



## Informacje o zagrożeniach związanych ze świadczoną usługą

Szanując prywatność oraz prawa naszych Klientów, NETICA, w związku ze świadczeniem usług telekomunikacyjnych, przetwarza tylko te dane, do których przetwarzania jest uprawniona lub zobowiązana na podstawie odpowiednich przepisów prawa. Zastosowanie mają tu w szczególności Ustawa Prawo Telekomunikacyjne z dnia 16 lipca 2004 r. (Dz.U. Nr 171, poz. 1800) z późniejszymi zmianami oraz Ustawa o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 r. (Dz.U. Nr 133, poz. 883) z późniejszymi zmianami. Dane przetwarzane są również na podstawie aktualnych zgód wyrażonych przez Abonentów w szczególności podczas zawierania umowy oraz podczas czynności obsługowych. Odbywa się to tylko i wyłącznie w ściśle ustalonym zakresie danych, okresie i celu. Dane przetwarzane są przez naszych pracowników w systemach informatycznych z zachowaniem najwyższej jakości wymagań określonych w wewnętrznych instrukcjach i procedurach. Dane objęte tajemnicą telekomunikacyjną udostępniane są wyłącznie uprawnionym ustawowo podmiotom. Niezależnie od powyższego użytkownicy usług telekomunikacyjnych, a w szczególności użytkownicy usługi dostępu do Internetu poprzez stosowanie się do niżej wymienionych zasad mogą dodatkowo chronić swoją prywatność oraz dane osobowe podczas korzystania z usług:

Korzystając z serwisów wymagających rejestracji i podania Twoich danych, w tym danych osobowych, zawsze zwracaj uwagę na wiarygodność takich serwisów. Sprawdź czy Twoje prawa są odpowiednio chronione w umowie czy regulaminie określającym zasady korzystania z tego serwisu. Podawaj tylko te dane, które związane są ze świadczoną usługą.

Publikując swoje dane osobowe oraz inne informacje o sobie w Internecie, w szczególności w serwisach społecznościowych, bądź świadomy, że upublicznienie tych danych, informacji pozbawia Cię skutecznych narzędzi ochrony tych danych. Rób to rozważnie. Twoje dane mogą być wykorzystane w złej wierze przez innych użytkowników Internetu.

Korzystając z komunikatorów, poprzez które wymieniasz prywatne, poufne informacje z rodziną, przyjaciółmi, zwracaj uwagę czy komunikatory te dysponują mechanizmami szyfrowania wysyłanych komunikatów.

Korzystając z poczty elektronicznej wybieraj tylko sprawdzonych i wiarygodnych usługodawców, zapewniających tajemnicę korespondencji.

Nie pobieraj z Internetu (także poprzez pocztę elektroniczną) i nie uruchamiaj oprogramowania z niepewnego, w szczególności nieznanego źródła. Oprogramowanie takie może zawierać złośliwe oprogramowanie.

Korzystając z serwisów bankowości elektronicznej zwracaj zawsze uwagę na to, czy wyświetlony adres URL jest prawidłowy. Sprawdzaj czy logowanie się do takiego serwisu jest realizowane przez bezpieczne połączenie (protokół https).

Zabezpieczając swój dostęp do usług świadczonych drogą elektroniczną zawsze używaj bezpiecznych i silnych haseł. Nie zapisuj haseł w plikach umieszczonych w komputerze. Nie zdradzaj haseł innym osobom. Usługodawca nigdy, wyłączając proces logowania, nie powinien Cię prosić o podanie takiego hasła (w szczególności w korespondencji elektronicznej). Jeśli tak się dzieje może to świadczyć o próbie wyłudzenia hasła.

Wyposaż swój komputer w oprogramowanie antywirusowe i zaporę sieciową (firewall). Większość z dostępnego oprogramowania antywirusowego analizuje i zgłasza większość z wymienionych powyżej zagrożeń.