Uchwała nr 63/I/2018

Komendy Hufca ZHP Jaworzno z dnia 7 czerwca 2018 r..

w sprawie przyjęcia Regulaminu ochrony danych osobowych w Hufcu Jaworzno

§ 1. Komenda Hufca ZHP Jaworzno przyjmuje Regulamin ochrony danych osobowych w Hufcu Jaworzno, stanowiący załącznik do niniejszej uchwały.

§ 2. Zobowiązuje się wszystkich drużynowych i instruktorów hufca do zapoznania się i stosowania Regulaminu ochrony danych osobowych w Hufcu Jaworzno, regulaminów ZHP oraz powszechnie obowiązujących przepisów prawa w zakresie ochrony danych osobowych.

- hm. Kinga Jędrzejek …….
- hm. Marta Jewuła …….
- phm. Magdalena Mika …….
- hm. Paweł Duda …….
- phm. Karina Gaj-Woźniak …….
- hm. Robert Duda …….
- hm. Renata Frankowicz …….

Regulamin Ochrony Danych Osobowych w Hufcu Jaworzno Związku Harcerstwa Polskiego

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Instruktorów Hufca
- Osób pełniących funkcje instruktorskie w Hufcu,
- Wolontariuszy
- Stażystów
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

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

SPIS TREŚCI

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, urządzeń biurowych, tabletów i smartfonów).
2. Demontaż, instalowanie lub podłączanie dodatkowych urządzeń jest dopuszczalne wyłącznie za zgodą komendanta lub skarbnika hufca.
3. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione. Dokumenty zawierające dane osobowe mogą być przechowywane wyłącznie w zabezpieczonych folderach.
4. Użytkownik jest zobowiązany do przekazania komendantowi nośników przeznaczonych do zniszczenia.

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy z zachowaniem ochrony danych osobowych, najlepiej na własnym koncie pocztowym w domenie ZHP.
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim komputerze.
3. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu.**
5. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu (**WINDOWS + L**) lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8 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.
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. Hasła muszą być zmieniane co 90 dni
7. Użytkownik zobowiązany jest do samodzielnej zmiany hasła

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Osoby posiadające dostęp do danych osobowych, na zasadach obowiązujących w ZHP, są zobowiązane do stosowania tzw. „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych.

2. Zbędne dokumenty zawierające dane osobowe należy niszczyć w niszczarkach.
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych, w szczególności w harcówce Hufca.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.

5 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA ORGANIZACJĘ

1. Użytkownicy nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash).
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.

6 ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się instalowania programów z Internetu bez konsultacji z członkiem zespołu IT.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie.
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem do pobrania oraz na hackerskie.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Pliki z danymi osobowymi w Wordzie, Excelu, w Pdf lub spakowane (7zip), przed wysłaniem ich do osób trzecich powinny być zahasłowane, a hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. **WAŻNE:** Nie otwierać załączników (.zip, .rar, .xlsm, .pdf, .exe) od nieznanych nadawców, które mogą zainfekować komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.
5. **WAŻNE:** Nie wolno „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink może zainfekować komputer oraz inne komputery w sieci. WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.
6. Należy zgłaszać członkowi zespołu IT przypadki podejrzanych e-maili.
7. Użytkownicy nie powinni rozsyłać emaili w formie „łańcuszków szczęścia"
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „**Ukryte do wiadomości – UDW**”. Rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości” może być stosowane wyłącznie w przypadku osób, których adresy mailowe są upublicznione na stronie hufca (np. komendant@jaworzno.zhp.pl).
9. Użytkownicy powinni okresowo kasować niepotrzebne maile.
10. Użytkownik bez zgody Komendanta Hufca nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Hufca, jego członków, współpracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Komendanta / Instruktora ds. Ewidencji 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 (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 wskazują 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 pozwala na wgląd osób postronnych w dane osobowe,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Komendanta,
    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 lub hasła,
    k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
    l. hasła do systemów przyklejone są w pobliżu komputera .

9 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań,
    b. zachowania w tajemnicy danych osobowych do których ma dostęp,
    c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań,
    d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
2. 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.

3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

10 POSTĘPOWANIE DYSCYPLINARNE

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