4. Dane osobowe mogą być ujawnione osobom upoważnionym przez ADO, podmiotom świadczącym na rzecz ADO usługi, w tym usługi techniczne i organizacyjne, usługi prawne, usługi doradcze, usługi finansowe, a także innym podmiotom/organom w zakresie i na zasadach określonych przepisami prawa.
5. Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.



6. Dane osobowe, których dotyczy niniejsze oświadczenie, będą przetwarzane przez okres realizacji celu, w jakim zgoda na przetwarzanie danych została udzielona, jednak nie dłużej niż do czasu wycofania zgody.
7. Przysługuje mi prawo żądania dostępu do treści danych osobowych oraz prawo ich sprostowania.
8. W przypadkach określonych przepisami prawa przysługuje mi prawo żądania usunięcia danych, żądania ograniczenia przetwarzania danych, prawo do przeniesienia danych, prawo sprzeciwu wobec przetwarzania danych.
9. Przysługuje mi prawo cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
10. Przysługuje mi prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych gdy uznaję, że ADO naruszył przepisy dotyczące ochrony danych osobowych.
11. Podanie przeze mnie danych osobowych jest dobrowolne, jednak ich niepodanie może uniemożliwić lub utrudniać realizację celu, dla którego realizacji wyraziłem zgodę na przetwarzanie danych osobowych.
12. Dane osobowe nie będą wykorzystywane do zautomatyzowanego podejmowania decyzji względem mnie, w tym do profilowania.

.....

Data i czytelny podpis

do Polityki ochrony danych osobowych obowiązującej  
w Federacji Stowarzyszeń Służb Mundurowych RP

**ZGODA NA ROZPOWSZECHNIANIE WIZERUNKU**

Ja, niżej podpisana/y, .....,  
PESEL ....., niniejszym wyrażam zgodę na przetwarzanie moich  
danych osobowych w postaci rozpowszechniania mojego wizerunku przez Federację  
Stowarzyszeń Służb Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32  
lok. 35, 00-864 Warszawa, w formie zdjęć bez konieczności każdorazowego ich  
zatwierdzania.

Powyższa zgoda obejmuje:

- 1) dokonywanie niezbędnych przeróbek i zmian takich jak, np. kadrowanie, obróbka  
materiału w zakresie, w jakim będzie to uzasadnione celem i sposobem prezentacji  
wizerunku;
- 2) powielanie i rozpowszechnianie za pośrednictwem dowolnego medium, w szczególności  
za pośrednictwem portali społecznościowych, strony internetowej, materiałów  
promocyjnych,

wyłącznie do celów informacyjno-promocyjnych związanych z działalnością Federacji.

Oświadczam, że z tytułu udzielonej zgody nie będę domagał/-a się zapłaty wynagrodzenie  
ani żadnej innej gratyfikacji.

Niniejsza zgoda stanowi zezwolenie na rozpowszechnianie wizerunku w rozumieniu art. 81  
ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity  
Dz. U. z 2018 r., poz. 1191, 1293, 1669, 2245, 2339).

.....  
Data i czytelny podpis

Oświadczam, że zostałem/-am poinformowany/-a o tym, że:

1. Administratorem moich w/w danych osobowych jest Federacja Stowarzyszeń Służb

Mundurowych RP z siedzibą w Warszawie, adres: ul. Krochmalna 32 lok. 35, 00-864 Warszawa, e-mail: [sekretariat@fssm.pl](mailto:sekretariat@fssm.pl), nr telefonu: ....., dalej jako ADO.

2. Dane osobowe będą przetwarzane w celu, na jakim wyraziłem/am zgodę powyżej.
3. Podstawą prawną przetwarzania danych osobowych jest wyrażona powyżej zgoda (tj. art. 6 ust. 1 lit. a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, dalej jako RODO).
4. Dane osobowe mogą być ujawnione osobom upoważnionym przez ADO, podmiotom świadczącym na rzecz ADO usługi, w tym usługi techniczne i organizacyjne, usługi prawne, usługi doradcze, usługi finansowe, a także innym podmiotom/osobom/organom w zakresie i na zasadach określonych przepisami prawa.
5. Dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
6. Dane osobowe, których dotyczy niniejsze oświadczenie, będą przetwarzane przez okres realizacji celu, w jakim zgoda na przetwarzanie danych została udzielona, jednak nie dłużej niż do czasu wycofania zgody.
7. Przysługuje mi prawo żądania dostępu do treści danych osobowych oraz prawo ich sprostowania.
8. W przypadkach określonych przepisami prawa przysługuje mi prawo żądania usunięcia danych, żądania ograniczenia przetwarzania danych, prawo do przeniesienia danych, prawo sprzeciwu wobec przetwarzania danych.
9. Przysługuje mi prawo cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem.
10. Przysługuje mi prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych gdy uznaję, że ADO naruszył przepisy dotyczące ochrony danych osobowych.
11. Podanie przeze mnie danych osobowych jest dobrowolne, jednak ich niepodanie może uniemożliwić lub utrudniać realizację celu, dla którego realizacji wyraziłem zgodę na przetwarzanie danych osobowych.

.....  
Data i czytelny podpis