POLITYKA BEZPIECZEŃSTWA INFORMACJI

Firma
POMORSKI KLUB SPORTOWY

SPIS TREŚCI

Podstawa prawna

Rozporządzenie Ogólne o Ochronie Danych Osobowych – RODO, tj. Rozporządzenie Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu tych danych.

Powołanie Inspektora Ochrony Danych Osobowych IOD
Powołanie IOD dla Firmy nie jest wymagane, w Firmie nie powołano Inspektora Ochrony Danych Osobowych.

Politykę bezpieczeństwa przygotowano zgodnie z posiadaną wiedzą, z dochowaniem należytej staranności aby spełnić wymogi rozporządzenia RODO

Podstawowe pojęcia

Firma – w tym dokumencie jest rozumiana jako „POMORSKI KLUB SPORTOWY” działająca pod adresem L. WARYŃSKIEGO 37/5A, 80-433 GDAŃSK, identyfikująca się numerami NIP: 5842738720, REGON: 222175928, KRS: 0000525072.

Polityka – rozumiana jako Polityka bezpieczeństwa systemu informatycznego, obowiązująca w Firmie

Użytkownik systemu – osoba upoważniona do dostępu i przetwarzania danych osobowych w systemie

Login – to identyfikator użytkownika tworzony na potrzeby identyfikacji i przydzielenia praw do systemu

System – Zespół współpracujących ze sobą programów, urządzeń i procedur, związanych z przetwarzaniem plików, programów, różnych danych i danych osobowych

Przetwarzanie danych – rzetelne i w sposób przejrzysty, dopisywanie, poprawianie, utrwalanie, usuwanie danych osobowych w zbiorach danych.

Zabezpieczenie danych – wdrożenie i wykorzystywanie znanych i dostępnych środków technicznych i organizacyjnych mających za zadanie zapewnienie ochrony danych przed ich nieuprawnionym dostępem i przetwarzaniem.

Sieć lokalna – wewnętrzna sieć komputerowa, połączone na obszarze Firmy znane komputery i urządzenia sieciowe będące własnością Firmy

Sieć publiczna – sieć internetowa funkcjonująca poza siedzibą, routerem Firmy, niebędąca siecią wewnętrzną.

Administrator - administratorem, właścicielem danych jest Firma „POMORSKI KLUB SPORTOWY” działająca pod adresem L. WARYŃSKIEGO 37/5A, 80-433 GDAŃSK, identyfikująca się identyfikująca się numerami NIP: 5842738720, REGON: 222175928, KRS: 0000525072.

Par. 1 – DANE
Identyfikacja danych osobowych

Dane osobowe przetwarzane przez „POMORSKI KLUB SPORTOWY” działająca pod adresem L. WARYŃSKIEGO 37/5A, 80-433 GDAŃSK, identyfikująca się numerami NIP: 5842738720, REGON: 222175928, KRS: 0000525072 są danymi zwykłymi i nie są to dane wrażliwe.

Firma przetwarza dane osobowe tylko na potrzeby obsługi spraw kadrowo-płacowych, wystawianych faktur, świadczonych usług, prowadzeniu korespondencji e-mail.

Dane pracowników są zapisane w programie Microsoft Excel oraz Rewizor, za pomocą którego Firma spełnia obowiązek wynikający z przepisów o ubezpieczeniach społecznych.

W programie Microsoft Excel oraz Rewizor zapisane są dane osobowe wymagane przepisami o ubezpieczeniu społecznym.

Wynagrodzenia, listy płac są przeliczane za pomocą oprogramowania Rewizor.

Baza kontrahentów, zapisana jest w oprogramowaniu Microsoft Excel, utrzymywanym na serwerze Firmy, w bazie oprogramowania zapisane są dane:

- nazwa Firmy,
- imię i nazwisko właściciela, jeśli występuje w nazwie,
- adres pod którym prowadzona jest działalność Firmy,
- kraj,
- numer identyfikacji podatkowej NIP,
- adres email,
- telefon,

W programie pocztowym zapisane są:

- imię nazwisko,
- Firma,
- adres email,
- telefon do osoby upoważnionej do kontaktu.

Zasadność przetwarzanych danych

Zgodnie z art. 6 pkt. b, RODO, przetwarzanie danych osobowych klientów, kontrahentów oraz pracowników Firmy jest niezbędne w prowadzonej działalności gospodarczej.

Firma korzysta z przetwarzanych danych osobowych na potrzeby kampanii marketingowych i może rozsyłać emaile w celu marketingowym.

Firma nie przetwarza danych nadmiarowych.

Dane osobowe są przechowywane przez cały czas prowadzenia działalności.

W określonym przypadku będą usunięte z bazy danych na wyraźne życzenie zainteresowanej osoby, jednak życzenie to nie może to stać w sprzeczności wobec obowiązujących przepisów księgowych i podatkowych.

Obowiązek informacyjny - oświadczenie
Firmy i osoby których dane są przetwarzane są informowane o fakcie przetwarzania danych.

Treść oświadczenia zawartego w umowie jest ustalana indywidualnie

Wystawiane reklamy, ogłoszenia, cenniki, itp. zawierają informację:

Administratorem, podmiotem przetwarzającym dane osobowe, jest „POMORSKI KLUB SPORTOWY”

W korespondencji email, w stopce umieszczony jest dopisek:

Administratorem, podmiotem przetwarzającym dane osobowe, jest „POMORSKI KLUB SPORTOWY”

Par. 2 – INFRASTRUKTURA

Wykaz miejsc w których przetwarzane są dane osobowe

LP.	ADRES	OZNACZENIE	ZABEZPIECZENIE
1.	L. WARYŃSKIEGO 37/5A, 80-433 GDAŃSK	DELL 1/2014	Komputer TYPU LAPTOP zabezpieczony hasłem.

Zbiory danych przetwarzane w systemach informatycznych

ZBIÓR DANYCH BAZA DANYCH	PROGRAM INFORMATYCZNY UŻYWANY DO PRZETWARZANIA DANYCH	MIEJSCE PRZETWARZANIA	ODPOWIEDZIALNY
Baza klientów	Microsoft Excel	Komputer Firmowy	Upoważnione osoby
Baza kontrahentów	Microsoft Excel	Komputer Firmowy	Upoważnione osoby
Katalog z elektronicznymi wersjami dokumentów	Microsoft Excel, Word	Komputery Firmowy	Upoważnione osoby
Oferty	Microsoft Excel, Word	Komputer Firmowy	Upoważnione osoby
Korespondencja e-mail	Program pocztowy, witryna internetowa.	Komputer Firmowy	Upoważnione osoby
Sprawy kadrowo-płacowe	Rewizor	Firma Zewnętrzna – wolontariat na rzecz stowarzyszenia PKS	Upoważnione osoby
Deklaracje VAT	Rewizor	Firma Zewnętrzna – wolontariat na rzecz stowarzyszenia PKS	Upoważnione osoby

Zbiory danych przetwarzane w sposób tradycyjny.

Ewidencja spraw kadrowo-płacowych jest przetwarzana również przez program komputerowy Rewizor – wolontariat w tym zakresie, na rzecz stowarzyszenia, prowadzi LAUREA Usługi Finansowo Administracyjne Laura Szatkowska z siedzibą w Koleczkowie, ul. Słoneczna 16. NIP: 5891437664, REGON: 2221759928.

Dokumentacja w wersji papierowej, przechowywana jest w zamykanym pokoju archiwum, w segregatorach.

Dane zawarte w umowach nie są udostępniane, ani przetwarzane.

Par. 3 – BEZPIECZEŃSTWO

Zagrożenia i ryzyko w przetwarzaniu danych

W Firmie ustalono następującą skalę ryzyka naruszenia danych:

0 - brak ryzyka, nie zauważono ryzyka w tym obszarze
1 - bardzo niskie ryzyko, ryzyko nie istnieje, ale nie wyklucza się że jest taka możliwość
2 - niskie ryzyko, ryzyko istnieje, ale nie występuje w badanej przestrzeni
3 - średnie ryzyko, istnieją przesłanki do stwierdzenia iż ryzyko może wystąpić
4 - ryzyko umiarkowane, ryzyko wystąpienia zdarzenia jest wysoce prawdopodobne
5 - duże ryzyko, ryzyko występuje, może wystąpić często

Ocena ryzyka.

MIEJSCE PRZETWARZANIA	RYZYKA	OCENA RYZYKA	zalecenia
Komputer Firmowy	Zdarzenia losowe, pożar, zalanie	1	
Komputer Firmowy	Kradzież z włamaniem	3	
Komputer Firmowy	Zawirusowanie	3	
Komputer Firmowy	Włamanie przez narzędzia hackerskie	3	
Komputer Firmowy	Włamanie do pomieszczenia	2	
Pendrive	Zagubienie	0	
Dokumenty kadrowo-płacowe	Kradzież	0	
	Zagubienie dokumentów	0	

Określenie ryzyk

- Poziom naruszenia ryzyka bezpieczeństwa danych w Firmie jest stosunkowo niski. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla określonych systemów, zbiorów i kategorii danych osobowych.

- Komputery pracują w sieci wewnętrznej, za routerem, bez bezpośredniego dostępu do Internetu. Aktualizacje oprogramowania instalowane są na bieżąco. Komputery posiada aktualizowane oprogramowanie antywirusowe.

- Pen Drive-y nie są wykorzystywane w Firmie - nie przenosi się na nich danych osobowych.

- Poczta elektroniczna utrzymana jest na zabezpieczonym serwerze.

- Domena zarejestrowana jest na serwerze Firmy: LinuxPl.com, H88 S.A. Ul. F. Roosevelta 22, 60-829 Poznań.

- Strona internetowa – opublikowana strona internetowa jest zgodna z przyjętymi wymogami dla witryn internetowych www. Firma nie prowadzi sprzedaży internetowej.

Zabezpieczenia systemu - środki techniczne i organizacyjne stosowane w przetwarzaniu danych,

Realizując politykę bezpieczeństwa informacji zgodną z RODO, Firma zapewnia:

- poufność, tj. przetwarzane informacje nie są udostępniane lub ujawniane nieupoważnionym osobom, podmiotom lub procesom.
- integralność, przetwarzane dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany,

Do celów biznesowych, w elektronicznym przetwarzaniu danych mają zastosowanie komputery, z systemem operacyjnym Windows 7. System operacyjny aktualizowany jest automatycznie i na bieżąco.

- na komputerach wykorzystuje się licencjonowane oprogramowanie
- jako środki bezpieczeństwa stosuje się:

a) fizyczne zabezpieczenie dostępu do pomieszczeń, komputerów,
b) zainstalowane na komputerze aktywne oprogramowanie antywirusowe,
c) złożone hasło dostępu pozwalające na uruchomienie komputera tylko przez upoważnione osoby

- każdy system, oprogramowanie, wykorzystywane do przetwarzania danych osobowych, posiada dodatkowo własny system zabezpieczenia kont i uprawnień użytkowników zabezpieczonych hasłem.
- tworzone kopie zapasowe są zapisane na dysku serwera.

Par. 4 – PROCEDURY

Zapewnienie prawa do bycia zapomnianym, usunięcie danych

Zgodnie z art. 17 RODO, w przypadku gdy osoba fizyczna skorzysta z uprawnienia do bycia zapomnianym, lub zażąda zaprzestania przetwarzania danych, ich usunięcia, znajdują postanowienia niniejszego paragrafu.

Jeżeli zaistnieje zdarzenie kwalifikujące kontakt z Firmą jako osobę fizyczną, zgodnie z ww. Rozporządzeniem i na wniosek osoby zainteresowanej, administrator spełni żądanie, zmieni w bazie danych Firmy wnioskowane dane osobowe lub zgodnie z prośbą, dane zostaną usunięte.

Osoba składająca wniosek otrzyma informację o statusie swojego wniosku niezwłocznie, ale nie później niż w czasie 30 dni.

Korespondencja będzie realizowana w sposób elektroniczny, na adres email wnioskodawcy, lub w sposób wskazany przez zainteresowaną stronę.

Jeżeli zmiana danych osobowych nie jest zgodna z innymi obowiązującymi przepisami, np. ustawą o VAT, polityką rachunkowości, bądź naruszy integralność danych, to zainteresowana osoba zostanie uprzedzona o braku możliwości spełnienia żądania do bycia zapomnianym, bądź o braku możliwości usunięcia danych z systemu.

Sprostowanie danych

W przypadku gdy do Firmy wpłynie wniosek o sprostowanie danych, jeżeli wniosek ten będzie zasadny, dane zostaną poprawione.

Osoba składająca wniosek otrzyma informację o statusie swojego wniosku niezwłocznie, ale nie później niż w czasie 30 dni.

Udostępnienie i powierzenie danych osobowych

Na pisemny wniosek upoważnionej Firmy, instytucji, zgodnie z przepisami prawa, dane osób, których on dotyczy, mogą być udostępnione.

Naruszenie danych

W przypadku stwierdzenia naruszenia danych, bądź nieuprawnionego dostępu, niezwłocznie zostaną podjęte kroki:
- identyfikacja problemu i miejsca naruszenia dostępu,
- zgłoszenie naruszenia do GIODO,
- naprawa przyczyny wystąpienia naruszenia.

Nadawanie uprawnień do przetwarzania danych

Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników, odpowiada właściciel Firmy, lub upoważniona przez niego osoba.

Upoważniony użytkownik, właściciel, jest odpowiedzialny za przetwarzanie danych osobowych.

Właściciel, osoba upoważniona, zobowiązuje się stosownym oświadczeniem, do zachowania w tajemnicy, wszelkich danych osobowych w posiadanie których wejdzie, w ramach prowadzonej działalności gospodarczej.