INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
PRZETWARZAJĄCYM DANE OSOBOWE
W FIRMIE

JACEK TURCZYNOWICZ
YACHTING JACEK TURCZYNOWICZ
ul. Gen. Józefa Zajączka 23/22, 01-505 Warszawa
NIP: 1231056768, REGON: 142763110

.....	.....	.....
pieczęć firmowa	podpis administratora danych osobowych	data

Rozdział 1

Postanowienia ogólne

Ilekroć w Instrukcji jest mowa o:

1. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.),
2. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań,
3. **zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
6. **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
7. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
8. **administratorze danych** – rozumie się przez to Jacka Turczynowicza, prowadzącego działalność gospodarczą pod firmą Yachting Jacek Turczynowicz, NIP: 1231056768, REGON: 142763110,
9. **administratorze systemu** – rozumie się przez to osobę zarządzającą systemem informatycznym przetwarzającym dane osobowe, tj. Jacka Turczynowicza, prowadzącego działalność gospodarczą pod firmą Yachting Jacek Turczynowicz, NIP: 1231056768, REGON: 142763110,
10. **użytkowniku systemu** – rozumie się przez to osobę, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie,

11. **elektronicznym nośniku** – rozumie się przez to elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu jego ponownego odtworzenia w systemie informatycznym,

12. **zgodzie 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; zgoda może być odwołana w każdym czasie,

13. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem,

14. **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego,

15. **obszarze przetwarzania danych** – należy przez to rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,

16. **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,

17. **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,

18. **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi,

19. **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Rozdział 2
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, zastosowano wysoki poziom bezpieczeństwa.

2. Osobą odpowiedzialną za nadawanie uprawnień w systemie informatycznym jest administrator danych.

3. Procedura nadawania, modyfikowania i odbierania uprawnień użytkownikowi w systemie informatycznym obejmuje w kolejności:

a) zapoznanie osoby z przepisami dotyczącymi ochrony danych osobowych oraz procedurami bezpieczeństwa systemu informatycznego,

b) nadanie upoważnienia do przetwarzania danych osobowych oraz odebranie oświadczenia o zachowaniu poufności danych osobowych i przestrzeganiu wewnętrznej dokumentacji ochrony danych osobowych,

c) zwrócenie się z wnioskiem do administratora systemu o nadanie uprawnień w systemie informatycznym w niezbędnym zakresie,

d) nadanie uprawnienia w systemie informatycznym w niezbędnym zakresie, po zweryfikowaniu przez administratora systemu treści upoważnienia do przetwarzania danych osobowych lub innej podstawy prawnej pozwalającej na przydzielenie uprawnień,

e) modyfikację i odbieranie uprawnień użytkownika w systemie informatycznym.

4. Procedura rejestrowania uprawnień użytkownika w systemie informatycznym jest przeprowadzana przez administratora tego systemu i obejmuje w kolejności:

a) przypisanie indywidualnego identyfikatora użytkownika w systemie informatycznym do konkretnej osoby, przy zapewnieniu, że identyfikator ten nie był wcześniej przydzielony innemu użytkownikowi, wraz z datą przyznania i odebrania uprawnień,

b) przypisanie zakresu przydzielonych uprawnień w systemie informatycznym do konkretnego identyfikatora użytkownika.

Rozdział 3
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W zakresie uwierzytelniania użytkownika w systemie informatycznym zastosowano identyfikator i hasło.

2. Hasło zastosowane do uwierzytelnienia użytkownika w systemie informatycznym składa się z co najmniej 8 znaków, w tym musi zawierać małe i duże litery oraz liczbę lub znak specjalny. Hasło jest zmieniane w cyklach nie dłuższych niż 30 dni.

3. Zmiana hasła dokonywana jest przez użytkownika manualnie.

4. Hasło zastosowane do uwierzytelnienia administratora systemu w systemie informatycznym składa się z co najmniej 8 znaków, w tym musi zawierać małe i duże litery oraz liczbę lub znak specjalny. Każdorazowe użycie konta administratora systemu jest odnotowywane w tym systemie w formie logów dostępowych. Hasło jest zmieniane w cyklach nie dłuższych niż 6 miesięcy.

5. Użytkownicy systemów informatycznych są zapoznawani z zagrożeniami wynikającymi ze stosowania haseł jako formy ich uwierzytelniania w systemie informatycznym.

Rozdział 4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu informatycznego

1. Przed rozpoczęciem pracy w systemie informatycznym użytkownik weryfikuje bezpieczeństwo treści wyświetlanych na ekranie ze względu na przebywanie osób nieupoważnionych w obszarze przetwarzania.
2. Przed przerwaniem pracy w systemie informatycznym i tymczasowym odejściem od punktu dostępowego systemu informatycznego użytkownik blokuje swój dostęp poprzez manualne uruchomienie wygaszacza ekranu chronionego hasłem.
3. Po zakończeniu pracy w systemie informatycznym użytkownik zamyka system informatyczny, do którego ma dostęp.

Rozdział 5

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Kopie wykonywane są na dysku zewnętrznym lub nośniku elektronicznym typu pendrive.
2. W przypadku zużycia lub uszkodzenia nośnika zewnętrznego lub elektronicznego, należy uszkodzony nośnik zutylizować w sposób uniemożliwiający odczytanie danych na nim zawartych.

Rozdział 6

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

1. W przypadku korzystania z elektronicznych nośników zawierających dane osobowe, w szczególności takich jak płyty CD/DVD/BR, pendrive'y, Karty SD, zewnętrzne dyski, taśmy magnetyczne, są one przechowywane w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym.
2. W celu usunięcia danych osobowych z elektronicznego nośnika danych użytkownicy stosują metodę trzykrotnego nadpisania pełnej zawartości nośnika danymi niezawierającymi danych osobowych.
3. W przypadku zużycia lub uszkodzenia elektronicznego nośnika zawierającego kopie zapasowe, w celu jego utylizacji uszkadza się go mechanicznie w taki sposób, aby odtworzenie danych było niemożliwe.

Rozdział 7

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. W systemie informatycznym zostało zainstalowane automatycznie aktualizujące się oprogramowanie antywirusowe.
2. Na styku sieci wewnętrznej z siecią publiczną zastosowano zaporę systemową w ramach programu antywirusowego Wise Registry Cleaner oraz zaporę sieciową na routerze Huawei HB434666RBC.
3. Użytkownicy systemu niezwłocznie informują administratora systemu o zagrożeniach wskazywanych przez oprogramowanie antywirusowe.

Rozdział 8

Sposób odnotowania informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

Administrator danych udostępnia dane odbiorcom danych samodzielnie tj. z pominięciem przyznawania dostępu odbiorcom danych do systemu informatycznego administratora danych.

Rozdział 9

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Administrator systemu informatycznego prowadzi okresowe przeglądy systemu informatycznego w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo danych przetwarzanych z jego wykorzystaniem.
2. Administrator systemu przeprowadza ww. przegląd nie rzadziej niż raz na 5 lat.
3. W przypadku konieczności dokonania naprawy elementu infrastruktury systemu informatycznego przez osobę nieupoważnioną (np. zewnętrzny serwis informatyczny), wszelkie czynności dokonywane są pod bezpośrednim nadzorem osób upoważnionych.

Rozdział 10

Postanowienia końcowe

1. Wszelkie zasady opisane w niniejszej Instrukcji są przestrzegane przez użytkowników i administratorów systemów ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Instrukcja obowiązuje od dnia jej zatwierdzenia przez administratora danych.