Procedura RODO dla instruktorów ZHP

Wytyczne dotyczące przetwarzania danych osobowych przeznaczone dla instruktorów i innych osób działających z upoważnienia ZHP i mających dostęp do danych osobowych

Instruktorki, Instruktorzy!

Skuteczna ochrona danych osobowych w ZHP jest niemożliwa bez Waszego zaangażowania, opartego na świadomości podstawowych zagadnień dotyczących postępowania z danymi osobowymi.

Oddajemy w Wasze ręce niniejsze wytyczne, polecając wnikliwe zapoznanie się z nimi oraz stosowanie się do nich w codziennej służbie instruktorskiej. Poniżej zamieszczamy krótką listę umiejętności, które powinien posiąść każdy instruktor. Z jej pomocą możecie dokonać samooceny i określić kierunki samokształcenia w zakresie ochrony danych osobowych.

Instruktor:

- Wie, czym są dane osobowe i ich przetwarzanie, oraz potrafi zidentyfikować operacje przetwarzania danych osobowych w swojej codziennej służbie instruktorskiej;
- Baczy, by nie wykroczyć poza zakres polecenia przetwarzania danych osobowych;
- Aktywnie zapobiega nadmiernemu zbieraniu i przetwarzaniu danych osobowych;
- Zna podstawowe zasady bezpieczeństwa danych osobowych, zarówno tych przetwarzanych w zbiorach danych, jak i tych przetwarzanych w systemach informatycznych;
- Zna szczególne zasady bezpieczeństwa danych osobowych w czasie pobytu w terenie;
- Potrafi rozpoznać typowe przypadki naruszenia ochrony danych osobowych;
- Jest świadomy doniosłości obowiązku niezwłocznego zawiadomienia o naruszeniu ochrony danych osobowych oraz wie, kogo o naruszeniu zawiadomić;
- Ułatwia inspektorowi ochrony danych wykonywanie jego zadań oraz stosuje się do jego zaleceń i rad;
- Baczy, by nie ujawnić danych osobowych osobom, organizacjom i władzom nieuprawnionym do ich otrzymania.

ROZDZIAŁ 1. PODSTAWOWE POJĘCIA

Czym są dane osobowe i ich przetwarzanie?

Dane osobowe to nie tylko imię, nazwisko, data urodzenia czy numer PESEL. To każda informacja, dzięki której dowiadujemy się czegoś o określonej osobie, i to bez względu na to, czy taka informacja jest precyzyjna, aktualna i prawdziwa.

Wszechobecność danych osobowych sprawia, że w toku służby w ZHP stykamy się z nimi na co dzień. Zbieramy je, wprowadzamy do Ewidencji ZHP lub innych systemów informatycznych ZHP albo też przechowujemy je w formie papierowej, porządkujemy je, analizujemy, wyciągamy na ich podstawie wnioski, na końcu zaś usuwamy je, niszczymy albo też zatrzymujemy na potrzeby badań naukowych nad historią harcerstwa. Wszystkie te czynności, nazywamy przetwarzaniem danych osobowych.

Kiedy możesz przetwarzać dane osobowe?

Możesz przetwarzać dane osobowe jedynie na polecenie ZHP, przy czym „polecenie" należy rozumieć szeroko. Polecenie może mieć charakter ogólny, a jego źródłem mogą być:

- przepisy i regulaminy ZHP nakładające na osoby pełniące funkcje instruktorskie obowiązki, których wykonanie ze swej natury wymaga przetwarzania danych osobowych (np. drużynowy ma obowiązek prowadzić książkę pracy drużyny)

- imienny dokument zawierający polecenie i upoważnienie do przetwarzania danych osobowych (zwanego dawniej upoważnieniem do przetwarzania danych osobowych).

Polecenie może mieć również charakter szczególny, tj. może dotyczyć jednorazowego wykonania określonego zadania. Jego źródłem jest wówczas doraźny rozkaz przełożonego, którego wykonanie ze swej natury wymaga przetwarzania danych osobowych. Jeżeli masz wątpliwości, czy wykonanie takiego rozkazu nie zagrozi bezpieczeństwu danych osobowych, nie wahaj się zapytać o zdanie inspektora ochrony danych.

Niezależnie od charakteru i źródła polecenia wyznacza ono granice postępowania z danymi osobowymi. Granice te wolno Ci przekroczyć jedynie na mocy przepisów prawa, np. na żądanie uprawnionych organów władzy publicznej.

W jaki sposób możesz przetwarzać dane osobowe?

W granicach polecenia przetwarzania nie możesz działać zupełnie dowolnie. Staraj się osiągać założone cele, przetwarzając jak najmniej danych osobowych, a nawet (o ile to możliwe) w ogóle rezygnując z ich przetwarzania.

Pamiętaj, że niedopuszczalne jest przetwarzanie danych osobowych „na zapas" i „na wszelki wypadek". Dotyczy to zarówno zbierania danych osobowych, jak i ich dalszego przetwarzania (np. sporządzania kopii dokumentów zawierających dane osobowe bez potrzeby albo ponad potrzebę).

Pamiętaj również, że niedopuszczalne jest:

- wykorzystywanie danych osobowych, o których dowiedziałeś się w związku ze służbą instruktorską, do jakichkolwiek innych celów, w szczególności do celów prywatnych;

- kopiowanie dokumentów zawierających dane osobowe do jakichkolwiek celów niezwiązanych ze służbą instruktorską, w szczególności do celów prywatnych.

ROZDZIAŁ 2. BEZPIECZEŃSTWO DANYCH OSOBOWYCH ORAZ REGUŁY POSTĘPOWANIA W RAZIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Na czym polega bezpieczeństwo danych osobowych?

Dane osobowe są bezpieczne, jeżeli:

- nie mają do nich dostępu osoby postronne (jest to tzw. **poufność danych**),
- nie podlegają przypadkowym lub nieuprawnionym zmianom (jest to tzw. **integralność danych**),
- dostęp do nich oraz dokonywanie na nich określonych działań nie napotykają żadnych przeszkód (jest to tzw. **dostępność danych**).

Na czym polega naruszenie ochrony danych osobowych?

Naruszeniem ochrony danych jest zdarzenie, które prowadzi lub może prowadzić do zniszczenia, utracenia, zmodyfikowania, ujawnienia lub uzyskania dostępu do danych osobowych. Zdarzenie to może być zarówno dziełem przypadku, jak i rezultatem celowego, bezprawnego działania.

Naruszeniem bezpieczeństwa jest również takie zdarzenie, które nie sprowadziło żadnych negatywnych skutków dla osoby, której dane dotyczą, chociaż w danych okolicznościach mogło sprowadzić takie skutki (np. włamanie do pomieszczenia, w którym przechowywane są nośniki danych osobowych, stanowi naruszenie ochrony danych, chociażby nie ukradziono żadnego z tych nośników).

Praktyczne przykłady naruszeń ochrony danych osobowych

Naruszeniem poufności jest np.

- wysłanie (pocztą elektroniczną lub tradycyjną) wiadomości zawierającej dane osobowe do niewłaściwego adresata,
- umieszczenie adresatów masowej wiadomości e-mail w polu CC (do wiadomości) zamiast BCC (ukryte do wiadomości); dotyczy to np. wiadomości wysyłanej do ogółu uczestników konkursu organizowanego przez ZHP; nie dotyczy to z kolei np. wiadomości wysyłanej do wyłącznie do członków ZHP na ich służbowe adresy e-mail,
- zgubienie niezaszyfrowanego pendrive'a zawierającego dane osobowe,
- przypadkowe pozostawienie dokumentów zawierających dane osobowe,
- wyrzucenie dokumentu zawierającego dane osobowe do zwykłego kosza na śmieci, zamiast do specjalnej niszczarki.

Naruszeniem integralności jest np. nadpisanie danych przetwarzanych w Ewidencji ZHP danymi nieaktualnymi albo niezweryfikowanymi co do poprawności.

Naruszeniem dostępności jest np.

- przypadkowe zniszczenie lub utrata dokumentów zawierających dane osobowe,
- zamoknięcie dokumentów zawierających dane osobowe,

- przypadkowe usunięcie plików zawierających dane osobowe z elektronicznych nośników (dysku twardego komputera lub pendrive'a).

- przypadkowa utrata klucza (hasła) pozwalającego na odczytanie zaszyfrowanych danych

- czasowy brak dostępu do danych przetwarzanych w Ewidencji ZHP z powodu awarii zasilania.

Jak należy postępować w przypadku podejrzenia naruszenia?

- Jeżeli podejrzewasz, że dane zdarzenie może prowadzić do naruszenia ochrony danych osobowych, masz obowiązek niezwłocznie zawiadomić o tym Inspektora ochrony danych ZHP albo inną wyznaczoną osobę w Głównej Kwaterze ZHP

  Dane kontaktowe:
  tel. +48 22 339 0645
  fax: +48 22 339 0606
  e-mail: rodo@zhp.pl

- Inspektora ochrony danych Chorągwi [●] albo inną wyznaczoną osobę w Komendzie Chorągwi [●]

  Dane kontaktowe [●]

Obowiązek powiadomienia powinieneś spełnić osobiście. Nie polegaj na innych osobach, a w szczególności nie odstępuj od spełnienia obowiązku zawiadomienia z tego powodu, że są jeszcze inne osoby zobowiązane na równi z Tobą do zawiadomienia (np. są świadkami tego samego zdarzenia). Obowiązek zawiadomienia powstaje, gdy istnieje choć cień podejrzenia, że określone zdarzenie może prowadzić do naruszenia bezpieczeństwa danych osobowych, nie zaś wtedy, gdy podejrzenie naruszenia graniczy z pewnością. Dlatego nie bój się zawiadamiać „z ostrożności" i „na wszelki wypadek". Być może dzięki takiemu zawiadomieniu uda się ujawnić słabe strony stosowanych zabezpieczeń i zapobiec naruszeniom, które mogłyby stąd wyniknąć. Powinieneś zawiadomić o podejrzeniu naruszenia danych osobowych natychmiast. Jeżeli jednak z powodu obiektywnych przeszkód dokonanie zawiadomienia jest czasowo niemożliwe, powinieneś natychmiast zanotować chwilę (dzień, godzinę i minutę), w której dowiedziałeś się o zdarzeniu, które Twoim zdaniem zagraża bezpieczeństwu danych osobowych. Dokonując zawiadomienia po ustaniu obiektywnych przeszkód, koniecznie podaj zanotowaną chwilę, w której dowiedziałeś się o zdarzeniu. Pamiętaj, że ZHP ma tylko 72 godziny na powiadomienie właściwych władz o naruszeniu. Stąd obowiązek powiadomienia powinieneś wykonać z pierwszeństwem przed innymi obowiązkami względem ZHP. Inne, nawet pilne, obowiązki nie usprawiedliwiają opóźnienia z powiadomieniem. Zawiadamiając inspektora ochrony danych lub inną wyznaczoną osobę, powinieneś opowiedzieć własnymi słowami, na czym polega zdarzenie, które Twoim zdaniem zagraża bezpieczeństwu danych osobowych. Nie trać czasu na przemyślenie i ułożenie w głowie treści zawiadomienia – inspektor lub inna wyznaczona osoba w razie potrzeby zadadzą Ci odpowiednie pytania pomocnicze,
które pozwolą wyjaśnić wszystkie okoliczności zdarzenia.

Jeżeli jednak chcesz ułatwić inspektorowi wyjaśnienie okoliczności zdarzenia i nie spowoduje to opóźnienia, możesz dokonać zawiadomienia, przekazując **następujące informacje**:

- na czym polegało zdarzenie?
- kiedy miało miejsce zdarzenie?
- jakich danych osobowych dotyczy zdarzenie?
- kto, oprócz Ciebie, może mieć wiedzę o zdarzeniu (świadkowie, osoby, od których uzyskałeś/uzyskałaś informację o zdarzeniu)?

Jeżeli nie posiadasz wszystkich powyższych informacji, wystarczy, że podzielisz się z inspektorem ochrony danych tym, co wiesz. Nikt nie będzie od ciebie wymagał wiedzy specjalistycznej w dziedzinie ochrony danych osobowych.

ROZDZIAŁ 3. OGÓLNE ZASADY BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Jak postępować z danymi osobowymi przechowywanymi w pomieszczeniach zajmowanych przez ZHP?

W celu zapewnienia bezpieczeństwa danych osobowych, ZHP wyposażył Główną Kwaterę, komendy chorągwi oraz inne pomieszczenia zajmowane przez ZHP w sprzęty takie jak np. czytnik kart wejściowych, zamykane na klucz pokoje i szafki, niszczarki dokumentów, profesjonalne kontenery na dokumenty skierowane do niszczenia. Każdy z Was jest obowiązany do odpowiedniego stosowania wszystkich dostarczonych przez ZHP sprzętów i narzędzi. Twoje stanowisko pracy wraz z ze znajdującymi się tam komputerami i innymi urządzeniami, kartotekami, księgami, wykazami i innymi zbiorami zawierającymi dane osobowe, pozostaje pod Twoją pieczą.

Osoby nieupoważnione do przetwarzania danych osobowych (w szczególności goście ZHP oraz osoby świadczące usługi sprzątania, serwisu sprzętu biurowego i bieżących napraw) mogą przebywać w pomieszczeniach biurowych ZHP jedynie w obecności instruktora lub pracownika upoważnionego do przetwarzania danych osobowych. Zapewnij, by towarzyszył im co najmniej jeden instruktor lub pracownik upoważniony do przetwarzania danych osobowych. Jeżeli nie możesz tego zapewnić, poproś osobę nieupoważnioną o zaczekanie na zewnątrz pomieszczenia, w których są przechowywane dane osobowe. Jeżeli jest to możliwe, zaproś tę osobę do miejsca, w którym nie są przechowywane dane osobowe, a w którym osoba ta będzie mogła zaczekać w komfortowych warunkach (np. wolna sala konferencyjna).

Jeżeli zapewnienie, by osobom nieupoważnionym towarzyszył co najmniej jeden instruktor lub pracownik upoważniony do przetwarzania danych osobowych jest niemożliwe lub nadmiernie utrudnione (dotyczy to np. świadczenia usług sprzątania poza zwykłymi godzinami pracy), udzielenie takim osobom dostępu do pomieszczeń biurowych ZHP jest dopuszczalne pod warunkiem, że wszystkie nośniki danych osobowych będą odpowiednio zabezpieczone. Należy w związku z tym bezwzględnie umieścić wszystkie dokumenty zawierające dane osobowe w zamkniętych na klucz szafkach (zasada „czystego biurka") oraz upewnić się, że wszystkie urządzenia służące do przetwarzania danych osobowych są wyłączone lub zablokowane (zasada „czystego ekranu").

Jeżeli grupa osób nieupoważnionych, przebywających w pomieszczeniach zajmowanych przez ZHP jest odpowiednio liczna, zapewnij, by towarzyszył im więcej niż jeden instruktor lub pracownik upoważniony do przetwarzania danych osobowych.

Jeżeli wychodzisz z pokoju, w którym pracujesz, zostawiając pokój pusty, zamykaj drzwi na klucz.

Jak postępować z danymi osobowymi zawartymi w dokumentacji papierowej?

Dokumentacja zawierająca dane osobowe obejmuje odręczne notatki, dokumenty i ich kopie, wydruki komputerowe, kartoteki, skorowidze, księgi, wykazy oraz inne zbiory dokumentów, niezależnie od nośnika tych danych. Jeżeli masz jakiekolwiek wątpliwości czy dokumentacja zawiera dane osobowe, traktuj ją tak, jakby takie dane zawierała.

Dokumentację zawierającą dane osobowe, która nie jest Ci w danym momencie potrzebna, trzymaj w szafkach zamykanych na klucz. Po zakończeniu dnia pracy uporządkuj biurko, tak, aby dokumentacja nie pozostała w widocznym lub łatwo dostępnym miejscu.

Nie oddawaj klucza do szafki innym osobom, jeżeli nie są upoważnione do przetwarzania tych danych, nie wyłączając najbardziej zaufanych druhów i druhny. Nie pozostawiaj go również w widocznym lub łatwo dostępnym miejscu.

Pod żadnym pozorem nie wyrzucaj dokumentacji zawierającej dane osobowe do kosza na śmieci, nawet po jej podarciu lub pocięciu. Dokumentacja taka może być niszczona wyłącznie w niszczarce lub wrzucona do profesjonalnego kontenera na dokumentację przeznaczoną do niszczenia.

Nie wynoś dokumentacji zawierającej dane osobowe, w tym sporządzonych doraźnie kopii lub wydruków, poza pomieszczenia zajmowane przez ZHP pracy bez uprzedniej zgody inspektora ochrony danych, chyba że:

- jedziesz do sądu, urzędu itd. w celach służbowych, do których te dokumenty są Ci niezbędne,

- jedziesz na biwak lub inną formę wypoczynku dzieci i młodzieży (o czym szczegółowo poniżej).

Czy wolno przechowywać dane osobowe we własnym domu lub w harcówce?

Po uzyskaniu zgody inspektora ochrony danych wolno Ci przechowywać dokumentację zawierającą dane osobowe oraz urządzenia służbowe służące do przetwarzania danych osobowych w pomieszczeniach zajmowanych lub wykorzystywanych nie tylko przez ZHP, lecz również przez inne osoby lub organizacje (np. w harcówce) oraz w prywatnym domu lub mieszkaniu. Masz jednak obowiązek stosować się do poniższych wytycznych:

- Zawsze przechowuj dokumentację i urządzenia jedynie w budynkach, lokalach i pomieszczeniach zapewniających **bezpieczeństwo danych osobowych**.

- O ile to możliwe, przechowuj dokumentację i urządzenia w **pomieszczeniach, do których inne osoby nie mają wstępu** (np. w domu/mieszkaniu, które zajmujesz sam, albo w domu/mieszkaniu, które zajmujesz wspólnie z innymi osobami, mając jednak do wyłącznej dyspozycji osobne pomieszczenie zamykane na klucz). Pomieszczenia takie muszą być zamykane na klucz.

- Możesz również przechowywać dokumentację i urządzenia w **pomieszczeniach, do których wstęp mają również inne osoby**, o ile spełniony jest jeden z poniższych warunków:

    - masz do wyłącznej dyspozycji osobną szafkę zamykaną na klucz; w takim przypadku masz obowiązek przechowywać dokumentację i urządzenia w tej szafce, o ile w danej chwili na nich nie pracujesz;

    - wyjątkowo - nie masz do wyłącznej dyspozycji osobnej szafki zamykanej na klucz, jednakże z powodu wyjątkowych okoliczności musisz się oddalić, pozostawiając w pomieszczeniu dokumentację i urządzenia, a pozostałe osoby mające wstęp do pomieszczenia dają gwarancję tego, że nie będą w tym czasie z niego korzystać (np. złożą wiarygodne oświadczenie); w takim przypadku Twoja nieobecność musi być bardzo krótka.

Poza pomieszczeniami zajmowanymi lub wykorzystywanymi wyłącznie przez ZHP wolno Ci przechowywać **na stałe** dokumentację pracy z drużyną, a pozostałą dokumentację oraz urządzenia – jedynie **tymczasowo**, przez czas niezbędny do wykonania szczególnego zadania.

ROZDZIAŁ 4. ZASADY BEZPIECZEŃSTWA DANYCH OSOBOWYCH W SYSTEMACH IT

Wstęp

Poniższe zasady dotyczą postępowania z danymi osobowymi, które są przechowywane lub w inny sposób przetwarzane przy pomocy urządzeń takich jak komputery stacjonarne, laptopy, telefony. Dotyczy to także nawiązywania za pomocą takich urządzeń zdalnego połączenia z Ewidencją ZHP lub innymi bazami danych zawierającymi dane osobowe.

Pamiętajcie, że poniższe zasady stosują się bez względu na to, czyją własnością jest urządzenie. W związku z tym zalecamy szczególnie uważną lekturę tym spośród Was, którzy korzystają z prywatnego urządzeń przy wykonywaniu zadań w ramach służby w ZHP,

Hasła

Używaj jedynie odpowiednio skomplikowanych i silnych haseł do uwierzytelniania w Ewidencji ZHP, w innych aplikacjach ZHP oraz w systemach operacyjnych urządzeń.

- **Skomplikowanie hasła.** Ustanawiaj hasła liczące co najmniej 10 znaków, w tym co najmniej jedną wielką i jedną małą literę, jedną cyfrę oraz jeden znak specjalny.

- **Siła hasła.** Hasła odpowiadające powyższym wymogom dotyczącym skomplikowania mogą różnić się od siebie poziomem bezpieczeństwa. Dlatego, zachowując powyższe wymogi, nie ustanawiaj haseł, które składają się z:

    - kolejno następujących po sobie cyfr,

    - liter w porządku, w jakim występują w alfabecie lub na klawiaturze QWERTY albo w odwrotnym porządku,

    - tych samych, wielokrotnie powtarzających się, cyfr lub liter,

    - imienia, nazwiska, daty urodzenia lub numeru PESEL Twojego lub Twoich bliskich,

    - nazw własnych, które łatwo powiązać z Twoją osobą, np. Twojego hobby, ulubionego artysty, imienia Twojego zwierzaka,

    - całych wyrazów słownikowych.

Wyłącz zapamiętywanie haseł w przeglądarce. Zamiast tego korzystaj z bezpiecznych managerów haseł, takich jak KeePass. Nie zapisuj haseł w miejscach łatwo dostępnych dla osoby, która mogłaby uzyskać bezprawnie lub przypadkowo dostęp do Twojego urządzenia. W szczególności nie zapisuj haseł:

- na karteczce umieszczonej na tablicy korkowej lub przy monitorze komputera,

- w pliku tekstowym zapisanym w pamięci komputera lub

- w notatniku trzymanym w plecaku na laptopa.

Nie ujawniaj obecnych ani dawnych haseł innym osobom, nie wyłączając najbardziej zaufanych druhów i druhen. Nie używaj haseł ustanowionych przez inne osoby, nawet na ich wyraźną prośbę.

Opuszczając, chociażby na chwilę, miejsce pracy, blokuj komputery i inne urządzenia.

Korzystanie z prywatnego komputera

Jeżeli przy wykonywaniu zadań w ramach służby w ZHP pracujesz na swoim własnym komputerze, utwórz odrębne konto użytkownika przeznaczone wyłącznie do wykonywania tych zadań. Dotyczy to w szczególności pracy na komputerze, z którego oprócz Ciebie korzystają jeszcze inne osoby (np. Twoi domownicy).

Zabezpiecz dostęp do specjalnie utworzonego konta odpowiednio silnym i skomplikowanym hasłem, zgodnie z wytycznymi zawartymi powyżej. Przy wykonywaniu operacji na danych osobowych wykorzystywanych w związku z działalnością ZHP używaj jedynie specjalnie utworzonego konta.

Dostęp zdalny

Jeżeli używasz służbowego komputera przenośnego, zachowaj szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza miejscem pracy. Korzystaj z zainstalowanego na tym komputerze oprogramowania do szyfrowania dysku.

Jeżeli pracujesz na danych osobowych poza zwykłym miejscem wykonywaniu zadań w ramach służby w ZHP, np. w czasie biwaku lub innej formy wypoczynku, stosuj się do następujących wskazówek:

- Unikaj miejsc łatwo dostępnych dla osób postronnych, takich jak biblioteki i kawiarnie. Upewnij się, że obraz wyświetlany na Twoim urządzeniu nie jest obserwowany przez osoby postronne;

- Nie korzystaj z niezabezpieczonych lub obcych łączy internetowych, np. z punktów HotSpot w miejscach publicznie dostępnych, w hotelach, szpitalach itd.

- Nie korzystaj z cudzych urządzeń (innych niż urządzenia przeznaczone przez ZHP do użytku związanego z pełnioną służbą), a w szczególności nie używaj tych urządzeń do logowania się do Ewidencji ZHP i innych serwisów ZHP oraz nie zapisuj żadnych danych osobowych w pamięci tych urządzeń.

Zainstalowane aplikacje

Instaluj na swoim urządzeniu aplikacje pochodzące jedynie z zaufanych źródeł. W razie wątpliwości skonsultuj się z Administratorem Systemów Informatycznych. Poniżej znajdziesz wskazówki dotyczące postępowania w razie przypadkowego zainstalowania na swoim urządzeniu podejrzanej aplikacji.

Starsze wersje zainstalowanych aplikacji mają szereg ogólnie znanych podatności, które mogą być wykorzystane w celu naruszenia bezpieczeństwa danych, w tym również danych osobowych. Dokonuj przeglądów zainstalowanych aplikacji w celu stwierdzenia czy będziesz ich jeszcze potrzebował czy nie. Jeżeli dana aplikacja przestała Ci być potrzebna, odinstaluj ją. Pozostałe aplikacje poddawaj regularnym aktualizacjom (w celu ograniczenia liczby potencjalnych podatności).

Ochrona przed złośliwym oprogramowaniem

Zainstaluj na swoim urządzeniu aplikację chroniącą urządzenie i inne aplikacje przed złośliwym oprogramowaniem takim jak wirusy, konie trojańskie, spyware lub ransomware. Aplikacja taka powinna w miarę możliwości mieć funkcjonalność skanowania wiadomości email, otwieranych stron internetowych oraz pobieranych plików. Nie wyłączaj zapory sieciowej (firewall).

Przeprowadzaj pełne skanowanie urządzenia co najmniej raz w tygodniu.

Zwracaj szczególną uwagę na następujące typowe źródła infekcji złośliwym oprogramowaniem:

- wiadomości email zawierającej załącznik ze złośliwym oprogramowaniem,
- wiadomości email zawierającej odnośnik do strony ze złośliwym oprogramowaniem,
- pobranie pliku lub programu ze strony internetowej zawierającej złośliwe oprogramowanie,
- podłączenie do urządzenia nośnika danych zawierającego złośliwe oprogramowanie.

Jeżeli podejrzewasz infekcję złośliwym oprogramowaniem natychmiast zaprzestań pracy na urządzeniu (nie dokonując zapisu pracy, kopiowania aplikacji) oraz skontaktuj się z osobą odpowiedzialną za zarządzanie systemami informatycznymi lub po prostu z informatykiem.

Likwidacja lub naprawa elektronicznych nośników danych osobowych

Jeżeli urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające lub mogące zawierać dane osobowe mają być wydane osobom nieupoważnionym do przetwarzania danych osobowych w imieniu ZHP w związku z ich:

- likwidacją
- naprawą
- sprzedażą, najmem lub przeniesieniem posiadania pod innym tytułem prawnym

upewnij się, że przed wydaniem zostały pozbawione zapisu danych osobowych, w sposób uniemożliwiający ich odczytanie i odzyskanie.

ROZDZIAŁ 5. SZCZEGÓLNE ZASADY BEZPIECZEŃSTWA DANYCH OSOBOWYCH W TERENIE

Bezpieczeństwo danych osobowych stosunkowo łatwo jest zapewnić, gdy dane są przechowywane w pomieszczeniach komendy hufca lub chorągwi albo w innych pomieszczeniach zajmowanych przez ZHP i zasadniczo niedostępnych dla osób postronnych. Prawdziwe wyzwania dla bezpieczeństwa danych osobowych pojawiają się dopiero wtedy, gdy dane opuszczają te pomieszczenia – w szczególności w związku z organizacją zlotów, biwaków lub innych form wypoczynku. Niniejsza część wytycznych dotyczy właśnie takich przypadków (które będziemy zbiorczo nazywać „pobytem w terenie").

Z punktu widzenia bezpieczeństwa danych osobowych, im więcej dokumentów zawierających dane osobowe pozostawisz w komendzie, tym lepiej. Niekiedy jednak z przepisów prawa lub praktyki różnych organów władzy publicznej wynika obowiązek posiadania określonych dokumentów i okazania ich na każde wezwanie (np. karty kwalifikacyjne uczestników wypoczynku, informacje z Krajowego Rejestru Sprawców Przestępstw na Tle Seksualnym). Bez uszczerbku dla tego obowiązku, ogranicz do minimum liczbę dokumentów, które zabierasz poza pomieszczenia komendy. W czasie pobytu w terenie skorzystaj z możliwości pozostawienia dokumentacji w zamykanym na klucz pomieszczeniu w ośrodku wypoczynkowym lub schronisku albo w bagażniku samochodu osobowego. Niedopuszczalne jest jednak pozostawienie w takim miejscu dokumentacji, która ze względu na ochronę życia i zdrowia uczestników powinna być łatwo dostępna w każdej chwili. Niedopuszczalne jest również pozostawienie w takim miejscu pozostałej dokumentacji, jeżeli wiązałoby się to z ograniczeniem jej dostępności przez dłuższy czas (np. pozostawienie jej w schronisku na czas kilkudniowej wędrówki po górach).

Dokumentacja, którą zdecydowałeś/zdecydowałaś się pozostawić przy sobie, powinna być odpowiednio zabezpieczona z uwzględnieniem szczególnych warunków pobytu w terenie. Poniżej przedstawiamy niektóre typowe zagrożenia dla bezpieczeństwa danych osobowych oraz propozycje postępowania. Zagrożeń jest jednak o wiele więcej niż możemy opisać w ramach niniejszych wytycznych. Dlatego zamiast przedstawiać gotowe scenariusze postępowania, zalecamy, by w każdej sytuacji mieć szeroko otwarte oczy i kierować się zdrowym rozsądkiem.

Zagrożenie	Propozycja postępowania
Zabranie nośników danych przez osobę nieuprawnioną	Trzymaj nośniki danych przy sobie lub w zasięgu swojego wzroku Nie zostawiaj nośników danych bez nadzoru osób upoważnionych do przetwarzania tych danych Trzymaj nośniki danych w plecaku i używaj małej kłódki, aby utrudnić otwarcie suwaka
Podejrzenie danych przez osobę nieuprawnioną, w tym przez samych podopiecznych	Nie zostawiaj nośników danych bez nadzoru osób upoważnionych do przetwarzania tych danych Trzymaj nośniki danych w plecaku i używaj małej kłódki, aby utrudnić otwarcie suwaka

Uszkodzenie lub zniszczenie nośnika danych przez zamoknięcie i działanie innych czynników atmosferycznych	Opakuj dokumentacje w koszulki foliowe lub laminowane teczki
Porwanie nośników danych przez wiatr	Zszyj lub w inny sposób połącz ze sobą kartki dokumentów albo załóż segregator na dokumenty

Powyższe uwagi dotyczące papierowej dokumentacji, zawierającej dane osobowe, mają zastosowanie również do elektronicznych nośników takich danych. Należy jednak pamiętać, że ze względu na ograniczony dostęp do źródeł zasilania lub ograniczony zasięg sieci telekomunikacyjnych, przechowywanie danych osobowych na elektronicznych nośnikach danych może nie zapewniać należytej dostępności tych danych w terenie.

ROZDZIAŁ 6. WSPÓŁPRACA Z INSPEKTOREM OCHRONY DANYCH

Zadania inspektora

Inspektor ochrony danych to osoba mająca wiedzę fachową w zakresie ochrony danych osobowych, której ZHP powierzył zadania związane z:

- kontrolą przestrzegania przepisów o ochronie danych osobowych,
- informowaniem władz ZHP oraz instruktorów o ich obowiązkach dotyczących ochrony danych osobowych oraz doradzaniem im w tych sprawach,
- pośrednictwem w kontaktach z Prezesem Urzędu Ochrony Danych Osobowych oraz z osobami, których dane dotyczą.

W związku z wykonywaniem tych zadań inspektor ochrony danych cieszy się niezależnością od władz ZHP. Inspektor jest zatem bezstronnym specjalistą, do którego możesz się zwrócić w każdej sprawie związanej z ochroną danych osobowych.

Informowanie o nieprawidłowościach

Pamiętaj, że Twoje zaangażowanie jest najlepszą gwarancją prawidłowego funkcjonowania ZHP, w tym również prawidłowego postępowania z danymi osobowymi. Jeżeli dostrzegasz lub podejrzewasz jakiekolwiek nieprawidłowości dotyczące postępowania z danymi osobowymi, opowiedz o nich inspektorowi ochrony danych. Możesz również przekazać inspektorowi swoje propozycje zaradzenia tym nieprawidłowościom. Zapewniamy, że z powodu poinformowania o dostrzeżonych lub podejrzewanych nieprawidłowościach nie może Cię spotkać żadna przykrość. Jeśli chcesz, możesz skorzystać z możliwości anonimowego poinformowania inspektora.

Pomoc przy wykonywaniu zadań inspektora

Dołóż starań w celu zapewnienia inspektorowi warunków niezbędnych do sprawnego przeprowadzenia audytu oraz prawidłowego ustalenia stanu rzeczy, a w szczególności:

- zapewnij wstęp do wszelkich budynków, lokali i innych pomieszczeń,
- okaż dokumenty,
- udziel informacji ustnie lub na piśmie,
- wydaj urządzenia i nośniki danych,
- udziel dostępu systemów informatycznych służących do przetwarzania danych,
- sporządź i wydaj kopie dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach informatycznych służących do przetwarzania danych.

Wykonuj rzetelnie polecenia wydawane przez inspektora ochrony danych, a w szczególności:

- polecenia podjęcia działań w celu zapobieżenia lub zmniejszenia negatywnych skutków naruszenia ochrony danych osobowych,

- polecenia usunięcia nieprawidłowości stwierdzonych w toku audytu.

Zasięganie rady inspektora

Pamiętaj, żeby skonsultować się z inspektorem w sprawie planowanych nowych działań wymagających przetwarzania danych osobowych, o których inspektor nie miał dotąd okazji się wypowiedzieć. To samo dotyczy istotnej zmiany dotychczasowych działań, wymagających przetwarzania danych osobowych. Każdy nowy element planowanych działań powinien zostać poddany ocenie pod względem zgodności z przepisami o ochronie danych osobowych.

Korzystaj z okazji do wzięcia udziału w okresowych szkoleniach i kursach organizowanych przez inspektora ochrony danych. Stosuj się do zaleceń i wystąpień formułowanych przez inspektora, mających na celu jednolite i prawidłowe stosowanie przepisów o ochronie danych osobowych w praktyce działania ZHP. Pamiętaj, że możesz zwrócić się do inspektora o wyjaśnienie zawiłych przepisów RODO i o udzielenie porady co do sposobu załatwienia konkretnej sprawy.

ROZDZIAŁ 7. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Jak postępować w związku z żądaniem dostępu do danych, zgłoszonym przez osobę, której dane dotyczą?

Udzielaniem odpowiedzi na żądania dostępu do danych oraz inne żądania zgłaszane przez osobę, której dane dotyczą, zajmują się w ZHP inspektor ochrony danych oraz osoby wyznaczone do pomocy inspektorowi w wypełnieniu jego zadań.

Zatem jeżeli członek ZHP (albo działający w jego imieniu rodzic lub opiekun) zgłasza wobec Ciebie żądanie, powinieneś przekazać je niezwłocznie inspektorowi ochrony danych. Inspektor rozpatrzy to żądanie, rozstrzygnie o jego zasadności i udzieli odpowiedzi osobie, której dane dotyczą.

Jednakże, gdy żądanie dostępu do danych możesz spełnić „od ręki" na podstawie dokumentów i innych nośników informacji, które masz przy sobie (np. żądanie wglądu do książki pracy drużyny), powinieneś je spełnić, a nie przekazywać inspektorowi. Pamiętaj, że spełnienie żądania dostępu do danych nie może prowadzić do ujawnienia danych osobowych dotyczących innych osób. Dotyczy to zwłaszcza spełnienia żądania przez okazanie dokumentu lub innego nośnika danych osobie zgłaszającej żądanie.

Nie wahaj się również udzielać „od ręki" informacji dotyczących stanu zdrowia, samopoczucia czy zachowania się dziecka w czasie wypoczynku na żądanie zgłoszone telefonicznie
przez jego rodziców lub opiekunów. W celu weryfikacji tożsamości osoby dzwoniącej, wykorzystaj dane zawarte w karcie kwalifikacyjnej. Jeżeli osoba dzwoniąca korzysta z numeru telefonu podanego w karcie kwalifikacyjnej, możesz poprzestać na pytaniu o jej imię
i nazwisko.

Jak postępować z danymi osobowymi w związku z ich udostępnianiem?

Dane osobowe, które przetwarzasz, w nie powinny być ujawniane innym osobom, organizacjom lub władzom poza ZHP z wyjątkiem:

- służb, inspekcji i innych władz publicznych uprawnionych na mocy ustaw do wglądu do danych osobowych w związku z prowadzoną kontrolą lub innym postępowaniem,

- lekarzy, pielęgniarek, ratowników medycznych oraz innych osób udzielających świadczeń opieki zdrowotnej w związku z potrzebą udzielenia takich świadczeń osobom będącym pod Twoją pieczą,

- władz naczelnych ZHP (ZHP jest odrębnym od poszczególnych chorągwi administratorem danych) w związku z prowadzoną przez nie kontrolą prawidłowości działania chorągwi i hufców.

Jeżeli zajdzie potrzeba ujawnienia danych osobowych wymienionym powyżej osobom, organizacjom lub władzom, powinieneś zadbać o to, by zostały ujawnione jedynie takie dane, które są rzeczywiście niezbędne ze względu na uzasadnione cele ich ujawnienia.

Jeżeli zajdzie potrzeba ujawnienia danych osobowych osobom, organizacjom lub władzom innym niż wymienione powyżej, powinieneś skonsultować się z inspektorem ochrony danych w sprawie zgodności z prawem zamierzonego ujawnienia danych.