Załącznik nr 1 do uchwały Zarządu Głównego PTTK

nr 169/XIX/2020 z dnia 4 lipca 2020 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH
WRAZ Z INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
PRZETWARZAJĄCYM DANE OSOBOWE
W POLSKIM TOWARZYSTWIE TURYSTYCZNO-KRAJOZNAWCZYM

Spis treści

Wstęp 2
Definicje 3
Zadania IOD 6
Ocena skutków (analiza ryzyka) 8
Opis operacji przetwarzania (inwentaryzacja aktywów) 8
Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO) 8
Analiza ryzyka 9
Definicje 9
Wyznaczenie zagrożeń 10
Wyliczenie ryzyka dla zagrożeń 10
Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem 11
Reakcja na wartość ryzyka 11
Ponowna analiza ryzyka 11
Plan postępowania z ryzykiem 12
Instrukcja postępowania z incydentami 12
Rejestr czynności przetwarzania 14
Polityka kluczy 14
Wykaz zbiorów danych osobowych 15
Opis struktury zbiorów danych wraz ze sposobem przepływu 15
Zabezpieczenia organizacyjne 16
Zabezpieczenia fizyczne danych osobowych. 16
Kontrola systemu ochrony danych osobowych 17
Sprawozdanie roczne stanu systemu ochrony danych osobowych 17
Szkolenia pracowników 18
Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe 19
Zarządzane uprawnieniami użytkowników 19
Dostęp do systemów informatycznych przetwarzających dane osobowe- zabezpieczenia informatyczne 19
Polityka haseł 19
Hasła do sieci i serwera 20
Hasła do programów przetwarzających dane osobowe 20
Hasła administratora 20
Procedura rozpoczęcia, zawieszenia i zakończenia pracy- zabezpieczenia informatyczne 21
Procedura tworzenia kopii zapasowych- zabezpieczenia informatyczne 21
Tworzenie kopii bezpieczeństwa programu Kadrowo-Płacowego 21
Tworzenie kopii bezpieczeństwa programu księgowego 22
Tworzenie kopii bezpieczeństwa serwera w centrali 22
Przechowywanie elektronicznych nośników i dokumentów zawierające dane osobowe- zabezpieczenia informatyczne 22
Zabezpieczenie elektronicznych nośników informacji 22

Zabezpieczenie dokumentów i wydruków 23
Oprogramowania antywirusowe- zabezpieczenia informatyczne 24
Ochrona antywirusowa 24
Dostęp do sieci lokalnej 24
Procedura wykonywania przeglądów i konserwacji 24
Postanowienia końcowe 25
Wykaz załączników 26

Wstęp

Celem Polityki Ochrony Danych Osobowych, zwanej dalej Polityką, oraz Instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwanej dalej Instrukcją, jest zapewnienie ochrony danych przetwarzanych przez Polskie Towarzystwo Turystyczno-Krajoznawcze przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka wraz z Instrukcją jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) i wydanych na jej podstawie aktów wykonawczych.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, zabezpieczenia organizacyjne oraz zabezpieczenia informatyczne.

Zastosowane zabezpieczenia mają służyć ochronie danych osobowych i zapewnić:

1. **poufność danych** - dane nie są udostępniane nieupoważnionym osobom;
2. **integralność danych** - dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3. **rozliczalność danych** - działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4. **integralność systemu** - nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Definicje

1. **Polityka** – rozumie się przez to Politykę Ochrony Danych Osobowych w Polskim Towarzystwie Turystyczno-Krajoznawczym;
2. **Administrator** – Polskie Towarzystwo Turystyczno-Krajoznawcze, decydujący o celach i środkach przetwarzania danych osobowych;
3. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez Polskie Towarzystwo Turystyczno-Krajoznawcze, odpowiedzialna za organizację ochrony danych osobowych;
4. **RODO** – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016);
5. **Dane osobowe (dane)** – to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamość tej osoby fizycznej;
6. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;
7. **Przetwarzanie danych osobowych** – to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych, która obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.
8. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9. **Ograniczenie przetwarzania** – polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
10. **Anonimizacja** – zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych;

11. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
12. **Baza danych osobowych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
13. **Ocena skutków w ochronie danych (analiza ryzyka)** – to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;
14. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
15. **Administrator systemu (ASI)** – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień; główny informatyk;
16. **Pracownik** – osoba fizyczna wykonująca określonego rodzaju pracę na rzecz pracodawcy, pod jego kierownictwem, w wyznaczonym przez niego miejscu i czasie, za co przysługuje jej wynagrodzenie; również zleceniobiorca, współpracownik bądź członek stowarzyszenia, który jest zobowiązany do wykonania usługi na rzecz Administratora;
17. **Użytkownik** – pracownik Administratora posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
18. **Zabezpieczenie systemu informatycznego** – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
19. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;
20. **Podmiot przetwarzający (Procesor)** – to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora;

21. **Pseudonimizacja** – oznacza przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
22. **Szczególne kategorie danych osobowych (dane wrażliwe)** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, członkostwo w związkach zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientacji seksualnej. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach;
23. **Profilowanie** – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Zadania IOD

Do najważniejszych obowiązków Inspektora Ochrony Danych należy:

1. informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawnych o ochronie danych i doradzanie im w tej sprawie;
2. monitorowanie przestrzegania przepisów o ochronie danych przez Administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe;
3. zapewnienie przetwarzania danych osobowych zgodnie z uregulowaniami Polityki Ochrony Danych Osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
4. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
5. pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
6. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;
9. współpraca z Prezesem Urzędu Ochrony Danych Osobowych.

Inspektor Ochrony Danych ma prawo:

1. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w Polskim Towarzystwie Turystyczno-Krajoznawczym;

2. wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z przepisami prawa;
3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego;
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli;
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

Ocena skutków (analiza ryzyka)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka, za wykonanie której odpowiada Administrator. Jeżeli Administrator / podmiot przetwarzający nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.
W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

Opis operacji przetwarzania (inwentaryzacja aktywów)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku Wykaz zbiorów danych osobowych – załącznik nr 1.
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
    a. nazwę zbioru (opis kategorii osób),
    b. opis celów przetwarzania,
    c. charakter, zakres, kontekst danych osobowych,
    d. odbiorcy danych,
    e. funkcjonalny opis operacji przetwarzania,
    f. aktywa służące do przetwarzania danych osobowych (informacje, programy, systemy operacyjne, infrastruktura IT, infrastruktura, pracownicy i współpracownicy, outsourcing),
    g. informacja o konieczności wpisu do rejestru czynności przetwarzania,
    h. informacja o konieczności przeprowadzenia oceny skutków dla zbioru.

Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)

W ramach przeprowadzenia oceny skutków (**analizy ryzyka** – załącznik nr 2) Administrator zobowiązany jest do spełnienia obowiązków prawnych wobec danych w zbiorach (dla kategorii osób - patrz **Rejestr czynności przetwarzania** – załącznik nr 3).

W szczególności należy zapewnić, że:

1. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
2. dane te są adekwatne w stosunku do celów przetwarzania,
3. dane te są przetwarzane przez określony czas (retencja danych),
4. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
5. opracowano klauzule informacyjne dla powyższych osób (patrz załącznik **Klauzule informacyjne** – załącznik nr 4),
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO) zgodnie z załącznikiem **Umowa powierzenia** – załącznik nr 5 (wykaz podmiotów przetwarzających prowadzony jest w załączniku **Ewidencja podmiotów zewnętrznych** – załącznik nr 6,
7. potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w załączniku **Wykaz zbiorów danych osobowych** – załącznik nr 1.

Analiza ryzyka

Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy).

Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. Naruszenie (Incydent) ochrony danych osobowych - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).

4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.
3. Wykaz przykładowych zagrożeń znajduje się w arkuszu Aktywa w Załączniku **Analiza ryzyka** – załącznik nr 2.

Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Skalę Prawdopodobieństwa (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1

średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie),
    b. unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),
    c. redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza firmę).
3. Wykaz przykładowych zabezpieczeń znajduje się w arkuszu Aktywa w Załączniku **Analiza ryzyka** – załącznik nr 2.
4. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie) **Analiza ryzyka** – załącznik nr 2.

Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych 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 typowych incydentów bezpieczeństwa danych osobowych 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. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki**,**
    b. inicjuje ewentualne działania dyscyplinarne**,**
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu**,**
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – Formularz rejestracji incydentu – załącznik nr 7.
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.

Rejestr czynności przetwarzania

W przypadku konieczności prowadzenia rejestru czynności przetwarzania przez Administratora, wypełnia on **Rejestr czynności przetwarzania** – załącznik nr 3**.**

Polityka kluczy

1. Polityka kluczy obejmuje budynki:
    - Polskie Towarzystwo Turystyczno-Krajoznawcze Biuro Zarządu Głównego przy ul. Senatorskiej 11 w Warszawie;
    - Centrum Fotografii Krajoznawczej PTTK przy ul. Wigury 12a w Łodzi;
    - Centralny Ośrodek Turystyki Górskiej przy ul. Jagiellońskiej 6 w Krakowie;
    - Centrum Turystyki Wodnej przy ul. Kasprowicza 40 w Warszawie;
    - Okręgowy Zespół Gospodarki Turystycznej przy ul. Westerplatte 15/16 w Krakowie;
    - Centrum Szkolenia Podwodnego przy ul. Senatorskiej 11 w Warszawie;
    - Zarząd Majątkiem PTTK przy ul. Krakowskie Przedmieście 4 w Warszawie;
    - Centralna Biblioteka Polskiego Towarzystwa Turystyczno-Krajoznawczego im. Kazimierza Kulwiecia przy ul. Senatorskiej 11 w Warszawie.
2. Obowiązuje pięciodniowy tydzień pracy, tzn. od poniedziałku do piątku, w godzinach 08:00 – 16:00.
3. W obiektach wyszczególnionych w punkcie 1 Polityki Kluczy, po godzinie 16:30, przebywać mogą jedynie:

   - dozorca/portier,

   - osoby zatrudnione do sprzątania,

   - inne osoby, po uzyskaniu bezpośredniej zgody Kierownika danej jednostki lub Sekretarza Generalnego ZG PTTK (w odniesieniu do Biura ZG PTTK).
4. Dostęp do pomieszczeń biurowych możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Wszystkie pozostałe drzwi umożliwiające dostęp do pomieszczeń biurowych powinny być trwale zamknięte na klucz. Zabrania się otwierania tych drzwi przez pracowników bez zgody Administratora.
5. Klucze zapasowe przechowywane są w odpowiednio zabezpieczonym pomieszczeniu, wskazanym przez Kierownika danej jednostki (patrz Polityka kluczy, punkt 1). W obiekcie Senatorska 11 osobą odpowiedzialną za powyższe jest Sekretarz Generalny ZG PTTK.

6. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
7. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą ~~o~~dpowiedzialność za ich należyte zabezpieczenie.
8. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
9. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
10. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń, a w szczególności:
    - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
    - wyłączenia oświetlenia,
    - zabezpieczenia i zamknięcia okien i drzwi,
    - zamknięcia szaf i szafek na klucz oraz zabezpieczenie kluczy,
    - zastosowania Polityki czystego biurka - zabronione jest pozostawianie niezabezpieczonych dokumentów zawierających dane osobowe po zakończeniu pracy,
    - pozostawienia kluczy do pomieszczeń biurowych w wyznaczonym przez Kierownika jednostki bądź Sekretarza Generalnego ZG PTTK (w odniesieniu do Biura ZG PTTK) miejscu.
11. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Wykaz zbiorów danych osobowych

Wykaz zbiorów danych osobowych to ewidencja zbiorów danych osobowych, z określoną lokalizacją w organizacji, określonymi zabezpieczeniami fizycznymi, organizacyjnymi i informatycznymi.
Zbiory danych osobowych występują w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych **Wykaz zbiorów danych osobowych** – załącznik nr 1.

Opis struktury zbiorów danych wraz ze sposobem przepływu

Opis systemów informatycznych, w których przetwarzane są dane osobowe oraz sposób przepływu danych pomiędzy programami został przedstawiony w **Opisie struktury zbiorów danych w systemach informatycznych wraz ze sposobem przepływu danych pomiędzy nimi** – załącznik nr 8.

Zabezpieczenia organizacyjne:

1. został wyznaczony Inspektor Ochrony Danych nadzorujący przestrzeganie zasad ochrony danych osobowych **Wyznaczenie IOD** – załącznik nr 9;
2. została opracowana i wdrożona Polityka Ochrony Danych Osobowych;
3. została opracowana i wdrożona Instrukcja zarządzania systemem informatycznym;
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora – **Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych** – załącznik nr 10**;**
5. prowadzona jest Ewidencja osób upoważnionych do przetwarzania danych – **Ewidencja osób upoważnionych do przetwarzania danych osobowych** – załącznik nr 11;
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy – **Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych** – załącznik nr 10**;**
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
10. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe, których Administratorem jest Polskie Towarzystwo Turystyczno-Krajoznawcze – **Umowa powierzenia** – załącznik nr 4.

Zabezpieczenia fizyczne danych osobowych:

Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej:

1. drzwi zamykane na klucz,
2. zamknięte na klucz niemetalowe szafy,
3. niszczarki dokumentów,

4. Polityka kluczy,
5. Polityka czystego biurka,
6. służba ochrony/alarm,
7. gaśnice.

Zabezpieczenia informatyczne:

Szczegółowy opis zabezpieczeń uwzględniają zapisy niniejszego dokumentu.

Kontrola systemu ochrony danych osobowych

1. Do kontroli stanu ochrony danych osobowych upoważniony jest IOD, wyznaczeni kontrolerzy wewnętrzni, najwyższe kierownictwo.
2. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami Ustawy.
3. IOD przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
4. Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi. Na jego podstawie IOD inicjuje działania korygujące lub zapobiegawcze.

Sprawozdanie roczne stanu systemu ochrony danych osobowych

1. Raz w roku IOD przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych
2. W spotkaniu sprawozdawczym uczestniczą: IOD, Kierownicy działów, w których przetwarzane są dane osobowe, Informatyk.

Szkolenia pracowników

1. Każdy pracownik przed dopuszczeniem do pracy z wykorzystaniem danych osobowych winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada IOD, a za jego zorganizowanie odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Politykami, instrukcjami oraz Regulaminami obowiązującymi u Administratora, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje zakończone podpisaniem przez pracownika Oświadczenia o poufności. Dokument ten jest przechowywany w aktach osobowych pracowników.

   Po zakończonym szkoleniu Administrator nadaje pracownikowi Upoważnienie do przetwarzania danych osobowych. Dokument ten jest przechowywany w aktach osobowych pracowników.

Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe

Zarządzane uprawnieniami użytkowników

1. Pracownik przed podjęciem działań mających na celu przetwarzanie danych osobowych w systemie informatycznym lub w zbiorze papierowym otrzymuje od Administratora pisemne upoważnienie do przetwarzania danych osobowych. Informacja o nadaniu upoważnienia przekazywana jest Inspektorowi Ochrony Danych.
2. W przypadku nadania bądź zmiany uprawnienia, IOD zobowiązany jest do sprawdzenia, czy użytkownik:
    a. odbył szkolenie z zakresu ochrony danych osobowych,
    b. podpisał oświadczenie o zachowaniu poufności,
    c. będzie przetwarzał dane osobowe w zakresie i celu określonym w Polityce i Instrukcji,
    d. zakres ustanowionego upoważnienia jest adekwatny do zakresu obowiązków służbowych.
3. W celu usunięcia uprawnień użytkownikowi Główny Informatyk (ASI) jest zobowiązany do wyrejestrowania go z systemu po uprzednim poinformowaniu o sytuacji IOD.
4. Usunięty identyfikator użytkownika nie może być przydzielany innej osobie.
5. Administrator bądź bezpośredni przełożony w imieniu Administratora, w sposób formalny, zgodnie z powyższą procedurą, nadaje upoważnienie do przetwarzania danych osobowych.
6. Upoważnienie do przetwarzania danych osobowych jest przechowywane w aktach osobowych pracownika.

Dostęp do systemów informatycznych przetwarzających dane osobowe- zabezpieczenia informatyczne

Polityka haseł

1. Bezpośredni przełożony pracownika informuje ASI oraz IOD o nadaniu upoważnienia do przetwarzania danych osobowych w wybranych systemach informatycznych, przed przystąpieniem pracownika do przetwarzania.
2. W upoważnieniu określony jest zakres możliwych działań pracownika w wyznaczonych systemach.

3. Zakres upoważnienia obejmuje: wgląd, archiwizację, modyfikację, usunięcie, uprawnienia administracyjne.
4. ASI informuje użytkownika o nadaniu pierwszego hasła do systemu.
5. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
6. Użytkownik systemu w trakcie pracy w systemie może zmienić swoje hasło.
7. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów (swoich oraz bliskich osób) oraz numerów rejestracyjnych samochodów, numerów telefonów.
8. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
9. Zabronione jest zapisywanie haseł w sposób jawny oraz udostępnianie ich innym osobom.

Hasła do sieci i serwera

1. Hasło dostępu do (serwera / sieci) składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 6 miesięcy i jest wymuszana przez system.

Hasła do programów przetwarzających dane osobowe

1. Hasło dostępu do programu składa się co najmniej z 8 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się raz na 6 miesięcy w sposób manualny lub jest wymuszana przez system.

Hasła administratora

1. Hasło administratora składa się co najmniej z 12 znaków.
2. Hasło składa się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Hasło powinno być znane tylko administratorowi. Metryka hasła powinna zawierać: treść hasła, datę jego wprowadzenia do systemu, datę i powód awaryjnego udostępnienia hasła oraz być przechowywane przez okres 5 lat.
4. Administrator systemu zobowiązany jest do umieszczenia haseł administratora w zamkniętych kopertach w sejfie.
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których osoba ta miała dostęp.

6. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane osobie zastępującej administratora systemu.
7. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy - zabezpieczenia informatyczne

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem loginu i hasła.
2. Użytkownik jest zobowiązany do powiadomienia IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
4. Użytkownik jest zobowiązany do podjęcia wszelkich działań w celu uniemożliwienia osobom niepowołanym wgląd do danych wyświetlanych na monitorach komputerowych – tzw. **Polityka czystego ekranu**.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 15 minut system automatycznie aktywuje wygaszacz.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe,
    c. dokumentacje oraz nośniki schować do szafy zamkniętej na klucz,
    d. przechowywania kluczy do szafek w miejscu znanym jedynie pracownikowi.

Procedura tworzenia kopii zapasowych - zabezpieczenia informatyczne

Tworzenie kopii bezpieczeństwa programu kadrowo-płacowego

1. Pełna kopia bazy wykonywana jest co 4 tygodnie w sposób automatyczny na zasób poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

2. Codziennie w dni robocze, w sposób automatyczny wykonywana jest kopia przyrostowa bazy na zasób poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

3. Raz w miesiącu wykonywana jest kopia na nośnik zewnętrzny wraz z odtworzeniem bazy na serwerze testowym. Nośnik przechowywany jest w sejfie. Kopie wykonuje wyznaczony operator. Informacja o wykonanej kopii zapisywana jest w karcie charakterystyki operatora.

Tworzenie kopii bezpieczeństwa programu księgowego

1. Pełna kopia bazy wykonywana jest co 4 tygodnie w sposób automatyczny na zasób poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

2. Codziennie w dni robocze, w sposób automatyczny wykonywana jest kopia przyrostowa bazy na zasób poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

3. Raz w miesiącu wykonywana jest kopia na nośnik zewnętrzny wraz z odtworzeniem bazy na serwerze testowym. Nośnik przechowywany jest w sejfie. Kopie wykonuje wyznaczony operator. Informacja o wykonanej kopii zapisywana jest w karcie charakterystyki operatora.

Tworzenie kopii bezpieczeństwa serwera w centrali

1. Pełna kopia zasobów zgromadzonych na serwerze plików wykonywana jest co 4 tygodnie w sposób automatyczny na macierz dyskową poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

2. Codziennie w dni robocze, w sposób automatyczny wykonywana jest kopia przyrostowa na macierz dyskową poza środowisko produkcyjne. Weryfikacja wykonywana jest przez administratora systemu.

Przechowywanie elektronicznych nośników i dokumentów zawierających dane osobowe - zabezpieczenia informatyczne

Zabezpieczenie elektronicznych nośników informacji

1. Nośniki danych są przechowywane w miejscu niedostępnym dla osób nieupoważnionych, zabezpieczone w sposób uniemożliwiający dostęp do nich osób nieuprawnionych z uwzględnieniem ryzyka zagrożenia pożaru bądź zalania.

2. Zabrania się wynoszenia poza obszar organizacji nośników danych, w szczególności dysków twardych. Zakaz ten nie ma zastosowania w przypadku otrzymania bezpośredniego pozwolenia od Kierownika danej jednostki lub Sekretarza Generalnego ZG PTTK w odniesieniu do Biura ZG PTTK.
3. W sytuacji przekazywania nośników z danymi osobowymi poza obszar organizacji należy 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.
4. Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania (chyba, że z powodu odrębnych przepisów należy dane zachowywać).
5. Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny w/g **Protokołu zniszczenia uszkodzonych nośników**.
6. Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).
7. Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczeniach ich (w szafach, biurkach) przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy tzw. Polityka czystego biurka.

Zabezpieczenie dokumentów i wydruków

1. Dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach zabezpieczonych fizycznie zgodnie z zasadami określonymi w Polityce.
2. Pracownicy są odpowiedzialni za zabezpieczenie dokumentów zawierających dane osobowe, które przetwarzają. Kierownicy działów są odpowiedzialni za kontrole pracowników w tym zakresie.
3. Pracownicy są zobowiązani do przestrzegania tzw. **Polityki czystego biurka,** czyli zabezpieczenie dokumentów w szafach zamkniętych na klucz, podczas nieobecności

w pomieszczeniu.

4. Pracownicy są zobowiązani do niszczenia dokumentów w niszczarkach po ustaniu celu ich przetwarzania.
5. Pracownicy są zobowiązani do niepozostawiania wydruków i ksero na urządzeniach bez nadzoru.

Oprogramowania antywirusowe- zabezpieczenia informatyczne

Ochrona antywirusowa

1. Za instalację ochrony antywirusowej odpowiada Główny Informatyk (ASI).
2. Oprogramowanie antywirusowe jest programem licencjonowanym, a ilość licencji jest dostosowana do liczby użytkowników.
3. Oprogramowanie antywirusowe zainstalowano na wszystkich komputerach pracowników.
4. Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
5. Użytkownicy zapewniają stałą aktywność programu antywirusowego. Program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
6. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić Głównego Informatyka (ASI).

Dostęp do sieci lokalnej

1. Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI
2. Stosowany jest Firewall sprzętowy zintegrowany z routerem i programowy na stacjach z Windows,
3. Dostęp do sieci wewnętrznej chronimy jest za pomocą routerów z zaimplementowanym i skonfigurowanym Fiewallem sprzętowym oraz włączoną translacją adresów (NAT).
4. Sieć bezprzewodową zabezpieczono technologią WPA2 PSK

Procedura wykonywania przeglądów i konserwacji

1. ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.

2. Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
3. Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
4. ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
5. ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty email.
6. ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania w celu ich niezwłocznego usunięcia.
7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
8. Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.
9. Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:
    a. wymontować nośniki z danymi osobowymi,
    b. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
    c. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

Postanowienia końcowe

1. Polityka Ochrony Danych Osobowych jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Administratorzy są obowiązani zapoznać się z zasadami wynikającymi z „Polityki ochrony danych osobowych wraz z instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe w Polskim Towarzystwie Turystyczno-Krajoznawczym”.
3. Zobowiązuje się Kierowników jednostek specjalistycznych i gospodarczych działających w

ramach osobowości prawnej Polskiego Towarzystwo Turystyczno-Krajoznawczego, do zapoznania wszystkich podległych pracowników z „Polityką ochrony danych osobowych wraz z instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe w Polskim Towarzystwie Turystyczno-Krajoznawczym”.

4. Zobowiązuje się administratorów do zapoznania wszystkich członków Oddziału oraz pracowników z przyjętym w Oddziale **Regulaminem Ochrony Danych Osobowych**.
5. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Ochrony Danych Osobowych dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
6. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.
7. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
8. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz.U. 2018 poz. 1000) oraz wydanych na jej podstawie aktów wykonawczych oraz Rozporządzenie 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).

Wykaz Załączników

Załącznik 1 Wykaz zbiorów danych osobowych

Załącznik 2 Analiza ryzyka

Załącznik 3 Rejestr czynności przetwarzania

Załącznik 4 Klauzule informacyjne

Załącznik 5 Umowa powierzenia danych osobowych

Załącznik 6 Ewidencja podmiotów zewnętrznych

Załącznik 7 Formularz rejestracji incydentu

Załącznik 8 Opis struktury zbiorów danych w systemach informatycznych wraz ze sposobem przepływu danych pomiędzy nimi.

Załącznik 9 Wyznaczenie IOD

Załącznik 10 Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych

Załącznik 11 Ewidencja osób upoważnionych