

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

1.1. Szanując prywatność oraz prawa Abonentów, JPK 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).

1.2. Dane przetwarzane są również na podstawie aktualnych zgód wyrażonych przez Abonentów w szczególności podczas zawierania umowy oraz podczas czynności obsługowych.

1.3. 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. 1.4. 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:

a) 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.

b) 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.

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

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

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

f) 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).

g) 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.

h) 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.

i) 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.

j) Dokładnie weryfikuj nieznaną numer, 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.

k) 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.

l) 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.

ł) 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).

2.1 Konsekwencje prawne wykorzystania usług telekomunikacyjnych oraz usług świadczonych drogą elektroniczną w sposób niezgodny z prawem lub stanowiący rozpowszechnianie szkodliwych treści mogą być zarówno regulaminowe jak i prawne.

2.2 Zgodnie z postanowieniami Regulamin świadczenia usług JPK lub Regulaminów Promocji, w stosunku do Abonentów, którzy dopuszczają się nadużyć, mogą być wyciągnięte następujące konsekwencje:

- a) upomnienie telefoniczne lub listowne,
- b) czasowe zawieszenie świadczenia usług,
- c) wypowiedzenie umowy abonenckiej.

2.3 Konsekwencje prawne naruszeń są określone w szczególności w:

- a) Ustawie z dnia 6 czerwca 1997 r. Kodeks karny;
- b) Ustawie z dn. 4 lutego 1996 r. o prawie autorskim i prawach pokrewnych;
- c) Ustawie z dnia 20 maja 1971 r. Kodeks wykroczeń;
- d) Ustawie z dnia 23 kwietnia 1964 r. Kodeks cywilny;
- e) Ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną;
- f) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

2.4 Konsekwencje naruszeń mogą polegać na wymierzeniu kary pozbawienia wolności, ograniczenia wolności lub grzywny oraz odebrania przedmiotów służących do popełnienia przestępstwa. Szczegółowo konsekwencje dla poszczególnych naruszeń są określone w powyżej wymienionych aktach prawnych.

2.5 W przypadku, gdy JPK stwierdzi powyższe naruszenia, jest uprawniony do blokady inicjowania połączeń lub zawieszenia wszelkich usług wobec Abonenta dopuszczającego się naruszeń. Odbywa się to na zasadach określonych w regulaminach.

2.6 Niezależnie, w przypadku gdy dane działanie wypełnia znamiona przestępstwa, JPK bądź inna osoba dotknięta naruszeniem może złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa do odpowiednich organów ścigania.

2.7 JPK w razie poniesienia szkody w związku z opisanymi powyżej działaniami może również skorzystać z drogi sądowej, w celu uzyskania odpowiedniego odszkodowania za poniesioną szkodę (postępowanie cywilno-prawne).

2.8 Sposoby pozasądowego rozwiązywania sporów Spory pomiędzy Abonentem a JPK rozwiązywane są w pierwszej kolejności w trybie postępowania reklamacyjnego. Tryb reklamacyjny określony jest w Regulaminie świadczenia usług JPK. Po wyczerpaniu drogi postępowania reklamacyjnego konsumentowi przysługuje prawo do dochodzenia swoich roszczeń w trybie pozasądowego rozwiązywania sporów.

2.9 Pozostałe informacje o niezgodnych z prawem sposobach wykorzystania usług telekomunikacyjnych i usług świadczonych drogą elektroniczną oraz możliwości ochrony bezpieczeństwa, prywatności i danych osobowych podczas korzystania z publicznie dostępnych usług telekomunikacyjnych oraz usług świadczonych drogą elektroniczną jest dostępna na stronie: <https://archiwum.uke.gov.pl/badz-swiadomy-zagrozen-w-sieci-12886>