Załącznik nr 1 do Regulaminu Serwisu Hediup

.....
(miejscowość, data)

.....

.....

.....

(imię, nazwisko,
adres konsumenta)

Hediup – Michał Boczkowski Hediup
ul. Bałtycka 15 lok. 2.1
51-109 Wrocław

OŚWIADCZENIE O ODSTĄPIENIU OD UMOWY ZAWARTEJ NA ODLEGŁOŚĆ

Na podstawie ustawy z dnia 30 maja 2014 r. o prawach konsumenta, zgodnie z przysługującym mi prawem, odstępuję od umowy zawartej na odległość dnia .....

Odstąpienie od umowy dotyczy zamówienia: .....

Adres e-mail użyty podczas składania zamówienia: .....

Jednocześnie proszę o zwrot ceny zakupionej usługi w sposób, w jaki dokonano płatności* / na numer konta bankowego nr:

.....

.....
Podpis konsumenta

***** Niepotrzebne skreślić

Załącznik nr 2 do Regulaminu Serwisu Hediup

INFORMACJA O SZCZEGÓLNYCH ZAGROŻENIACH ZWIĄZANYCH Z KORZYSTANIEM Z USŁUGI ŚWIADCZONEJ DROGĄ ELEKTRONICZNĄ

1. Hediup informuje o szczególnych zagrożeniach związanych z korzystaniem z usług świadczonych drogą elektroniczną. Informacja niniejsza dotyczy zagrożeń, które mogą wystąpić jedynie potencjalne, ale które powinny być brane pod uwagę, mimo stosowania przez Hediup środków zabezpieczających infrastrukturę Hediup przed nieuprawnionym działaniem osób trzecich. Do podstawowych zagrożeń związanych z korzystaniem z sieci Internet należą:
    a. złośliwe oprogramowanie (ang. malware) – różnego rodzaju aplikacje lub skrypty mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do systemu teleinformatycznego użytkownika sieci, takie jak wirusy, robaki, trojany (konie trojańskie), keyloggery, dialery;
    b. programy szpiegujące (ang. spyware) – programy śledzące działania użytkownika, które gromadzą informacje o użytkowniku i wysyłają je - zazwyczaj bez jego wiedzy i zgody - autorowi programu;
    c. spam - niechciane i nie zamawiane wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców, często zawierające treści o charakterze reklamowym;
    d. wyłudzanie poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. phishing);
    e. włamania do systemu teleinformatycznego użytkownika z użyciem m.in. takich narzędzi hackerskich jak exploit i rootkit.
2. Aby uniknąć powyższych zagrożeń, należy zaopatrzyć swoje urządzenia elektroniczne, wykorzystywane w celu podłączania się do Internetu, w program antywirusowy. Program taki powinien być stale aktualizowany. Ochronę przed zagrożeniami związanymi z korzystaniem z usług świadczonych drogą elektroniczną zapewniają także:
    a. włączona zapora sieciowa (ang. firewall);
    b. aktualizacja wszelkiego oprogramowania;
    c. nieotwieranie załączników poczty elektronicznej niewiadomego pochodzenia;
    d. czytanie okien instalacyjnych aplikacji, a także ich licencji;
    e. wyłączenie makr w plikach MS Office nieznanego pochodzenia;
    f. regularne całościowe skany systemu programem antywirusowym i antymalware;
    g. szyfrowanie transmisji danych;
    h. instalacja programów prewencyjnych (wykrywania i zapobiegania włamaniom);
    i. używanie oryginalnego systemu i aplikacji, pochodzących z legalnego źródła.