Regulamin Ochrony Danych Osobowych

w Polskim Związku Krótkofalowców

Na podstawie Par 20 ust. 3 lit. J Statutu PZK, Zarząd Główny PZK uchwala co następuje:

Rozdział I.

Postanowienia ogólne.

1. Nadzór całościowy/ogólny nad systemem RODO w PZK pełni Prezes PZK
2. Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych PZK zgodnie z przepisami RODO dla:
   - Członków Prezydium Zarządu Głównego Polskiego Związku Krótkofalowców,
   - Członków Głównej Komisji Rewizyjnej Polskiego Związku Krótkofalowców w zakresie uprawnień kontrolnych,
   - Administratora SI Polskiego Związku Krótkofalowców,
   - Upoważnionych Członków Zarządów Oddziałów Terenowych Polskiego Związku Krótkofalowców,
   - Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych PZK przetwarzanych przez Podmiot przetwarzający,
   - Użytkowników systemów informatycznych z dostępem do danych osobowych dostępnych na serwerach PZK

3. Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

Ochrona danych osobowych odbywa się na dwóch poziomach ewidencji danych osobowych PZK:
1. Ochrona danych osobowych w wersji elektronicznej na poziomie Centrali PZK obejmuje systemy elektroniczne ewidencji członków PZK – [OSEC] zainstalowane na serwerze PZK.
2. Ochrona danych osobowych w wersji papierowej na poziomie Centrali PZK obejmuje:
   - Deklaracje członkowskie,
   - Karty informacyjne członków,
   - Zgody opiekunów prawnych,

przekazane przez Oddziały Terenowe PZK do Działu centralnej dokumentacji członkowskiej PZK.
3. Ochrona danych osobowych na poziomie OT PZK obejmuje ewidencję członków PZK w wersji elektronicznej, prowadzoną przez osoby uprawnione. Dokumentacja papierowa, przyjmowana w Oddziale Terenowym PZK – Deklaracje członkowskie, Karty Informacyjne członków, zgody opiekunów prawnych - po wprowadzaniu danych osobowych członków PZK do systemu ewidencji elektronicznej członków PZK, przekazywana jest do Centrali PZK zgodnie z Regulaminem ODO PZK.
4. Ochrona danych osobowych odbywa się na dwóch poziomach ewidencji danych osobowych PZK:
   a/ Ochrona danych osobowych na poziomie Centrali PZK obejmuje systemy elektroniczne ewidencji członków PZK – [OSEC] zainstalowane na serwerze PZK
   b/ Ochrona danych osobowych na poziomie OT PZK obejmuje ewidencję członków PZK w wersji dokumentacji papierowej – Deklaracje członkowskie, Karty Informacyjne członków, zgody opiekunów prawnych, oraz wprowadzanie danych osobowych członków PZK z dokumentacji papierowej do systemu ewidencji elektronicznej członków PZK [OSEC].
6. Nad całością spraw ochrony danych osobowych, nadzór pełni Inspektor Ochrony Danych Osobowych PZK [IODO PZK].
7. Inspektora ODO PZK powołuje i odwołuje Prezydium ZG PZK.

Rozdział II

Inspektor Ochrony Danych Osobowych
PZK

1. IOD PZK pomaga Prezesowi PZK oraz podmiotowi przetwarzającemu dane PZK we wszystkich kwestiach związanych z ochroną danych osobowych.

2. W szczególności obowiązkiem IOD jest:

- informowanie i doradzanie Prezesowi PZK oraz podmiotowi przetwarzającemu dane osobowe PZK, jak również ich pracownikom, w zakresie ich obowiązków wynikających z przepisów prawa o ochronie danych,
- monitorowanie zgodności funkcjonowania organizacji z wszystkimi przepisami prawa dotyczącego ochrony danych, w tym audyty, działania podnoszące świadomość, a także szkolenia dla personelu zajmującego się przetwarzaniem danych,
- udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- pełnienie funkcji punktu kontaktowego dla osób fizycznych składających wnioski i żądania dotyczące przetwarzania ich danych osobowych i wykonywania ich praw,
- współpraca z organami ochrony danych i pełnienie funkcji punktu kontaktowego dla organów ochrony danych w kwestiach związanych z przetwarzaniem.

3. IOD musi być niezwłocznie włączany we wszystkie sprawy organizacji dotyczące ochrony danych osobowych.

4. IOD nie może otrzymywać od administratora ani podmiotu przetwarzającego dane instrukcji dotyczących wykonywania swoich zadań.

5. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

6. IOD bezpośrednio podlega Prezesowi PZK.

Rozdział III

ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnione osoby Zarządów Oddziałów Terenowych PZK są zobowiązane do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach zabezpieczonych przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnione osoby Zarządów Oddziałów Terenowych PZK zobowiązane są do niszczenia zbędnych dokumentów i wydruków obejmujących dane osobowe członków PZK w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza siedzibą biura Oddziału Terenowego PZK.

4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich.

ROZDZIAŁ IV

ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, PROGRAMÓW

1. Dostęp do danych osobowych PZK w systemie elektronicznym ewidencji członków PZK [OSEC] odbywa się przez stronę https://pzk.org.pl dla upoważnionych użytkowników przez przydzielone loginy i hasła dostępu w zakresie udzielonych zgód na przetwarzanie danych osobowych.
2. W przypadku, gdy upoważniona osoba przetwarzająca dane osobowe korzysta ze sprzętu IT zobowiązana jest do jego zabezpieczenia przed niepowołanym dostępem osób trzecich za pomocą loginów i haseł. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, tablety i smartfony itp.
3. Upoważniona osoba jest zobowiązana zgłosić zagubienie, utratę Sprzętu IT używanego do przetwarzania danych osobowych PZK członkom Prezydium ZG PZK i Administratorowi SI PZK.
4. Upoważniona osoba jest zobowiązana do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów)
5. Jeśli upoważniona osoba jest uprawniona do niszczenia nośników, powinna TRWALE zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, mechaniczne zniszczenie twardego dysku, pendrive) / Jeśli nie, to uprawniona osoba jest zobowiązana do przekazania Administratorowi SI PZK nośników przeznaczonych do zniszczenia
6. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych
7. Dyski wewnętrzne komputerów zawierające dane osobowy muszą być szyfrowane za pomocą odpowiednich programów.

ROZDZIAŁ V

ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Upoważniona osoba musi posiadać swój własny indywidualny identyfikator (login) do logowania się w systemie ewidencji członków PZK - OSEC
2. Nadawanie uprawnień dla upoważnionych osób odbywa się na polecenie członka Prezydium ZG PZK nadzorującego systemem ewidencji elektronicznej PZK wykonywane przez Administratora SI PZK lub członka Prezydium ZG PZK nadzorującego system ewidencji elektronicznej PZK.
3. Upoważniona osoba musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie tej upoważnionej osoby.
4. Upoważniona osoba jest zobowiązana do powiadomienia Administratora SI PZK o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
5. W przypadku, gdy upoważniona osoba podczas próby zalogowania się zablokuje system, zobowiązana jest powiadomić o tym Administratora SI PZK
6. Upoważniona osoba jest zobowiązana do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu**

7. Przed czasowym opuszczeniem stanowiska pracy, upoważniona osoba zobowiązana jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
8. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy

ROZDZIAŁ VI

POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8/12 znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić
6. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła
7. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności
9. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym organizacji
10. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
11. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

Rozdział VII

ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA PZK

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Prezesa PZK/osoby z Prezydium ZG PZK nadzorującej systemy ewidencji elektronicznej danych osobowych członków PZK. Do takich nośników zalicz się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zabezpieczone hasłem pliki)

3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce
    b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą
    c. stosować bezpieczne koperty depozytowe
    d. przesyłkę należy przesyłać przez kuriera

ROZDZIAŁ VIII

ZASADY KORZYSTANIA Z INTERNETU

1. Upoważniona osoba przy przetwarzaniu danych osobowych PZK zobowiązana jest do korzystania z internetu wyłącznie przy połączeniu ze stroną https://pzk.org.pl .
2. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą ”https:”. Dla pewności należy „kliknąć” na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel
3. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie dotyczy to żądania podania takich informacji przez rzekomy bank.
4. W przypadku przetwarzania danych osobowych członków PZK nie można posługiwać się sieciami otwartymi typu hotspot, a używane technologie połączenia z internetem muszą być bezpieczne i szyfrowane.

ROZDZIAŁ IX

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Upoważnione Osoby muszą posługiwać się adresem skrzynki mailowej poczty z serwera PZK – SP0XXX@pzk.org.pl .
2. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione
3. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zabezpieczone hasłem, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS
4. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum (np. 12) znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em
5. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu
6. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata

7. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH
8. **WAŻNE:** Nie wolno „klikać” na hyperlinki w mailach, gdyż mogą to być hyperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hyperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH
9. Należy zgłaszać Administratorowi SI PZK przypadki podejrzanych e-maili
10. Użytkownicy nie powinni rozsyłać „niezawodowych” e-maili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”. Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”!
12. Użytkownicy powinni okresowo kasować niepotrzebne maile
13. Konta pocztowe służbowe muszą być odseparowane od poczty prywatnej.
14. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych
15. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób
16. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
17. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
18. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
19. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego
20. Upoważnieni Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania
21. Upoważniony Użytkownik bez zgody Prezesa PZK nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące członków PZK za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej

ROZDZIAŁ X

OCHRONA ANTYWIRUSOWA

1. Upoważnieni Użytkownicy powinni w swoich komputerach posiadać zainstalowany program antywirusowy.
2. Upoważnieni Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada
3. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe
4. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy”, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Administratora SI lub członka Prezydium ZG PZK nadzorującego elektroniczny system ewidencji członków.

ROZDZIAŁ XI

SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Prezesa PZK oraz Inspektora ODO PZK w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. dokumentacja jest niszczona bez użycia niszczarki,
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy,
    g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    h. telefoniczne próby wyłudzenia danych osobowych,
    i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drive z danymi osobowymi,
    j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
    k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    l. hasła do systemów przyklejone są w pobliżu komputera.

ROZDZIAŁ XII

OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Prezesa PZK zadaniach
b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Prezesa PZK
c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Prezesa PZK
d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania danych odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania organizacji, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta organizacja, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

ROZDZIAŁ XIII

POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Regulamin zatwierdzony Uchwałą Nr 701/01/23 w dniu 21.05.2023r.