Informacja o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną

Działając na podstawie art. 6 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jednolity: Dz. U. z 2020 r. poz. 344, z późn. zm.), Sprzedawca - Mille Sapori Plus sp. z o.o. z siedzibą w Warszawie przy ul. Kazimierza Gierdziejewskiego 7, 02-495 Warszawa, wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000361584, o kapitale zakładowym 500.000,00 złotych w całości wpłacony, NIP 5272633791, REGON 142437942, niniejszym informuje o potencjalnych zagrożeniach związanych z korzystaniem ze sklepu internetowego „Mille Sapori", jako usługi świadczonej drogą elektroniczną, w tym między innymi o:

- możliwości otrzymania spamu, czyli niezamówionej informacji reklamowej (handlowej) przekazywanej drogą elektroniczną;
- obecności i działania oprogramowania typu *malware*, w tym: wirusów komputerowych (szczególnego oprogramowania, które jest w stanie, po uruchomieniu, zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez użytkownika); wirusy mogą być mniej lub bardziej szkodliwe dla systemu operacyjnego, w którym się znajdują, ale nawet w najmniej poważnym przypadku są marnotrawstwem pamięci RAM, CPU i miejsca na twardym dysku. Termin *malware* odnosi się do natrętnego oprogramowania takiego jak: wirusy, konie trojańskie, *ransomware*, *spyware*, *adware*, *scareware* i inne szkodliwe programy;
- obecności i działania tzw. robaków internetowych (*worm*), czyli oprogramowania zdolnego do samopowielania;
- możliwości zadziałania oprogramowania szpiegującego typu *spyware*, to jest oprogramowania śledzącego działania użytkownika w Internecie, uaktywniającego się bez jego wiedzy, zgody i kontroli;
- możliwości wyłudzenia poufnych informacji osobistych (np. haseł) przez podszywanie się pod godną zaufania osobę lub instytucję (ang. *phishing*);
- możliwości włamania do systemu teleinformatycznego użytkownika z użyciem m.in. takich narzędzi hackerskich jak *exploit* i *rootkit*;
- czynnościach kryptoanalizy, tj. odnalezienia słabości systemu kryptograficznego, a tym samym umożliwienia jego złamania lub obejścia;

Zamawiający, aby uniknąć powyższych zagrożeń, powinien zaopatrzyć swój komputer i inne urządzenia elektroniczne, które wykorzystuje podłączając się do Internetu, w program antywirusowy i zaporę sieciową (firewall). Program taki powinien być stale aktualizowany.