

INFORMACJE O ZAGROŻENIACH ZWIĄZANYCH ZE ŚWIADCZONĄ USŁUGĄ, W TYM O SPOSOBACH OCHRONY BEZPIECZEŃSTWA, PRYWATNOŚCI I DANYCH OSOBOWYCH

Szanując prywatność oraz prawa naszych Klientów, Spółka, w związku ze świadczeniem usług, 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. z późniejszymi zmianami, Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r. z późniejszymi zmianami oraz ogólne rozporządzenie o ochronie danych (RODO). 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 oraz poza nimi 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 oraz usług świadczonych drogą elektroniczną, a w szczególności użytkownicy usługi dostępu do Internetu stacjonarnego oraz mobilnego, poprzez stosowanie się do niżej wymienionych zasad mogą dodatkowo chronić swoje bezpieczeństwo, 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 czy innym urządzeniu. 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 lub inne urządzenie (smartfon) w oprogramowanie antywirusowe i zaporę sieciową (firewall). Większość z dostępnego oprogramowania antywirusowego analizuje i zgłasza wymienione powyżej zagrożenia.
- W razie wykorzystania łączności bezprzewodowej dla Twojego urządzenia (telefonu, smartfona, komputera lub routera), takiej jak WiFi, Bluetooth, pamiętaj o konieczności zabezpieczenia połączenia łączności bezprzewodowej odpowiednimi hasłami oraz mechanizmami szyfrowania danych (jeśli są dostępne). W razie braku potrzeby wykorzystania łączności bezprzewodowej pamiętaj o wyłączeniu tych funkcji w urządzeniu. Niezabezpieczony dostęp poprzez mechanizmy łączności bezprzewodowej może ułatwiać włamanie do Twojego urządzenia lub sieci.
- Dokładnie weryfikuj nieznane numery, które do Ciebie dzwonią. Oddzwaniaj wyłącznie wtedy, kiedy masz pewność, że połączenie nie zostało zainicjowane w celu wyłudzenia połączenia międzynarodowego lub połączenia na usługi o podwyższonej opłacie.
- Dokładnie weryfikuj dokumenty i informacje, na podstawie których dokonujesz płatności (w szczególności numer rachunku bankowego). Oszuści często wysyłają wiadomości i dokumenty bardzo podobne do tych, które powinieneś otrzymać, chcąc abyś wpłacił pieniądze na fałszywe konto.
- Weryfikuj dokładnie oferty otrzymywane od innych operatorów i dostawców usług. Na rynku działają operatorzy i przedstawiciele handlowi, którzy celowo wprowadzają w błąd co do swojej tożsamości i firmy, bazując na podobieństwach nazw i marek znanych na rynku operatorów.
- Pamiętaj o osobistych i majątkowych prawach autorów. Utwory (teksty, filmy, muzyka, zdjęcia, aplikacje) mogą być ogólnodostępne w sieci Internet, ale nie oznacza to, że możesz je dowolnie wykorzystywać. W razie wątpliwości co do licencji i możliwości wykorzystania utworów kontaktuj się z autorem lub podmiotem, który go reprezentuje. Informacje na temat licencji oraz informacje o autorze powinny być w szczególności zawarte na stronie internetowej, na której rozpowszechniany jest utwór lub/oraz dołączone do utworu (np. w przypadku aplikacji).