Załącznik do uchwały Prezydium ZG PTTK
nr 103/XIX/2020 z dnia 26 maja 2020 r.

REGULAMIN OCHRONY DANYCH OSOBOWYCH W BIURZE ZG PTTK ORAZ W JEDNOSTKACH SPECJALISTYCZNYCH I GOSPODARCZYCH DZIAŁAJĄCYCH W RAMACH OSOBOWOŚCI PRAWNEJ POLSKIEGO TOWARZYSTWA TURYSTYCZNO-KRAJOZNAWCZEGO

SPIS TREŚCI

Niniejszy regulamin stanowi wyciąg najistotniejszych zasad zawartych w Polityce Ochrony Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym.
Obowiązuje wszystkich pracowników, mających upoważnienia do przetwarzania danych osobowych.

1 Definicje

1. **Polityka** – to Polityka Ochrony Danych Osobowych w Polskim Towarzystwie Turystyczno-Krajoznawczym;
2. **Instrukcja** - to Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe w Polskim Towarzystwo Turystyczno-Krajoznawcze;
3. **Administrator**– Polskie Towarzystwo Turystyczno-Krajoznawcze, decydujący o celach i środkach przetwarzania danych osobowych;
4. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez Polskie Towarzystwo Turystyczno-Krajoznawcze, odpowiedzialna za organizację ochrony danych osobowych;
5. **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);
6. **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;
7. **Zbiór danych** - zestaw danych osobowych posiadający określoną strukturę, prowadzony wg określonych kryteriów oraz celów;
8. **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, **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**- nieodwracalna 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 -** 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** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
16. **Użytkownik** – pracownik Administratora posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

17. **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;
18. **Nośnik komputerowy (wymienny)** – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;
19. **Podmiot przetwarzający (Procesor)-** to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora;
20. **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;
21. **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;
22. **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.
23. **Prawo do sprostowania danych -** osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych,

które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

24. **Prawo do usunięcia danych - tzw. prawo do zapomnienia**; osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z okoliczności z katalogu w art. 17 RODO.
25. **Prawo do ograniczenia przetwarzania** - osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w przypadkach określonych w art.18 RODO.
26. **Prawo do przenoszenia danych** - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, w przypadkach określonych w art.20 RODO.
27. **Prawo do sprzeciwu** - osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych opartego na jej wcześniejszej zgodzie, w tym profilowania. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
28. **Współadministratorzy** - jeżeli co najmniej dwóch Administratorów wspólnie ustala cele i sposoby przetwarzania, są oni Współadministratorami. W drodze wspólnych uzgodnień Współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu Administratorzy ci podlegają.
29. **Podmiot przetwarzający** - podmiot, który jest odpowiedzialny za przetwarzanie

danych w imieniu administratora; podmiot musi zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

2 Zasady bezpiecznego użytkowania sprzętu IT

1. Sprzęt IT służący do przetwarzania zbioru danych osobowych składa się z komputerów stacjonarnych, laptopów, urządzeń przenośnych, serwera, drukarek.
2. Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
3. Użytkownik zobowiązany jest do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych a w szczególności zawartości ekranów monitorów.
4. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
5. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
6. Korzystanie ze sprzętu IT stanowiącego własność Polskiego Towarzystwa Turystyczno-Krajoznawczego poza miejscem wykonywania pracy, dozwolone jest tylko po uzyskaniu zgody Kierownika danej jednostki lub Sekretarza Generalnego (w odniesieniu do pracowników Biura ZG PTTK).
7. Korzystanie ze Sprzętu IT nie będącego własnością Polskiego Towarzystwa Turystyczno-Krajoznawczego w godzinach pracy, podczas wykonywania obowiązków służbowych, dopuszczalne jest tylko za zgodą Kierownika jednostki lub Sekretarza Generalnego ZG PTTK (w odniesieniu do pracowników Biura ZG PTTK).

3 Zasady korzystania z oprogramowania

1. Użytkownik zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.

2. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na Sprzęcie IT przez Administratora na swoje własne potrzeby ani na potrzeby osób trzecich.
3. Instalowanie jakiegokolwiek oprogramowania na Sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.
4. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych dyskietek, płyt CD, programów pobieranych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.
5. Użytkownicy nie mają prawa do zmiany parametrów systemu, które mogą być zmienione tylko przez osobę upoważnioną.
6. W przypadku naruszenia któregokolwiek z powyższych postanowień Administrator ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

4 Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (np. ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https:”.
7. Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
9. W zakresie dozwolonym przepisami prawa, Administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem stosowania wyżej opisanych zasad.
10. Ponadto, w uzasadnionym zakresie, Administrator zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.
11. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

5 Zasady korzystania z poczty elektronicznej

1. Pracownik otrzymuje indywidualny adres mailowy wedle wzorca: imie.nazwisko@pttk.pl
2. Pracownik jest zobowiązany do zachowania hasła w poufności i nieujawniania go osobom trzecim.
3. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
4. W przypadku przesyłania informacji wrażliwych wewnątrz organizacji bądź poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych plików, podpis elektroniczny).
5. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębną wiadomością elektroniczną (dalej: „mailem”) lub inną metodą, np. telefonicznie lub SMS-em.

6. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
7. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
8. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.
9. Nie należy otwierać stron internetowych wskazanych hiperlinkami w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
10. Użytkownicy nie powinni rozsyłać za pośrednictwem maila informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia", itp.
11. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
12. Użytkownicy powinni okresowo kasować niepotrzebne maile.
13. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”.
14. Program do obsługi poczty elektronicznej jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
15. Użytkownicy mają prawo korzystać z programu do obsługi poczty elektronicznej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Korzystanie z programu do obsługi poczty elektronicznej dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
17. Przy korzystaniu z programu do obsługi poczty elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
18. Użytkownicy nie mają prawa korzystać z programu do obsługi poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania i przepisów prawa.
19. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów,

dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

6 Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

7 Nadawanie upoważnień i uprawnień do przetwarzania danych osobowych

1. Za nadawanie upoważnień odpowiada Administrator.
2. Każdy użytkownik systemu przed nadaniem upoważnienia musi:
    a. zapoznać się z niniejszym Regulaminem;
    b. odbyć szkolenie z zasad ochrony danych osobowych;
    c. podpisać Oświadczenie o poufności.
3. IOD bądź Administrator nadaje pisemne upoważnienia Pracownikom i Zleceniobiorcom.
4. Upoważnienie nadawane jest do zbiorów w wersji papierowej i elektronicznej.
5. W przypadku, gdy upoważnienie udzielane jest do zbioru w wersji elektronicznej, nadawany jest użytkownikowi identyfikator w systemie.
6. W przypadku anulowania upoważnienia, identyfikator użytkownika jest blokowany w systemie.

8 Polityka haseł

1. Hasło dostępu do zbioru danych składa się co najmniej z 8 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).

2. Zmiana hasła do systemu następuje nie rzadziej, niż co 6 miesięcy oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
3. Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.
4. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
5. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
6. Hasło nie może być takie samo, jak 12 poprzednich haseł.
7. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
8. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom bez zgody Pracodawcy/Przełożonego.

9 Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, nieupoważnionym pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. **Polityka czystego ekranu**.
3. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
4. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy,
    b. zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

10 Postępowanie z elektronicznymi nośnikami zawierającymi dane osobowe

1. Elektroniczne nośniki, to: Wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora.
3. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane.
4. W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
5. Przekazywanie nośników z danymi osobowymi powinno być przeprowadzane z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji IOD.

11 Postępowanie z danymi osobowymi w wersji papierowej

1. Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych.
2. Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
3. Użytkownicy są zobowiązani do stosowania „**Polityki czystego biurka**”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
4. Użytkownicy zobowiązani są do przewożenia dokumentów w sposób zapobiegający ich kradzieży, zagubieniu lub utracie.
5. Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

12 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 12.1, 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 Danych.
5. Klucze zapasowe przechowywane są w odpowiednio zabezpieczonym pomieszczeniu, wskazanym przez Kierownika danej jednostki (patrz punkt 12.1). W obiekcie Senatorska 11 osobą odpowiedzialną za powyższe jest Sekretarz Generalny ZG PTTK.
6. Klucze do pomieszczeń szczególnie chronionych np. archiwum pozostają pod osobistym nadzorem osób upoważnionych. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.

7. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
8. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą odpowiedzialność za ich należyte zabezpieczenie.
9. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
10. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
11. 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 osobow**e** po zakończeniu pracy,
    - pozostawienia kluczy do pomieszczeń we wskazanym przez Kierownika danej jednostki lub Sekretarza Generalnego ZG PTTK (w odniesieniu do Biura ZG PTT) miejscu.
12. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

13 Zapewnienie poufności danych osobowych

1. Użytkownik zobowiązany jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez Administratora.
2. Użytkownik zobowiązany jest do niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.
3. Użytkownik zobowiązany jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne.

4. Zabrania się przekazywania w tym bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.

14 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Użytkownik zobowiązany jest do powiadomienia IOD lub ASI w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić IOD:
    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 na dane osobowe,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia IOD,
    g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
    h. telefoniczne próby wyłudzenia danych osobowych,
    i. kradzież komputerów lub CD, twardych dysków, pendrive 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.

15 Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z Regulaminu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z Regulaminem Ochrony Danych Osobowych może też być uznane przez Administratora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.