Informacja o zagrożeniach związanych ze świadczoną usługą telekomunikacyjną.

W związku ze świadczeniem usług telekomunikacyjnych Częstochowska Spółdzielnia Mieszkaniowa „Nasza Praca" dla zachowania prywatności i danych osobowych Abonentów przetwarza tylko te dane, do których przetwarzania jest uprawniona lub zobowiązana na podstawie obowiązujących przepisów prawa, w szczególności Ustawy z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne (Dz.U. Nr 171, poz. 1800 z późn. zm.) oraz Ustawy z dnia 29 sierpnia 1997 r. o Ochronie Danych Osobowych (Dz.U. Nr 133, poz. 883 z późn. zm.).

Dane przetwarzane są również na podstawie zgody wyrażonej przez Abonenta podczas zawierania umowy i w czasie jego obsługi, wyłącznie w zakresie określonym w umowie i regulaminie.

Dane przetwarzane są przez pracowników Spółdzielni w systemach informatycznych zgodnie z wymaganiami określonymi w wewnętrznych procedurach i instrukcjach, przygotowanych dla zapewnienia bezpieczeństwa przetwarzanych danych. Dane objęte tajemnicą telekomunikacyjną udostępniane są wyłącznie uprawnionym prawnie podmiotom.

Niezależnie od powyższego Abonenci usług telekomunikacyjnych, a w szczególności użytkownicy usługi dostępu do Internetu mogą dodatkowo chronić swoją prywatność oraz dane osobowe podczas korzystania z usług poprzez stosowanie się do niżej wymienionych zasad.

<u>Zasady ochrony przez Abonentów swojej prywatności oraz danych osobowych:</u>

1) Korzystając z serwisów wymagających rejestracji i podania Twoich danych, w tym danych osobowych, zawsze zwracaj uwagę na wiarygodność takich serwisów. Sprawdzaj, czy Twoje prawa są odpowiednio chronione w umowie i regulaminie określającym zasady korzystania z danego serwisu i podawaj tylko takie dane, które związane są ze świadczoną usługą.

2) Publikując własne dane osobowe, czy inne informacje personalne w Internecie, a w szczególności w serwisach społecznościowych, musisz mieć świadomość, że dane mogą być wykorzystane w złej wierze przez innych użytkowników Internetu. Rób to rozważnie, ponieważ upublicznienie danych może Cię pozbawić narzędzi skutecznej obrony tych danych.

3) Korzystając z poczty elektronicznej wybieraj tylko sprawdzonych i wiarygodnych usługodawców, którzy zapewniają tajemnicę korespondencji.

4) Korzystając z serwisów bankowości elektronicznej należy zawsze zwracaj uwagę czy logowanie do takiego serwisu jest realizowane przez bezpieczne połączenie przy użyciu protokołu https oraz czy wyświetlony w przeglądarce adres URL jest prawidłowy.

5) Zawsze zabezpieczaj dostęp do usług świadczonych drogą elektroniczną poprzez używanie silnych haseł (ciąg minimum 12 znaków zawierających minimum jedną wielką i małą literę oraz znak specjalny). Nie wolno zapisywać haseł w plikach zapisanych w komputerze. Pamiętaj, że usługodawca nigdy, wyłączając proces logowania, nie prosi o podanie hasła – w szczególności w korespondencji elektronicznej. Jeśli tak się dzieje może to świadczyć o próbie wyłudzenia hasła.

6) W trakcie korzystania z komunikatorów internetowych zwracaj uwagę, czy dane komunikatory dysponują mechanizmami szyfrowania wysyłanych komunikatów.

7) Nie pobieraj z Internetu i nie uruchamiaj oprogramowania z niepewnego, w szczególności nieznanego źródła. Oprogramowanie takie może zawierać wirusy (złośliwe oprogramowanie). Dotyczy to również programów dostarczanych poprzez pocztę elektroniczną.

8) Zainstaluj w komputerze oprogramowanie antywirusowe i zaporę sieciową tzw. firewall. Większość z dostępnych programów antywirusowych analizuje i zgłasza większość z wymienionych powyżej zagrożeń.