ZWIĄZEK ŻOŁNIERZY WOJSKA POLSKIEGO
ZARZĄD GŁÓWNY

POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH
w ZWIĄZKU ŻOŁNIERZY WOJSKA POLSKIEGO

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.

1. Wprowadzenie

Niniejszy dokument opisuje reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w Związku Żołnierzy Wojska Polskiego – zwanego dalej Związkiem.

Opisane reguły określają granice dopuszczalnego zachowania wszystkich osób upoważnionych oraz użytkowników systemów informatycznych wspomagających pracę Związku

Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

Dokument „Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Związku Żołnierzy Wojska Polskiego" – zwany dalej: „Polityką bezpieczeństwa", lub „Dokumentem", wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczony dla osób pracujących przy przetwarzaniu danych osobowych w Związku.

2. Stosowane pojęcia

1) **polityka bezpieczeństwa (dokument)** – polityka bezpieczeństwa w zakresie ochrony danych osobowych w Związku Żołnierzy Wojska Polskiego,
2) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) **osoba możliwa do zidentyfikowania** - osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne,
4) **zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
5) **administrator danych** – Zarząd Główny, Zarząd Wojewódzki (Rejonowy), Zarząd Koła Związku Żołnierzy Wojska Polskiego- zwane dalej „Zarządem",
6) **prezes zarządu** – Prezes Związku, prezes zarządu wojewódzkiego (rejonowego) oraz koła,
7) **osoba upoważniona** – pracownik, członek zarządu, wolontariusz, osoba posiadająca pisemne upoważnienie do przetwarzania danych nadane przez administratora danych,
8) **przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

9) **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,

10) **zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,

11) **usuwanie danych** – zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

12) **zgoda osoby, której dane dotyczą** – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli innej treści,

13) **odbiorca danych -** każdy, komu udostępnia się dane osobowe, z wyłączeniem:

a) osoby, której dane dotyczą,

b) osoby upoważnionej do przetwarzania danych,

c) podmiotu, któremu administrator powierzył przetwarzanie danych na podstawie umowy zawartej na piśmie,

d) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

14) **ustawa -** ustawa z dnia 24 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. Nr 1000) oraz odpowiednio ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tj. Dz.U. z 2016 r. poz. 922) w zakresie obowiązującym.[1]

II. POLITYKA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH.

1. Dane osobowe przetwarzane są w siedzibach zarządów.
2. Za właściwe zabezpieczenie danych osobowych odpowiadają osoby upoważnione do przetwarzania danych osobowych.
3. W Związku przetwarzane są dane:
   1) członków Związku,
   2) pracowników,
   3) wolontariuszy,
   4) darczyńców,
   5) osób zwracających się do Związku w prośbami i wnioskami.
4. Dane członków Związku przetwarzane są w formie papierowej oraz elektronicznej i obejmują w szczególności:
   1) imię, nazwisko, imię ojca;
   2) datę i miejsce urodzenia;
   3) pełny adres zamieszkania;
   4) numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej;

[1] Z ustawy z dnia 29 sierpnia 1997 r. zachowują moc obowiązującą przepisy art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7.

5) posiadane odznaczenia;
6) przebieg służby wojskowej.

5. Dane pracowników 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;
   5) numer telefonu stacjonarnego i/lub komórkowego i/lub adres poczty elektronicznej;
   6) numer rachunku bankowego;
6. Dane osobowe wolontariuszy współpracujących ze Związkiem przetwarzane są w formie papierowej oraz 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.
7. Dane osobowe darczyńców Związku 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).
8. Zbiory danych tworzone są w programach pakietu MS Office lub pakietów równorzędnych (Libre Office, Open Office).
9. Strukturę zbiorów danych określa administrator danych określając w zależności od potrzeb:
   1) nazwę zbioru danych (np. deklaracje członkowskie i karty ewidencyjne, wnioski o udzielenie wyróżnień związkowych, resortowych i państwowych, wnioski o mianowanie);
   2) formę prowadzenia dokumentacji zbioru danych (papierowa, elektroniczna lub papierowo-elektroniczna);

10. Dane osobowe przetwarzane są przy użyciu edytora tekstu (MS Word), arkusza kalkulacyjnego (MS Excel) lub programów równorzędnych (np. pakiet Open Office) i innych dostępnych programów do tworzenia baz danych.
11. 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) wyższych instancji Związku, przez struktury organizacyjne szczebla niższego.
12. Dane z podmiotami wymienionymi w ppkt. 1 – 7 przesyłane są teletransmisyjnie za pośrednictwem Internetu oraz w formie papierowej.
13. Przelewy bankowe realizowane są za pośrednictwem Internetu lub przekazów pocztowych.

III. ŚRODKI ORGANIZACYJNE

1. Za wdrożenie zasad polityki bezpieczeństwa odpowiada prezes zarządu lub osoba przez niego upoważniona.
2. Osobami upoważnionymi do przetwarzania danych osobowych na szczeblu zarządu upoważnieni są:
    1) prezes;
    2) wiceprezesi;
    3) sekretarz;
    4) skarbnik;
    5) inne osoby posiadające pisemne upoważnienie wydane przez prezesa.
3. Dla potrzeb ochrony danych osobowych przetwarzanych w Związku w formie papierowej stosuje się, w zależności od możliwości, zabezpieczenia polegające na przechowywaniu:
    1) dokumentacji bieżącej – np. w szafach zamykanych na zamki lub kłódki w obszarach przetwarzania danych osobowych,
    2) dokumentacji archiwalnej i dokumentacji pracowniczej – np. w specjalnie do tego celu przeznaczonym pomieszczeniu.
4. Dostęp do danych osobowych przetwarzanych w systemach informatycznych (na komputerach) chroniony jest poprzez:

1) zastosowanie identyfikatorów użytkowników (loginów) i haseł uniemożliwiających nieuprawnione korzystanie osobom nieupoważnionym;
2) ustawienie monitorów komputerów w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

5. Loginy i hasła umożliwiające dostęp do komputerów znajdują się w zapieczętowanych kopertach przechowywanych w bezpiecznym miejscu.
6. W razie wystąpienia konieczności uzyskania dostępu do któregoś z komputerów w czasie nieobecności pracownika użytkującego komputer, osoba upoważniona przez prezesa może otworzyć zapieczętowaną kopertę i umożliwić wykonanie niezbędnych czynności innemu pracownikowi. Po powrocie pracownika użytkującego dany komputer hasło dostępu powinno zostać zmienione.
7. Dla potrzeb ochrony danych osobowych przetwarzanych w edytorach tekstu (MS Word), arkuszach kalkulacyjnych (MS Excel) lub programach równorzędnych (np. pakiet Libre Office) i innych programach do tworzenia baz danych do ochrony systemu informatycznego należy stosować systemy antywirusowe.
8. Elektroniczne przetwarzanie danych osobowych odbywa się na komputerach stacjonarnych oraz laptopach. Dla zminimalizowania ryzyka dostania się ich zawartości w niepowołane ręce komputery zabezpiecza się hasłami, a władze zarządów należy zapoznać z „Polityką bezpieczeństwa" i przeszkolić w zakresie ochrony danych osobowych.
9. Poza przypadkami uzasadnionymi przepisami prawa w Związku nie przetwarza się danych o stanie zdrowia, wynikach badań lekarskich, badań pochorobowych, o pochodzeniu rasowym i etnicznym, a także o wyznaniu.
10. Każdej osobie wymienionej w pkt. II.3 przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych przetwarzanych przez Związek, a zwłaszcza prawo do:
    1) uzyskania wyczerpującej informacji, czy taki zbiór istnieje oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy;
    2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
    3) uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące oraz podania w powszechnie zrozumiałej formie treści tych danych;
    4) uzyskania informacji o źródle danych, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany do zachowania w tym zakresie tajemnicy wynikającej z odrębnych przepisów,
    5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
    6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
11. Dane osobowe udostępnia się na pisemny, umotywowany wniosek. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych

osobowych oraz wskazywać ich zakres i przeznaczenie. Udostępnione dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

12. Związek może na podstawie umowy zawartej w formie pisemnej powierzyć podmiotowi zewnętrznemu przetwarzanie danych osobowych w realizowanym przez siebie zadaniu.

IV. OPIS ZDARZEŃ NARUSZAJACYCH OCHRONĘ DANYCH OSOBOWYCH

1. Podział zagrożeń:

   1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia sprzętu komputerowego – ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
   2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
   3) zagrożenia zamierzone, świadome i celowe – najpoważniejsze zagrożenia naruszenia poufności danych – zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy;
   4) Zagrożenia te możemy podzielić na:
      a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
      b) nieuprawniony dostęp do systemu z jego wnętrza,
      c) nieuprawniony przekaz danych,
      d) pogorszenie jakości sprzętu i oprogramowania,
      e) bezpośrednie zagrożenie materialnych składników systemu.

2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, niepożądana ingerencja ekipy remontowej itp.;

   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;

   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż;

   4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

   5) pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

7) stwierdzona próba modyfikacji lub modyfikacja danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

8) niedopuszczalna manipulacja danymi osobowymi w systemie;

9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

10) nieprzypadkowe odstępstwa od zasad bezpieczeństwa pracy w systemie lub sieci komputerowej wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;

11) podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia, jak również skasowanie lub skopiowanie w sposób niedozwolony danych osobowych;

12) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych itp.).

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej itp.

V. ZABEZPIECZENIE DANYCH OSOBOWYCH.

1. Administratorem danych osobowych zawartych i przetwarzanych w rejestrach zbiorów danych Związku Żołnierzy Wojska Polskiego jest odpowiednio do szczebla organizacyjnego Zarząd Główny, Zarząd Wojewódzki (Rejonowy), Zarząd Koła Związku Żołnierzy Wojska Polskiego.
2. Administrator danych osobowych jest obowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych i na nośnikach tradycyjnych, a w szczególności do:

   1) zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym;

   2) zapobiegania kradzieży danych;

   3) zapobiegania przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

3. W zależności od możliwości, do zastosowanych środków technicznych należy:

   1) przetwarzanie danych osobowych w wydzielonych, odpowiednio zabezpieczonych i przystosowanych do tego pomieszczeniach;

   2) zabezpieczenie wejścia do pomieszczeń, o których mowa w pkt 1;

3) wyposażenie pomieszczeń w szafy dające gwarancję bezpieczeństwa dokumentacji i nośników danych.

4. Do zastosowanych środków organizacyjnych należą następujące zasady:
   1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed jej przystąpieniem do pracy przy przetwarzaniu danych osobowych;
   2) przeszkolenie osób, o których mowa w pkt 1, w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych;
   3) kontrolowanie otwierania i zamykania pomieszczeń wymienionych w pkt 3.1, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianiu pomieszczenia w czasie pracy bez nadzoru.
5. Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie, przy czym dokumenty te nie mogą być sprzeczne z regulacjami określonymi w „Polityce bezpieczeństwa".

V. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. W przypadku stwierdzenia :
   1) naruszenia zabezpieczeń systemu informatycznego;
   2) naruszenia technicznego stanu urządzeń;
   3) naruszenia zawartości zbioru danych osobowych;
   4) ujawnienia metody pracy lub sposobu działania programu;
   5) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych;
   6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.),

   każda osoba zatrudniona przy przetwarzaniu danych osobowych jest zobowiązana niezwłocznie powiadomić o tym prezesa zarządu.

2. Do czasu przybycia na miejsce naruszenia danych osobowych prezesa zarządu lub upoważnionej przez niego osoby, należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia danych osobowych;
   2) udokumentować wstępnie zaistniałe naruszenie;
   3) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.
3. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych, prezes zarządu lub osoba przez niego upoważniona:

1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy;
2) może żądać dokładnej relacji z zaistniałego naruszenia lub ujawnienia ochrony danych osobowych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) nawiązuje bezpośredni kontakt – jeżeli zachodzi taka potrzeba – ze specjalistami spoza Związku.

4. Po wyczerpaniu niezbędnych środków doraźnych związanych z zaistniałym naruszeniem/ujawnieniem ochrony danych osobowych, prezes zarządu zasięga niezbędnych opinii i proponuje postępowanie naprawcze, w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
5. Prezes zarządu zarządza udokumentowanie zaistniałego przypadku naruszenia lub ujawnienia ochrony danych osobowych oraz sporządzenie raport, który powinien zawierać w szczególności:
   1) wskazanie osoby powiadamiającej oraz innych osób zaangażowanych lub odpytywanych w związku z naruszeniem lub ujawnieniem ochrony danych osobowych;
   2) określenie czasu i miejsca: naruszenia/ujawnienia i powiadomienia o tym fakcie;
   3) określenie okoliczności towarzyszących i rodzaju naruszenia/ujawnienia;
   4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
   5) wstępną ocenę przyczyn wystąpienia naruszenia/ujawnienia;
   6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

VI. **POSTANOWIENIA KOŃCOWE**

1. Osoby przetwarzające dane osobowe składają oświadczenie o zapoznaniu się z Polityką bezpieczeństwa.
2. W zarządzie prowadzi się ewidencję osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych.
3. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie.
4. Orzeczona kara wobec osoby uchylającej się od powiadomienia Administratora Danych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 24 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. Nr 1000) oraz możliwości wniesienia wobec niej przez Związek sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.
5. Wszystkie regulacje dotyczące systemów informatycznych określone w „Polityce bezpieczeństwa” dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.

6. Wdrożenie „Polityki bezpieczeństwa” odbywa się poprzez:
   a) zapoznanie osób wchodzących w skład organów Związku, pracowników, wolontariuszy, z treścią „Polityki bezpieczeństwa”;
   b) szkolenia z zakresu ochrony danych osobowych.
7. „Polityka bezpieczeństwa” wchodzi w życie w terminie określonym w treści uchwały. Prezydium Zarządu Głównego
8. Zmiany w „Polityce bezpieczeństwa” będą wchodzić w życie w terminach określonych w uchwałach Prezydium Zarządu Głównego dotyczących wprowadzenia zmian w dokumencie.

Załączniki- Instrukcja dla osób upoważnionych do przetwarzania danych osobowych.

Załącznik do „Polityki bezpieczeństwa
w zakresie ochrony danych osobowych
w Związku Żołnierzy Wojska Polskiego

INSTRUKCJA DLA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Niniejsza „Instrukcja dla osób upoważnionych do przetwarzania danych osobowych" – zwana dalej „Instrukcją" – określa tryb postępowania w przypadku, gdy:

1) stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie.
2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 2

Osoba upoważniona do przetwarzania danych zobowiązana jest do:

1) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych;
2) zachowania szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesu osób, których dane dotyczą;
3) stosowania określonych przez Administratora Danych procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
4) podporządkowania się poleceniom Administratora Danych w zakresie ochrony danych osobowych;
5) zachowania danych osobowych w tajemnicy;
6) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, a w szczególności:
   a) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem.
   b) zabezpieczenia danych osobowych przed ich zmianą.
   c) zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym.
   d) zamykania i zabezpieczania pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
   e) dopilnowania, by przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej.
   f) dopilnowania, by przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie.
   g) przetwarzania danych osobowych zgodnie z celem, dla którego zostały zebrane.

§ 3

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez prezesa zarządu.
2. Prezes zarządu ponosi odpowiedzialność za zaznajomienie osoby upoważnionej , która ma być dopuszczona do przetwarzania danych osobowych z przepisami towarzyszącymi ochronie danych osobowych. Fakt zapoznania się z przepisami osoba upoważniona potwierdza własnoręcznym podpisem.
3. Każda osoba upoważniona powinna odbyć szkolenie z zakresu ochrony danych osobowych.
4. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest
5. w formie papierowej i/lub elektronicznej.
6. W przypadku stwierdzenia naruszenia zasad postępowania przy przetwarzaniu danych osobowych lub naruszeniu zabezpieczenia danych osoba upoważniona zobowiązana jest niezwłocznie poinformować prezesa zarządu.

§ 4

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to głównie:

1. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.
2. Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.
3. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż.
4. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.
6. Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7. Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8. Nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie.
9. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń.
10. Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.

11. Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.
12. Podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane osobowe.
13. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

§ 5

1. Każda osoba w Związku (reprezentująca organ Związku bądź w niej zatrudniona lub współpracująca - włącznie z wolontariuszami), która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób, powinna niezwłocznie poinformować o tym osobę zatrudnioną przy przetwarzaniu tych danych, bezpośredniego przełożonego albo inną upoważnioną przez niego osobę.
2. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych zobowiązana jest niezwłocznie powiadomić o tym prezesa zarządu.

§ 6

1. Dane osobowe zostają ujawnione, gdy stają się znane w całości lub części pozwalającej na określenie osobom nieuprawnionym tożsamości osoby, której dane dotyczą.
2. W stosunku do danych, które zostały zagubione, pozostawione bez nadzoru poza obszarem bezpieczeństwa – należy przeprowadzić postępowanie wyjaśniające czy dane osobowe należy uznać za ujawnione.

§ 7

Niezwłocznie po uzyskaniu informacji o naruszeniu danych osobowych należy podjąć działania w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane poprzez:

1. Fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej.
2. Wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych.
3. Zmianę hasła na konto użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
4. Podjęcie innych – stosownych do zagrożenia – działań.

§ 8

Po uzyskaniu sygnału o naruszeniu danych osobowych – można w pierwszej kolejności, w zależności od kwalifikacji personelu podjąć następujące działania:

1. Zapisać wszelkie informacje związane z danym zdarzeniem.
2. Na bieżąco wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia.
3. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia – zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieuprawnionej.
4. Wyniki postępowania zabezpieczającego oraz okoliczności naruszenia bezpieczeństwa danych osobowych należy ująć w raporcie i niezwłocznie przekazać prezesowi zarządu.

§ 9

1. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych prezesa zarządu lub upoważnionej przez niego osoby należy:
   1) niezwłocznie podjąć czynności (określone w rozdziale V niniejszej „Polityki bezpieczeństwa") niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia – o ile istnieje taka możliwość – a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
   4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych – stosownie do objawów i komunikatów towarzyszących naruszeniu;
   5) podjąć stosowne działania – jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
   6) zastosować się do innych instrukcji i regulaminów – jeżeli odnoszą się one do zaistniałego przypadku;
   7) udokumentować wstępnie zaistniałe naruszenie;
   8) nie opuszczać – bez uzasadnionej potrzeby – miejsca zdarzenia do czasu przybycia prezesa zarządu lub upoważnionej przez niego osoby.
2. Po przybyciu na miejsce naruszenia lub ujawnienia ochrony danych osobowych prezes zarządu lub osoba go zastępująca:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy jednostki organizacyjnej Związku;
   2) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   3) jeżeli zachodzi taka potrzeba – zwraca się o pomoc specjalistów spoza Związku.

§ 10

1. Po dokonaniu czynności zabezpieczenia danych osobowych i ustaleniu przyczyn naruszenia ochrony danych osobowych należy niezwłocznie przywrócić normalny stan działania.
2. Po przywróceniu prawidłowego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
3. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych prezes zarządu niezwłocznie zarządza przeprowadzenie dodatkowego szkolenia dla osób biorących udział przy przetwarzaniu danych osobowych. Dokumentację z przeprowadzonego szkolenia załącza się do raportu określonego w treści § 11.

§ 11

1. Po dokonaniu czynności przedstawionych powyżej sporządza się szczegółowy raport zawierający:
   1) opis zdarzenia;
   2) przyczynę zaistnienia;
   3) skutki naruszenia ochrony danych osobowych;
   4) podjęte działania, zastosowane środki;
   5) analizę zdarzenia oraz wnioski dotyczące przedsięwzięć:
      a) organizacyjnych,
      b) technicznych,
      c) kadrowych.
2. Raport przedkłada niezwłocznie prezesowi zarządu, który wydaje pisemne zalecenia.
3. Całość dokumentacji w zakresie naruszenia systemu ochrony danych osobowych przechowuje się w zarządzie.
4. O przypadku naruszenia zasad ochrony danych osobowych informuje się Prezesa Związku lub Sekretarza Generalnego Zarządu Głównego.
5. Wnioski z analizy przypadku naruszenia zasad ochrony danych osobowych Prezes Związku lub Sekretarz Generalny przesyła do zarządów wojewódzkich (rejonowych), które przesyłają je do podległych kół.