POLITYKA PRYWATNOŚCI

§1.

Celem Polityki Ochrony Danych Osobowych, zwanej dalej Polityką Ochrony Danych, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania informacji zawierającej dane osobowe.

§2.

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1) Jednostka – Administrator danych osobowych, którego niniejszy dokument dotyczy,
2) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) przetwarzanie danych osobowych – gromadzenie, utrwalanie przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
4) Użytkownik – osoba upoważniona do przetwarzania danych osobowych,
5) Administrator systemów informatycznych – osoba upoważniona do zarządzania systemem informatycznym, jeżeli została powołana,
6) system informatyczny – system przetwarzania danych w wraz z zasobami ludzkimi, technicznymi oraz finansowymi, który dostarcza i rozprowadza informacje,
7) zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

§3.

1) Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2) Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
   1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
   2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
   3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
   4) Zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3. Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
   1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,

2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

§4.

1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§5.

Politykę stosuje się do:

1. danych osobowych przetwarzanych w systemie informatycznym,
2. wszystkich informacji dotyczących danych pracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów,
3. wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5. rejestru osób dopuszczonych do przetwarzania danych osobowych,
6. innych dokumentów zawierających dane osobowe.

§6.

1. Zakresy określone przez dokumenty Polityki mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
   2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
   3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, konsultanci, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

§7.

Dokumenty Polityki Ochrony Danych ustanawiają metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

§8.

Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Jednostce zasad ochrony danych osobowych.

§9.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

§10.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§11.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

§12.

Zarząd może powołać Inspektor danych osobowych. W przypadku nie powołania Inspektora, wszystkie wskazane w niniejszym oraz innych dokumentach dotyczących ochrony danych osobowych, zadania wykonuje Zarząd Jednostki.

§13.

Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Jednostki.

§14.

Administrator/Inspektor danych osobowych (jeżeli został powołany):

1. odpowiada za realizację ustawy o ochronie danych osobowych,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Jednostki,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,
6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Jednostki,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,

8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, palmtopach, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia Administratora systemów informatycznych o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi rejestr zbiorów danych osobowych Jednostki (przetwarzanych metodą tradycyjną lub w systemach informatycznych).
17. Odpowiada za określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych,
18. Odpowiada za określenie pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
19. Odpowiada za zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
20. Odpowiada za działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,

§15.

Administrator Systemów Informatycznych (jeżeli jest powołany) odpowiedzialny jest za:

1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego,
5. konfigurację i administrację oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

10. przyznawanie na wniosek Inspektora danych osobowych ściśle określonych praw dostępu do informacji w danym systemie,
11. wnioskowanie do Inspektora danych osobowych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12. zarządzanie licencjami, procedurami ich dotyczącymi,
13. prowadzenie profilaktyki antywirusowej.

§ 16.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich. Urządzenia informatyczne powinny być zabezpieczone w sposób opisany w niniejszym dokumencie.

§17.

1. Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy niszczyć w stopniu uniemożliwiającym ich odczytanie.
2. Urządzenia, dyski lub inne informatyczne nośniki danych, przeznaczone do naprawy, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Inspektora danych osobowych.

§18.

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy z zamkami,
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   - osobą odpowiedzialną za bezpieczeństwo danych jest Inspektor Danych Osobowych (IDO), jeżeli jest powołany
   - Jeżeli są powołani Inspektor Danych Osobowych, Administrator Systemu Informatycznego i wszyscy powołani administratorzy na bieżąco kontrolują pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie przyznane przez Inspektora Danych Osobowych.
5. W trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych.

6. W trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione.
7. Po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

INFORMACJA DLA OSÓB, KTÓRYCH DANE PRZETWARZANE SĄ NA PODSTAWIE ZGODY LUB UMOWY

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz.Urz. UE L 119, s. 1) – dalej RODO − informujemy, że:

1) Akademia Jachtingu Maciej Biechowski ul. Tatrzańska 25/4 81-328 Gdynia NIP 588-184-42-31 Kontakt telefoniczny: +48 507 455 798 Adres email: info@akademia-jachtingu.pl jest administratorem Pana/Pani danych osobowych.
2) Jako administrator będziemy przetwarzać Pana/Pani dane na podstawie Pana/Pani dobrowolnie wyrażonej zgody w celu:
   - Przeprowadzenia egzaminów;
   - Ubezpieczenia podczas korzystania z naszych usług;
   - Obowiązków księgowo-kadrowych;
   - Realizacji zamówień;
   - Przesyłania newslettera;
   - Statystycznym;
   - Przeprowadzania konkursów;
   - Prowadzenia strony internetowej;
   - Prowadzenia korespondencji handlowej;
   - Marketingowych.
3) W każdej chwili przysługuje Panu/Pani prawo do wycofania zgody na przetwarzanie swoich danych osobowych, ale cofnięcie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody udzielonej przed jej wycofaniem.
4) W każdej chwili przysługuje Panu/Pani prawo do wniesienia sprzeciwu wobec przetwarzania danych jw. Przestaniemy przetwarzać Pana/Pani dane w tych celach, chyba że będziemy w stanie wykazać, że w stosunku do Pana/Pani danych istnieją dla nas ważne prawnie uzasadnione podstawy, które są nadrzędne wobec Pana/Pani interesów, praw i wolności lub Pana/Pani dane będą nam niezbędne do ewentualnego ustalenia, dochodzenia lub obrony roszczeń.
5) Do Pana/Pani danych mogą też mieć dostęp podmioty przetwarzające te dane na nasze zlecenie a świadczące usługi z zakresu mi.in informatycznego, księgowo-podatkowego, prawnego.

6) Zgodnie z RODO, przysługuje Panu/Pani:
   a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
   b) prawo do sprostowania (poprawiania) swoich danych;
   c) prawo do usunięcia danych, ograniczenia przetwarzania danych;
   d) prawo do wniesienia sprzeciwu wobec przetwarzania danych;
   e) prawo do przenoszenia danych;
   f) prawo do wniesienia skargi do organu nadzorczego.

7) Pani/Pana dane osobowe będą przechowywane przez okres niezbędny do realizacji celu przetwarzania, a nie krócej niż w okresie określonym przepisami prawa.

8) Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

9) Dane nie będą przekazywane poza Europejski Obszar Gospodarczy, ani do innych organizacji międzynarodowych. Administrator jednocześnie informuje, że w celu ochrony danych przed ich utratą zostały wdrożone odpowiednie procedury, w tym procedura sporządzania kopii zapasowych.

10) W procesie przetwarzania danych możemy podejmujemy decyzje w sposób zautomatyzowany na podstawie danych, które posiadamy. W oparciu o te informacje przypisany będzie profil osobowy istotny z punktu widzenia możliwości zaoferowania naszych usług lub usług naszych partnerów oraz wysokości upustów, które możemy Ci przyznać. Decyzje te są podejmowane automatycznie. Decyzje podejmowane w ten sposób mają wpływ na dostępność produktów lub usług/doboru oferowanych produktów.

11) Profilowanie oznacza przetwarzanie danych osobowych polegające na wykorzystaniu danych osobowych do oceny niektórych cech, w szczególności do analizy lub prognozy aspektów dotyczących osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Profilujemy w celu dobrania oferty pod Pana/Pani preferencje.