

Załącznik nr 1

do Uchwały nr 21/2018 z dnia 13 czerwca 2018 r.
Rady Głównej Federacji Stowarzyszeń Rezerwistów
i Weteranów SZ RP.

**ZATWIERDZAM
PREZES FEDERACJI**

Zdzisław PRZESZŁOWSKI
/płk dypl./

**Polityka Bezpieczeństwa Danych
Osobowych wraz z Instrukcją
zarządzania systemem
informatycznym przetwarzającym
dane osobowe
w Federacji Stowarzyszeń
Rezerwistów i Weteranów SZ RP**



Wstęp

RODO nie przewiduje wykazu dokumentów obligatoryjnych jak również stosowania żadnych konkretnych rozwiązań lub procedur. Decyzja o podjęciu określonych działań pozostaje w gestii administratora danych (ADO).

Podstawą do wdrożenia określonych rozwiązań jest analiza ryzyka. Jej celem jest ocena zagrożeń dla poprawnego i bezpiecznego przetwarzania danych oraz wybór i wdrożenie środków zmniejszających prawdopodobieństwo ich wystąpienia.

Mając na uwadze strukturę, zmiany personalne, pracę wolontariuszy oraz stopień znajomość zagadnień RODO wprowadza się **„Politykę Bezpieczeństwa Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe w Federacji Stowarzyszeń Rezerwistów i Weteranów SZ RP.”**

1. Polityka Bezpieczeństwa

1. Podstawa prawna.

„Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych”) oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.”

Polityka Bezpieczeństwa Ochrony Danych Osobowych, zwana dalej Polityką, oraz Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwana dalej Instrukcją, została opracowana zgodnie z wymogami 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) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

2. Ocena ryzyka.

2.1. Ogólna ocena ryzyka przetwarzania danych osobowych.

2.1.1 Charakter, zakres i cele przetwarzania danych osobowych:

- ⊕ Federacja zajmuje dwa pomieszczenia (p. 229 i 230);
- ⊕ jako obiekt militarny podlega całodobowej ochronie,
- ⊕ dane osobowe są przetwarzane w Biurze Federacji (p.229);
- ⊕ dostępne są dla Dyrektora Biura i Prezydium Federacji (Prezesa, Wiceprezesów, Sekretarza Generalnego i Skarbnika);
- ⊕ przetwarzaniu podlega skład osobowy Rady Głównej oraz delegaci na spotkania międzynarodowe (około 60 osób),
- ⊕ przetwarzane są tylko dane zwykłe, zabronione jest zbieranie danych wrażliwych;
- ⊕ zabronione jest „magazynowanie” danych typu PESEL, numery dokumentów osobistych (dowód osobisty, paszport, numerów kart płatniczych);

2.1.2. Opis i identyfikacja wymagań:

- ▣ dane osobowe przetwarzane są w formie papierowej (druki MON), i na komputerze,
- ▣ dane osobowe przetwarzane są zgodnie z prawem, po uprzednim wyrażeniu zgody i zgodnie ze Statutem Federacji,
- ▣ nie korzysta się z usług zewnętrznych (w tym w chmurze);
- ▣ rejestracji na przedsięwzięcia międzynarodowe dokonuje się przy pomocy arkusza rejestracyjnego przysłanego przez organizatora;
- ▣ w kontaktach z jednostkami organizacyjnymi MON wykorzystywana jest wewnętrzna łączność resortu.

2.1.3. Ocena ryzyka wystąpienia zdarzenia naruszającego prawa osób których dane są przetwarzane.

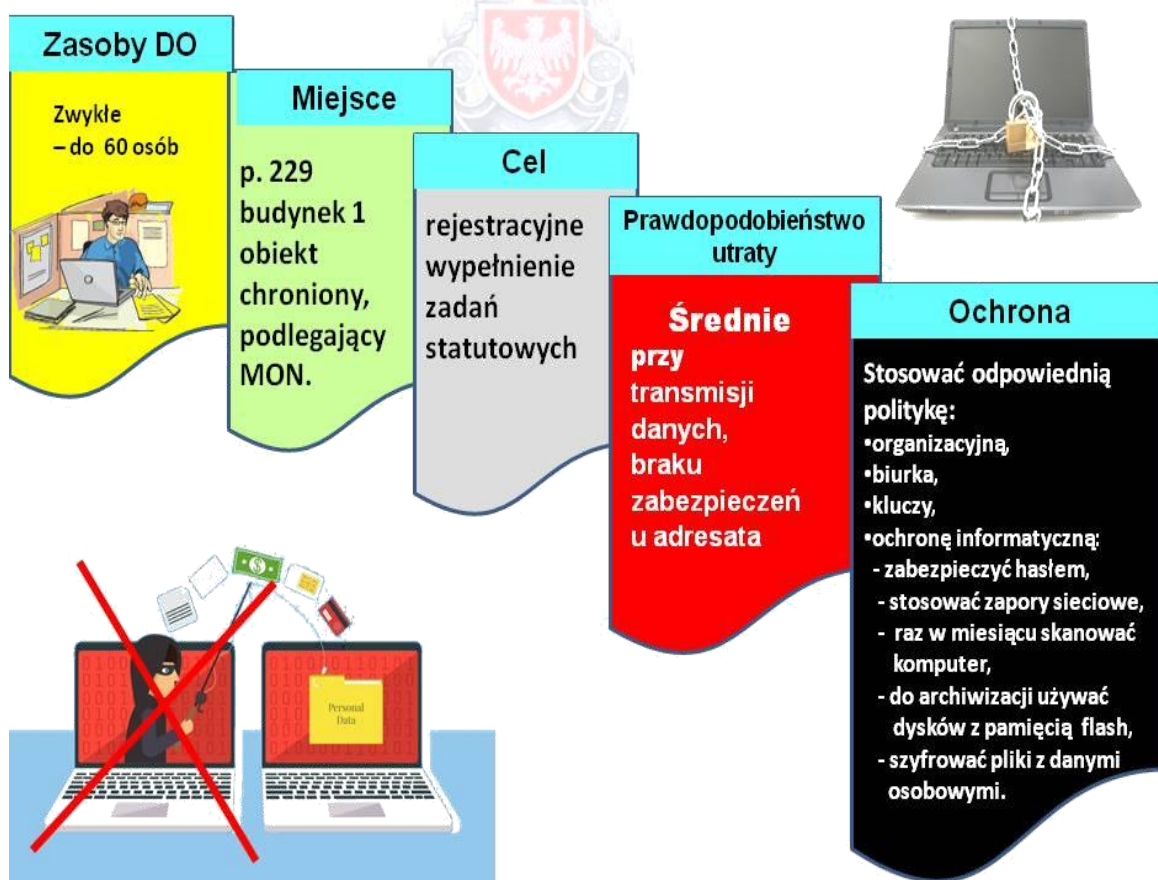
- ⊕ niski poziom wystąpienia przy korzystaniu z sieci MON;;
- ⊕ niski poziom przy wykorzystaniu arkusza rejestracyjnego;
- ⊕ średni poziom przy wykorzystaniu wirtualnej poczty,

2.1.4, Oddalenie ryzyka zdarzenia naruszającego prawa osób, których dane są przetwarzane.

- ☀ obniżono poziom ryzyka poprzez odpowiednią politykę:
 - organizacyjną,
 - biurka,
 - kluczy,
 - techniczną
- ☀ nie są przetwarzane dane wrażliwe,

21.4. Mapa ryzyka.

MAPA ZAGROZEŃ



3. Obowiązki Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji.

Administratorem Danych Osobowych (ADO) jest Federacja Stowarzyszeń Rezerwistów i Weteranów Sił Zbrojnych RP (zwana dalej Federacją).

Do najważniejszych obowiązków ADO, należy:

- 3.1. Przetwarzanie danych osobowych w kontekście działalności prowadzonej przez Federację powinno odbywać się zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
 - 3.2. Zabezpieczyć dane osobowe w ten sposób aby nie doprowadziły do identyfikacji osób fizycznych przez osoby postronne.
 - 3.3. Uzyskać zgodę, która powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwoleństwo osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia.
 - 3.4. Nadzorować przetwarzanie danych osobowych które powinno być zgodne z prawem i rzetelne. Zapewniać przejrzystość:
 - a) łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem dla osoby której dotyczą,
 - b) informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania,
 - c) należy uświadomić ryzyko, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych
 - d) określić dla osób, których dotyczą, w jakim celu są zbierane i przetwarzane
 - e) zapewnić adekwatność poprzez stosowne i ograniczone się do tego, co niezbędne do celów, dla których są one przetwarzane
 - f) zapewnić odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.
 - 3.5. Wydawanie i anulowanie upoważnień dla osób upoważnionych do przetwarzania danych osobowych;
 - 3.6. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
 - 3.7. Powołanie odpowiedzialnego za Bezpieczeństwo Informacji w miarę możliwości;
 - 3.8. Opracowanie i wdrożenie Polityki i Instrukcji (w tym zabezpieczenie zbiorów danych powierzonych do przetwarzania);
- 4. Obszarem przetwarzania danych osobowych jest budynek nr 1 pokój nr 229 przy ulicy 11 Listopada 17/19 w Warszawie.**

5. Zbiorem danych osobowych mogą być dane zwykle przy wykorzystaniu programów będących udostępnionych przez ADO i uzyskaniu zgody na przetwarzanie danych osobowych (Załącznik nr 2 i nr 2a),
Zabrania się tworzenia zbiorów i przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.
6. Zabrania się przepływu danych pomiędzy poszczególnymi systemami.
7. Wprowadza się „Rejestr czynności przetwarzania danych osobowych.” (Załącznik nr 3).
8. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:
 - 8.1 Zabezpieczenia organizacyjne (Polityka organizacyjna):
 - Ⓢ za bezpieczeństwa informacji odpowiedzialny jest Dyrektor Biura Federacji;
 - Ⓢ do przetwarzania danych dopuszczam Dyrektora Biura Federacji, Sekretarza Generalnego Federacji i I Wiceprezesa Federacji;
 - Ⓢ Dyrektor Biura obowiązany jest do zaznajomienia z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego wyżej wymienione osoby;
 - Ⓢ osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
 - Ⓢ przetwarzanie danych osobowych dokonywać w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
 - Ⓢ przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
 - 8.2 Polityka czystego biurka:
 - ◆ obowiązuje wszystkich zajmujących się zbieraniem i przetwarzaniem danych osobowych w Federacji;
 - ◆ na biurku znajdować się powinny dokumenty, które są niezbędne w danym momencie do pracy;
 - ◆ po zakończeniu pracy na dokumentach zawierającymi dane osobowe należy je zabezpieczyć w szafie (szufladzie) zamykanej na klucz;
 - ◆ dokumenty zbędne i niepodlegające archiwizacji należy niszczyć trwale.
 - 8.3 Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej (Polityka kluczy):
 - drzwi zamykać na klucz;
 - zamykać niemetalowe / metalowe szafy/;
 - dokumenty papierowe zawierające dane osobowe trwale niszczyć;

- klucze do pomieszczeń gdzie są przetwarzane dane osobowe udostępniać osobom dopuszczonym;
 - klucze zapasowe przechowywać w depozycie wyznaczonym przez administratora kompleksu;
 - wydanie kluczy może nastąpić dla osób upoważnionych w sytuacjach awaryjnych i uzasadnionych przypadkach;
 - naruszenie zasad polityki kluczy może spowodować poniesienie odpowiedzialności wynikających z art. 363 § 1. kodeksu cywilnego.
- 8.4 Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:
- ◆ dostęp do komputera/laptopa z danymi osobowymi odbywa się poprzez podanie loginu i hasła,
 - ◆ zastosowano system antywirusowy.

Instrukcja

1. Procedura nadawania uprawnień do przetwarzania danych osobowych:

- upoważnienie nadać osobie zapoznanej z zasadami ochrony danych osobowych zawartych w tym dokumencie ([Załącznik nr 4](#));
- po zapoznaniu się z zasadami ochrony podpisuje Oświadczenia o poufności ([Załącznik nr 5](#));
- Prezes Federacji nadaje wyżej wymienione upoważnienie;
- Dyrektor Biura prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie z [Załącznikiem nr 6](#).

2. Metody i środki uwierzytelnienia (polityka haseł):

- 🌐 hasła nie mogą być powszechnie używanymi słowami;
- 🌐 użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności i zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione;
- 🌐 zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom;
- 🌐 użytkownik zmienia hasło co 90 dni;
- 🌐 hasło składa się z co najmniej z 8 znaków, w tym dużych i małych liter oraz z cyfr lub znaków specjalnych.

3. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

- użytkownik loguje się do systemu/programu informatycznego przetwarzającego dane osobowe z użyciem hasła;
- użytkownik jest zobowiązany do powiadomienia ABl o próbach logowania się do systemu osoby nieupoważnionej - jeśli system to sygnalizuje;
- użytkownik jest zobowiązany do uniemożliwienia osobom nieupoważnionym

- wglądu do danych wyświetlanych na monitorach komputerowych;
- przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu;
- po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, wyłączyć sprzęt komputerowy oraz pozostawić „czyste biurko”.

4. Procedura tworzenia kopii zapasowych:

- ⊗ procedura obejmuje tworzenie kopii bezpieczeństwa;
- ⊗ kopie całościowe wykonywane są z częstotliwością 1-miesięczną;
- ⊗ kopie przyrostowe sporządzane są na pendrive lub dysku wymiennym;
- ⊗ każda kopia jest czytelnie opisana co do zawartości i daty sporządzenia;
- ⊗ kopie przechowywane są przez okres 5 lat;
- ⊗ dostęp do kopii mają osoby upoważnione;
- ⊗ kopie przechowywane są w sejfie lub w szafie zamykanej na klucz;
- ⊗ niszczenie kopii odbywa się poprzez trwałe/fizyczne zniszczenie nośnika lub nieodwracalne usunięcie danych z nośnika z użyciem specjalnego oprogramowania.

5. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków:

- typowymi nośnikami są: pendrive, przenośne twarde dyski, laptopy, dokumentacja papierowa;
- użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników po ustaniu celu ich przetwarzania;
- nośniki są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych);
- zabrania się wynoszenia poza obszar organizacji niezabezpieczonych nośników z danymi osobowymi – nośniki muszą być zaszyfrowane;
- w przypadku wysyłania danych pocztą elektroniczną, pliki muszą być opatrzone hasłem, hasło przesłane inną drogą;
- zabrania się przekazywania nośników z nieusuniętymi danymi osobowymi podmiotom lub osobom zewnętrznym (darowizny, naprawy);
- dane osobowe w postaci papierowej zabezpiecza się w wersji minimum (w szafach i biurkach zamykanych na klucz);
- zabrania się pozostawiania dokumentów i nośników, jako dostępnych dla osób postronnych
- niszczenie dokumentów i tymczasowych wydruków musi odbywać się w niszczarkach lub poprzez spalanie.

6. Procedura zabezpieczenia systemu informatycznego:

- ◆ każdy z komputerów musi być wyposażony w licencjonowany aktywny program Antywirusowy;
- ◆ każdy z komputerów (lub router dla sieci) powinien być wyposażony w firewall sprzętowy lub programowy.

7. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

- ✦ w przypadku udostępnienia danych osobowych innym podmiotom, niż na podstawie wymagań prawa, należy ten fakt odnotować;
- ✦ jeżeli system/program informatyczny na to pozwala, dane o udostępnieniu należy wprowadzić do systemu/programu. W przeciwnym wypadku należy dane te wpisać do zaprowadzonej specjalnie w tym celu Ewidencji ręcznej. **(Załącznik nr 7);**
- ✦ na żądanie osoby, której dane zostały udostępnione – informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub z ewidencji ręcznej.

8. Procedura wykonywania przeglądów i konserwacji

- ✦ prowadzone są przeglądy i konserwacje systemu informatycznego zgodnie z planem lub wytycznymi producentów;
- ✦ naprawa/konserwacja/serwis sprzętu komputerowego i programów, wykonywane przez podmiot zewnętrzny, powinny odbywać się pod ścisłym nadzorem osób upoważnionych;
- ✦ przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy trwale usunąć dane osobowe z nośników;
- ✦ aktualizację oprogramowania należy przeprowadzać zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.

Odpowiedzialność za bezpieczeństwo informacji

Z dniem 25 maja 2018 r. za bezpieczeństwo informacji odpowiedzialny jest **Dyrektor Biura Federacji Stowarzyszeń Rezerwistów i Weteranów Sił Zbrojnych RP.**

W zakresie realizacji zadań nałożonych na Administratora Danych Osobowych, podlega bezpośrednio Prezesowi Federacji.

Do zakresu jego obowiązków należą:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych;
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami polityki bezpieczeństwa informacji;
3. Wydawanie i anulowanie Upoważnień do przetwarzania danych osobowych;
4. Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych;
5. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
6. Nadzór nad bezpieczeństwem danych osobowych;
7. Kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
8. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

Ma on prawo :

1. Wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,
2. Wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
3. Żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. Żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. Żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Zgoda na przetwarzanie danych osobowych

Wyrażam zgodę na przetwarzanie moich danych osobowych zwykłych, wymienionych w tabeli, dla celów związanych z działalnością statutową przez Federacji Stowarzyszeń Rezerwistów i Weteranów Sił Zbrojnych RP – zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r./Dz. Urz. UE L 119 z 04.05.2016/ oraz Ustawą z dnia 10 maja 2018 o ochronie danych osobowych /Dz. U. poz. 1000/.

Adres do korespondencji	telefon	e-mail
----- miejsowość		-----
----- ulica		-----
----- Kod pocztowy		-----

.....
Miejscowość data

.....
Czytelny podpis

Zgodnie z art.13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. UE L 119 z 04.05.2016) informuję:

- 1) administratorem Pana danych osobowych jest Federacja Stowarzyszeń Rezerwistów i Weteranów Sił Zbrojnych RP z siedzibą w Warszawie przy ul. 11 Listopada 17/19 03-435 Warszawa blok 1 /pok. 229/;
- 2) kontakt z osobą odpowiedzialną (IOD) e-mail: antoni-borowski1950@wp.pl - (tel. 508297680);
- 3) Pana dane osobowe przetwarzane będą w celu:
 - a) adres do wejścia na teren obiektów ministerstwa Obrony Narodowej,
 - b) telefon i e-mail umożliwia kontakt Prezydium Federacji z członkami Rady Głównej Federacji.Podstawą do przekazywania danych (adres) jest Zarządzenie Dowódcy Jednostki (gospodarza obiektu) dotyczące systemu przepustowego.
- 4) odbiorcami Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa;
- 5) Pana dane osobowe przechowywane będą przez okres kadencji Rady Głównej Federacji;
- 6) posiada Pan prawo do żądania, od administratora, dostępu i sprostowania Swoich danych osobowych, usunięcia lub ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania danych, przenoszenia danych oraz prawo do cofnięcia zgody;
- 7) ma Pan prawo wniesienia skargi do organu nadrzędnego,

podanie danych osobowych wynika ze Statutu Federacji oraz Zarządzeń jednostek organizacyjnych MON, ich nie podanie może skutkować brakiem możliwości wypełniania Statutowych obowiązków Członka Rady Głównej

Rejestr czynności przetwarzania danych osobowych

Nazwa administratora danych lub podmiotu przetwarzającego/przedstawiciela administratora lub podmiotu przetwarzającego	
Współ administratorzy	
Osoba odpowiedzialna za ODO	
Cel przetwarzania	
Opis kategorii osób	
Kategorie odbiorców	
Kategorie danych osobowych	
Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	
Planowany termin usunięcia danych osobowych	
Opis technicznych i organizacyjnych środków bezpieczeństwa	

Upoważnienie do przetwarzania danych osobowych Nr

Z dniem upoważniam Panią/Panado przetwarzania danych osobowych.

Upoważnienie nadane jest celem realizacji obowiązków wynikających z realizacji powierzonych zadań Statutowych Federacji Stowarzyszeń Rezerwistów i Weteranów Sił Zbrojnych RP.

Zakres przetwarzania obejmuje: wgląd, drukowanie, wprowadzanie, modyfikację, usuwanie, archiwizację, przesyłanie, naprawę danych osobowych.

Zobowiązuję Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych, w szczególności 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) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

PREZES FEDERACJI

.....

Oświadczenie o poufności

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności 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) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji” oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”.

W szczególności zobowiązuję się do:

- ⊕ przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym Upoważnieniem;
- ⊕ zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków zadań zleconych przez Zleceniodawcę;
- ⊕ niewykorzystywania danych osobowych w celach pozastatutowych bądź niezgodnych ze zleceniem o ile nie są one jawne;
- ⊕ zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne;
- ⊕ ochrony danych osobowych przed udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane * przez ADO za naruszenie przepisów karnych 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) oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

.....
/czytelny podpis upoważnionego/

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nazwa zbioru danych (zakres upoważnienia)	Nazwisko i imię użytkownika	Identyfikator użytkownika	Rodzaj uprawnień (zakres upoważnienia)	Data nadania upoważnienia	Data ustania upoważnienia

Legenda: Uprawnienia: (WG) wgląd, (W) wprowadzanie, (M) modyfikacja, (U) usuwanie, (A) archiwizacja, (D) drukowanie (N) naprawę danych osobowych, (P) przesyłanie.

**Ewidencja udostępnienia danych**

Data udostępnienia danych	Nazwa i adres podmiotu, któremu dane udostępniono dane	podstawa prawna udostępnienia danych	Zakres udostępnionych danych

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Zbiór danych	Forma	System inf. (lub ND w przypadku wersji tekstowej)	Komórka organizacyjna
1	Baza danych członków Rady Głównej Federacji - adresy, telefony, e-mail	E+T	Word	Biuro Federacji
2	Baza danych członków Prezydium Rady Głównej Federacji - adresy, telefony, e-mail			
3	Baza danych osób wyjeżdżających za granicę			
4	Wnioski o mianowania, odznaczenia.			
5	Adresy, telefony i e-mail do komórek resortu MON.			
6	Życiorysy, CV			
7	Wykazy związane z działalnością statutową: Komisja Rewizyjna Kapituła HOO			

Legenda:

E – elektroniczna, T – tekstowa